Bugzilla ID: 406968
Bugzilla Summary: ADD camerifirma EV root certificates

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.
CA Contact Information	CA Email Alias: soporte@camerfirma.com CA Phone Number: 349 13 443743 Title / Department: Technical Department

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	There is a "Chambers of Commerce Root" root certificate currently included in NSS, which is SHA1 2048-bit. This new root is SHA1 4096-bit. This root will have internally-operated subordinate CAs that issue certificates for Spanish companies and representatives. Chambers of Commerce act as RAs for end user registration.	There is a "Global Chambersign Root" root certificate currently included in NSS, which is SHA1 2048-bit. This new root is SHA1 4096-bit. This root will have internally-operated subordinate CAs that issue 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)	https://server1.camerfirma.com:8081/	https://server2.camerfirma.com:8082/
CRL	http://crl.camerfirma.com/camerfirma_cserver-2009.crl http://crl.camerfirma.com/root_chambers_2008.crl	http://crl.camerfirma.com/racer-2009.crl http://crl.camerfirma.com/root_chambersign_2008.crl

CRL issuing frequency	CPS Section 2.6.2: Ordinarily the issuing CA certificates for end entities publishes a list of revoked certificates at once every 12 hours. CP EV section 4.5.8: The CA will publish and update the CRL at least once weekly and keeping it published for 10 days. Comment #45: “at the moment these CAs are not issuing certificates so we keep a CRL for 3 months, when we begin to issue certificates we will issue a daily CRL.”	
OCSP Responder URL	http://ocsp.camerfirma.com CP EV section 4.5.10 This service will be updated at least every 4 days. The OCSP responses to this service should have a valid period of 10 days.	
CA Hierarchy	Cert Hierarchy: http://www.camerfirma.com/mod_web/repositorio/otrascas.html This root will have 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 • Corporate Server EV Note: Chambers of Commerce are used as RAs for end users registration.	Cert Hierarchy: http://www.camerfirma.com/mod_web/repositorio/otrascas.html 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.
Sub-CAs operated by 3rd parties	None All roots are internally operated.	None All roots are internally operated.
Cross-Signing	None	None
Requested Trust Bits	Websites Email Code Signing	Websites Email Code Signing
SSL Validation Type DV, OV, and/or EV	OV, EV	
EV Policy OIDs	1.3.6.1.4.1.17326.10.14.2.*.*	1.3.6.1.4.1.17326.10.8.12.*.*
EV Policy OIDs	The last 2 digits are used for identify the Private Key management, and can be 1.2 or 2.2: 1.2 Private key generated stored in a software device and generated by the User	

	2.2 Private key generated stored in a SSCD device and generated by the User
CP/CPS	All Documents are in Spanish Policy Repository: http://policy.camerfirma.com/ Certificate Practice Statement: http://policy.camerfirma.com/politicas/CPS_V_3.1.4.pdf CP of RACER sub-CA: http://policy.camerfirma.com/pdf/PC_RACER_1_2_1.pdf Certification Policy Camerfirma Express Corporate Server: http://policy.camerfirma.com/politicas/PC_Camerfirma_Express_Corporate_Server_1_0_1.pdf Certification Policy for Camerfirma Corporate Server EV: http://www.camerfirma.com/mod_web/usuarios/pdf/PC_Camerfirma_Corporate_Server_EV_1_0.pdf Certification Policy for Code Signing: http://policy.camerfirma.com/politicas/PC_Camerfirma_CodeSign_1_0_1.pdf
AUDIT	Audit Type: WebTrust CA Auditor: Ernst & Young Auditor Website URL: http://www.ey.com Audit: https://cert.webtrust.org/ViewSeal?id=874 (2008.12.22) Both roots are covered in the WebTrust CA audit. Audit Type: WebTrust EV Auditor: Ernst & Young Audit (Spanish): http://docs.camerfirma.com/mod_web/usuarios/pdf/Informe_agrupado_Camerfirma_WebTrust_EV.pdf (2009.01.31) Audit (English): http://docs.camerfirma.com/mod_web/usuarios/pdf/Informe_agrupado_Camerfirma_EV_English.pdf Subject: Re: Confirming Authenticity of WebTrust EV audit report for Camerfirma From: Angel.IzquierdoEsteban@es.ey.com To: Kathleen Wilson <kwilson@mozilla.com> Hi Kathleen, Find below the answers to your questions: > Would you please reply to this email to confirm that Ernst & Young did indeed issue the auditor's statement at the above URL? Yes, I confirm it. > Since I cannot read Spanish, would you also please provide the date on which the actual audit completed? It looks like the first paragraph of the audit statement indicates that the audit completed in January of 2009. However, the signature on the audit statement is January 19, 2010. Yes, the statement´s date is correct although there is a later date in the report, here I send the english version: > Please also confirm that this audit statement covers the "Chambers of Commerce Root - 2008" and "Global Chambersign Root – 2008" roots and their corresponding CA hierarchies. Yes it does.

