

## Mozilla - CA Program

### Case Information

<b>Case Number</b>	00000080	<b>Case Record Type</b>	CA Owner/Root Inclusion Request
<b>CA Owner/Certificate Name</b>	Camerfirma	<b>Request Status</b>	Initial Request Received

### Additional Case Information

<b>Subject</b>	Include renewed Camerfirma Root Certs	<b>Case Reason</b>	New Owner/Root inclusion requested
----------------	---------------------------------------	--------------------	------------------------------------

### Bugzilla Information

<b>Link to Bugzilla Bug</b>	<a href="https://bugzilla.mozilla.org/show_bug.cgi?id=986854">https://bugzilla.mozilla.org/show_bug.cgi?id=986854</a>
-----------------------------	---

### General information about CA's associated organization

<b>CA Email Alias 1</b>	gestion_soporte@camerfirma.com		
<b>CA Email Alias 2</b>			
<b>Company Website</b>	<a href="http://www.camerfirma.com">http://www.camerfirma.com</a>	<b>Verified?</b>	Verified
<b>Organizational Type</b>	Commercial Organization	<b>Verified?</b>	Verified
<b>Organizational Type (Others)</b>		<b>Verified?</b>	Not Applicable
<b>Geographic Focus</b>	Spain	<b>Verified?</b>	Verified
<b>Primary Market / Customer Base</b>	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.	<b>Verified?</b>	Verified
<b>Impact to Mozilla Users</b>	Update/Replace currently included root certs.	<b>Verified?</b>	Verified

### Response to Mozilla's list of Recommended Practices

<b>Recommended Practices</b>	<a href="https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices">https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices</a>	<b>Recommended Practices Statement</b>	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.
<b>CA's Response to Recommended Practices</b>	<ol style="list-style-type: none"> <li>1) Publicly Available CP and CPS: Yes</li> <li>2) CA Hierarchy: Yes</li> <li>3) Audit Criteria: Yes</li> <li>4) Document Handling of IDNs in CP/CPS: No</li> <li>5) Revocation of Compromised Certificates: Yes (CPS section 4.8.2)</li> <li>6) Verifying Domain Name Ownership: Yes</li> <li>7) Verifying Email Address Control: Yes</li> <li>8) Verifying Identity of Code Signing Certificate Subscriber: Not applicable. Mozilla is no longer enabling the Code Signing trust bit for root certificates.</li> <li>9) DNS names go in SAN: Camerfirma confirms at least a DNSname is included in SAN. All domains included must be verified as SSL Verification practices</li> <li>10) Domain owned by a Natural Person: No SSL certificates have been issued to natural persons</li> <li>11) OCSP: Confirm OCSP responds according to expected</li> <li>12) Network Security Controls: Yes</li> </ol>	<b>Verified?</b>	Need Response From CA

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

<b>Potentially Problematic Practices</b>	<a href="https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices">https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices</a>	<b>Problematic Practices Statement</b>	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**

NEED CA's response to each of the items listed in [https://wiki.mozilla.org/CA:Problematic Practices#Potentially problematic CA practices](https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices)

Verified?

Need Response From CA

- 1) Long-lived DV certificates: ??? CA issue certificates till 3 year period. A contract is signed by the end user to revoke the certificate in case of any change.
- 2) Wildcard DV SSL certificates: certificates SSL certs are OV, CA only issue wildcard certificates to subscribers whose actual identity has been validated with organizational validation (OV).
- 3) Email Address Prefixes for DV Certs: DV Certs SSL certs are OV, the email used for verification is in WHOIS administration or technical contact.
- 4) Delegation of Domain / Email validation to third parties: See CPS section 2.2 The verifications can only be performed for RA. Each RA is internally audited by the CA auditors
- 5) 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
- 6) Allowing external entities to operate subordinate CAs: No
- 7) Distributing generated private keys in PKCS#12 files: No
- 8) Certificates referencing hostnames or private IP addresses: No
- 9) Issuing SSL Certificates for Internal Domains: No
- 10) OCSP Responses signed by a certificate under a different root: OCSP Responses are signed according RFC 6960 using an OCSP Responder certificate issued directly by the CA that is identified in the request.
- 11) SHA-1 Certificates: Yes
- 12) Generic names for CAs: No
- 13) Lack of Communication With End Users: No  
Anyone can contact with Camerfirma via contact info in section 1.7 of the CPS.
- 14) Backdating the notBefore date: No backdating is allowed.  
Certificates are issued with the notBefore field including the date which was issued (using official time sources as described in section 6.10 of the CPS).

