Bugzilla ID: 406968
Bugzilla Summary: ADD new root certificate for camerifirma

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	Camerfirma
Website URL	http://www.camerfirma.com
Organizational type	Private Company, Commercial CA, Regional CA in Spain
Primary market / customer base	AC Camerfirma S.A. is a commercial CA issuing certificates for companies primarily in Spain. Camerfirma is the digital certification authority for Chambers of Commerce in Spain.

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

Info Needed	Data	Data
Certificate Name	Chambers of Commerce Root - 2008	Global Chambersign Root - 2008
Cert summary / comments	This CA issues certificates for Spanish companies and representatives. Chambers of Commerce act as RAs for end user registration.	This CA issues certificates for general use globally. Other companies act as RAs for end user registration.
The root CA certificate URL	https://bugzilla.mozilla.org/attachment.cgi?id=339325	https://bugzilla.mozilla.org/attachment.cgi?id=339324
SHA-1 fingerprint.	78:6a:74:ac:76:ab:14:7f:9c:6a:30:50:ba:9e:a8:7e:fe:9a:ce:3c	4a:bd:ee:ec:95:0d:35:9c:89:ae:c7:52:a1:2c:5b:29:f6:d6:aa:0c
Valid from	2008-08-01	2008-08-01
Valid to	2038-07-31	2038-07-31
Cert Version	3	3
Modulus length	4096	4096
Test website(s)	Need url to a website whose SSL cert chains up to this root.	Need url to a website whose SSL cert chains up to this root.
CRL	http://crl.camerfirma.com/root_chambers_2008.crl	http://crl.camerfirma.com/root_chambersign_2008.crl
CRL issuing frequency	CPS version 3.1.1 section 4.5.9: Certification Authority will issue a new CRL immediately after a change in the CRL content and at least once a day in case of no change is produced.	
OCSP Responder URL	http://ocsp.camerfirma.com	
List or description of subordinate CAs operated by the CA organization associated with the root CA.	Cert Hierarchy: http://www.camerfirma.com/mod_web/repositorio/otrascas.html	Cert Hierarchy: http://www.camerfirma.com/mod_web/repositorio/otrascas.html

	This root has the following internally operated subordinate CAs: • AC Camerfirma, Certificados Camerales: Issues certificates for end entities (Enterprise certificates for employees and representatives) • TSA: for Time Stamping process that issues TSU certificates. • CodeSign • Express Corporate Server: for SSL certificates Note: Chambers of Commerce are used as RAs for end users registration.	An intermediate CA called AC Camerfirma issued another sub-CA called RACER. This 2nd level Intermediate CA issues certificates for citizens and enterprise employees and representatives.
Subordinate CAs operated by third parties	None All roots are internally operated.	None All roots are internally operated.
List any other root CAs that have issued cross-signing certificates for this root CA	None	None
Requested Trust Bits One or more of: • Websites (SSL/TLS) • Email (S/MIME) • Code Signing	Websites Email Code Signing	Websites Email Code Signing
If SSL certificates are issued within the hierarchy rooted at this root CA certificate: • DV • OV • EV	OV The name of the organization is verified and the relationship with the domain owner. The organization existence is checked by means of online access to registration data bases. We user different sources to check like: registration access services and Chambers of commerce data bases. Google Translated text from CPS section 3.1.8: The appointed applicant's physical and the presentation of his National Document Identity, residence card or passport. Identification of the company, for which the RA require documentation relevant to the type of entity. This information is included in the Operating manuals of RA.	
EV Policy OID(s)	Not requesting EV at this time.	
CP/CPS	Certificate Practice Statement: https://www.camerfirma.com/mod_web/usuarios/pdf/CPS_3.1.1.pdf	

	Translations into English of the sections of CP/CPS and/or RA Operating Manual having to do with verification of identity/organization, domain name ownership, and email address ownership.
AUDIT	Audit Type (WebTrust, ETSI etc.): WebTrust CA Auditor: Ernst & Young Auditor Website URL: http://www.ey.com Audit: https://cert.webtrust.org/ViewSeal?id=874 (2008-12-22)

Review CPS sections dealing with subscriber verification

- Verify domain check for SSL
    - CPS section 3.1.8: In regards to SSL certificates the subscriber identity will be checked by means of registration domain services access and the certificate issued will be seeded to those email that appeared in the technical contact and administrative contact. AC Camerfirma only accept PKCS10 request for SSL certificates.
    - Confirmed via Google Translate.
- 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.
    - CPS section 3.1.8: For signing end user certificates physical presence is required, id card and an authorisation of a enterprise representative. All communications are made by means of email.
    - Confirmed via Google Translate.
- Verify identity info in code signing certs is that of subscriber
    - CPS section 3.1.8: For signing code physical presence is required in a RA and an authorisation of a enterprise representative is needed
    - Confirmed via Google Translate.
- Make sure it's clear which checks are done for which context (cert usage)

Flag Problematic Practices

http://wiki.mozilla.org/CA:Problematic_Practices

- 1.1 Long-lived DV certificates
    - SSL certs are OV
    - Section 6.1.1 of the CPS indicates server certs can be 1, 2, or 3 years.
    - "We issue certificates till 3 year period. A contract is signed by the end user to revoke the certificate in case of any change."
- 1.2 Wildcard DV SSL certificates
    - SSL certs are OV
    - "We issue wildcard certificates but we are going to change this practice and include different 2nd lever domains in the subjectaltname."
- 1.3 Issuing end entity certificates directly from roots
    - As per the cert hierarchy diagram in the CPS, these roots are offline roots which issue subordinate CAs for issuing end entity certs.

- 1.4 Allowing external entities to operate unconstrained subordinate CAs
  - All roots are internally operated.
- 1.5 Distributing generated private keys in PKCS#12 files
  - no
- 1.6 Certificates referencing hostnames or private IP addresses
  - no
- 1.7 OCSP Responses signed by a certificate under a different root
  - no
- 1.8 CRL with critical CIDP Extension
  - CRL loaded successfully into Firefox.

Verify Audits

- Validate contact info in report, call to verify that they did indeed issue this report.
  - WebTrust CA audit is posted on cert.webtrust.org.
- For EV CA's, verify current WebTrust EV Audit done.
  - Not requesting EV at this time
- Review Audit to flag any issues noted in the report
  - Both roots are covered in the WebTrust CA audit. No issues noted in report.