Verification of Organization Identity	“The organization existence is checked by means of online access to registration data bases. We use different sources to check like: registration access services and Chambers of commerce data bases.” Translation of CPS section 3.1.8 Authentication of the identity of an individual, the organization and its linkage. To make a correct identification of a subscriber's identity, AC Camerfirma through the RA requires: Certificates recognized: • The physical Impartiality of the Applicant, or representative of the applicant if this is a legal entity and the presentation of his paper National identity card, residence card or passport. • Identification of the company, for which the required documentation RA relevant depending on the type of entity. This information is included in Operational Manuals and the RA's web Camerfirma. • Identification of representation . For certificates of empowerment and representation: documentation on the ability of representation of Signer / Subscriber regarding the entity, by delivery of notarial deeds demonstrate their performance. There will be a certificate issued by the commercial register with less than 10 days old. The RA may also have electronic means for the online consultation of the state representation of the applicant. Certificates of seizing the different powers are described in a table of entries, which are incorporated in the certificate of two ways: one placed in the Title field (TITLE) specify the details of representation, and two by a field link STATEMENT USER (USER NOTICE) to scripts scanned and signed by the RA operator. To link certificates must be presented in a authorization signed by a representative of the company. The certificate of legal person, where the signer / subscriber and the applicants are different should be documented that the applicant has sufficient powers to make such application certificate by submitting a commercial registration certificate not exceeding 10 days or query the data online registration. AC Camerfirma allows the replacement of the physical presence of the subscriber through access to the application forms through an electronic ID. AC Camerfirma estimated that the last physical presence was made on the date of marked by the certificate issuance of electronic ID and they take to perform their internal estimates. Technical Certificates: Certificates for secure Web server checks for the company through access to commercial registers or the BBDD or the tax office, the existence of the domain and the right to use this by the subscriber is checked through access to databases of Internet domains. The certificates are delivered to the authorities who appear in these databases. The issuance of certificates of corporate seal is supported by documentary by querying the existence of the company in the BBDD or the AEAT register and the authorization signed by a representative of the company. For code signing certificates Camerfirma brings to light the business by accessing the BBDD from the AEAT or trade register. AC Camerfirma request an authorization document signed by a representative of the company.

The encryption certificates will be issued by submitting a form telematics valid identity certificate.

Secure Server Certificates (EV) "extended validation" be made following the same procedures that a certificate has business, requiring physical presence of the applicant or an authorized person before the RA for the issuance of the certificate. The secure server certificate (EV) can be therefore considered a qualified certificate.

Translation of CPS Section 4.3, Issuing Certificates
The usual process followed in the issuance of certificates is as follows:

Previously, the subscriber has entered his application by accessing the form or by loading a batch of requests.

Be obtained from the subscriber's physical presence at the premises of RA or in a place agreed, provided that this application has not been done with a electronic ID or with a certificate recognized by AC Camerfirma admitted in this case will not be needed physical presence.

The administrator verifies the RA service payments, documentation on the request and the identity of the signer / subscriber.

If the signer / subscriber has a cryptographic device, once approved license application by the RA operator will generate the keys on the device and a standard PKCS10 request, the certificate will be issued automatically and shall carry the burden of the certificate on the device of the subscriber. All this process is performed in the setting of RA.

The subscriber could also conduct their own key generation in a cryptographic device and deliver the PKCS10 request for AC Camerfirma issue the certificate, once the RA has verified the relevant documents.

If the key is generated by the AC (AC Camerfirma currently emits only in this mode, software licenses) after approval of the request by the operator RA, you will reach the I / Subscriber:
A link to the page where you generate the certificate in PKCS # 12.
A PIN needed for installation of the key and certificate. The subscriber may choose in the application form sent
using SMS.
The Signer / Subscriber also needed for the process of creating key and certificate, a code that is printed on the contract with the RA and AC.

For secure server certificate issuance process is performed AC Camerfirma after verification by the existence of the company, the domain for which is to issue the certificate and the right to use the domain by the applicant. Subsequently, the certificate is sent to contacts administrative and technical that appear in the databases of the.

	For code signing certificates and corporate seal may be used two types Circuit: Petitions PKCS # 10 and shipments in response PKCS # 7 or send direct Camerfirma from the PKCS # 12. The RA verifies the data previously incorporate in the certificate. The RA will verify the existence of the company and identity subscriber's authorization to submit the applicant. Models authorizations are published on the website of AC Camerfirma SA. Encryption certificates are issued automatically, once the incumbent is identified with a valid identity certificate to the Web application developed to effect at https: / / www.camerfirma.com. Comment #43: From: CPS 3.1.8 SSL Certificates Section: Certificate subscript identity existence is validated against the Internet Domains Data Bases. Afterwards the organization existence associates with this domain must be checked against the Companies Register Data Bases (Spanish Chambers of Commerce Data Base). Finally the RA operator will send the certificate to the administrative contact and technical contact included in the Internet domain data base. From the Operating Manual v1.0 (internal document, but included in audits) Digital Certificate Generation Process. (section) From the RA application we get: URL to be certified, Organization Vat number identification, Digital certificate validity Applicant mail address. Before approve the request we must: Be assured of the organization existence, by means of one of these methods: a) Spanish Administration TAX Data Base. b) Chambers of Commerce Data Base. c) Spanish Companies Register Data Base. Be assured that the certificates is paid Be assured that the domain exists and is linked with the organization previously verified consulting the Internet Domain Data Bases. http://www.networksolutions.com http://www.gandi.net http://www.interdomain.com http://www.nic.es

	http://www.nominalia.com
Verification of Domain Name Ownership / Control Non-EV	CPS section 3.1.8: For secure server certificates, the subscriber identity is verified through access to databases of Internet domains and the certificates are delivered to the authorities who appear in those databases. From the RA Operating Manual (internal, audited document): Be assured of the organization existence, by means of one of these methods: Spanish Administration TAX Data Base. Chambers of Commerce Data Base. Spanish Companies Register Data Base. Be assured that the domain exists and is linked with the organization previously verified consulting the Internet Domain Data Bases.
Verification of Domain Name Ownership / Control EV	Translation of CPS Section 1.2.1: Corporate Server EV This intermediate certification authority issues digital certificates for services secure server or corporate seal with the same functionality that makes "Express Corporate Server ". In this case the Certification Authority is governed by legislation Additional Extended Validation (EV) subject to the requirements of the "CA / Browser Forum Guidelines for Issuance and Management of extended validation certificates. This legislation promotes the issuance of certificates with additional safeguards in the process identification of holders of certificates. In this case the name of the authority of adjective loses its certification, the guarantees Express accreditation obtain the certificate are more demanding and therefore require more time in their emission process. Translation of CP EV Section 1.2, Overview This document specifies the Certificate Policy Certification Camerfirma Corporate Server, and is based on the standard specification of RCF 2527 - Internet X. 509 Public Key Infrastructure Certificate Policy, the IETF. AC Camerfirma is in accordance with current versions of "CA / Browser Forum Gidelines for Issuance and Management of Extended Validation certificates "published in http://www.cabforum.org. In case of any inconsistency between these policies and the Guidelines were taken as valid latter. This policy is in accordance with the PC of Chambers of Commerce Root, which may locate at the following address http://policy.camerfirma.com and establishing standards, policies and procedures for the issuance of the second level. This policy defines the rules and responsibilities that should the Authority Second-level certification for issuance of secure server, also impose certain obligations that must be taken into account by the subscriber and relying party under its special relationship with this type of certificates. The secure server certificate is required to provide reasonable assurance the user of an application used to access Internet sites that the Web pages that you access and whose address is incorporated as a holder of digital certificate, is controlled by the entity whose name is incorporated into the same digital certificate. In addition, the certificate will ensure the confidentiality of data sent and received from the computer equipment where they live Web pages accessed by client

	applications through encryption techniques. Translation of CP EV CP Section 4.1, Certificate Request a) Before starting the procedure of issuance, the CA must inform the subscriber the terms and conditions pertaining to use of the certificate b) The CA shall communicate this information through a media durable, capable of being transmitted electronically and in language understandable. c) The CA shall ensure that: • The existence of the organization, through access to public records or owners. • Checking the identity of the applicant or person authorized by supporting evidence. The documentation will be delivered in person in an AC Camerfirma registration office. Physical presence could be substituted for an online application signed with a valid and recognized certificate and for those other options approved by the current legislation. • That the organization has the control in the uses of the domain through consultation in the registries of domain. d) The applicant's address and other contact details should be facilitated. e) The AC should comply with all the requirements imposed by the data protection legislation. Translation of CP EV CP Section 4.3, Issuing Certificates The CA must use all the means at its disposal to ensure that the emission and renewal of certificates is done safely. In particular: • The CA must make reasonable efforts within its scope to confirm the uniqueness of the DN assigned to the subscribers. • Confidentiality and integrity of data recorded will be especially protected when the data is exchanged with the subscriber or between different components of the certification system. • The CA must verify that registration data is exchanged recognized service providers, whose identity is authenticated. • The CA shall notify the applicant of the issuance of your certificate.
Verification of Email Address Ownership / Control	CPS section 3.1.8: For signing end user certificates physical presence is required, id card and an authorisation of a enterprise representative. All other communications are made by means of email.
Verification of Identity of Subscriber for Code Signing Certs	CPS section 3.1.8: For signing code physical presence is required in a RA and an authorisation of a enterprise representative is needed Certification Policy for Code Signing: http://policy.camerfirma.com/politicas/PC_Camerfirma_CodeSign_1_0_1.pdf
Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices • 1.1 Long-lived DV certificates o SSL certs are OV. Section 6.1.1 of the CPS indicates server certs can be 1, 2, or 3 years. o "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 o SSL certs are OV o "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 o 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 o All roots are internally operated. • 1.5 Distributing generated private keys in PKCS#12 files o No. AC Camerfirma only accept PKCS10 request for SSL certificates. • 1.6 Certificates referencing hostnames or private IP addresses o no • 1.7 OCSP Responses signed by a certificate under a different root o no • 1.8 CRL with critical CIDP Extension o CRLs loaded successfully into Firefox.