## Root Case Record # 1

### Root Case Information

<b>Root Certificate Name</b>	CHAMBERS OF COMMERCE ROOT - 2016	<b>Root Case No</b>	R00000116
<b>Request Status</b>	Initial Request Received	<b>Case Number</b>	00000080

### Additional Root Case Information

<b>Subject</b>	Include CHAMBERS OF COMMERCE ROOT - 2016
----------------	--

### Technical Information about Root Certificate

<b>O From Issuer Field</b>	AC CAMERFIRMA S.A.	<b>Verified?</b>	Verified
<b>OU From Issuer Field</b>	CHAMBERS OF COMMERCE ROOT - 2016	<b>Verified?</b>	Verified
<b>Certificate Summary</b>	There is a "Chambers of Commerce Root - 2008" root certificate now included in NSS, which is SHA-1 4096-bit. This new root is SHA-256 4096-bit and have internally-operated subordinate CAs that issue certificates for Spanish companies and representative.	<b>Verified?</b>	Verified
<b>Root Certificate Download URL</b>	<a href="http://www.camerfirma.com/certs/chambersofcommerceroot-2016.crt">http://www.camerfirma.com/certs/chambersofcommerceroot-2016.crt</a>	<b>Verified?</b>	Verified
<b>Valid From</b>	2016 Apr 14	<b>Verified?</b>	Verified
<b>Valid To</b>	2040 Apr 08	<b>Verified?</b>	Verified
<b>Certificate Version</b>		<b>Verified?</b>	Verified
<b>Certificate Signature Algorithm</b>	SHA-256	<b>Verified?</b>	Verified
<b>Signing Key Parameters</b>	4096	<b>Verified?</b>	Verified
<b>Test Website URL (SSL) or Example Cert</b>	<a href="https://cev.camerfirma.com/">https://cev.camerfirma.com/</a> <a href="https://cov.camerfirma.com/">https://cov.camerfirma.com/</a>	<b>Verified?</b>	Verified

<b>CRL URL(s)</b>	<a href="http://crl.camerfirma.com/chambersofcommerceroot-2016.crl">http://crl.camerfirma.com/chambersofcommerceroot-2016.crl</a>	Verified?	Verified
<b>OCSP URL(s)</b>	<a href="http://ocsp.camerfirma.com">http://ocsp.camerfirma.com</a>	Verified?	Verified
<b>Trust Bits</b>	Email; Websites	Verified?	Verified
<b>SSL Validation Type</b>	OV; EV	Verified?	Verified
<b>EV Policy OID(s)</b>	1.3.6.1.4.1.17326.10.14.2.1.2 1.3.6.1.4.1.17326.10.14.2.1.1 1.3.6.1.4.1.17326.10.16.3.5.1 1.3.6.1.4.1.17326.10.16.3.5.2 1.3.6.1.4.1.17326.10.16.3.6.1.3.2.1 1.3.6.1.4.1.17326.10.16.3.6.1.3.2.2	Verified?	Verified
<b>Root Stores Included In</b>	Microsoft; Mozilla	Verified?	Verified
<b>Mozilla Applied Constraints</b>	No	Verified?	Verified

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

<b>Revocation Tested</b>	No Error	Verified?	Verified
<b>CA/Browser Forum Lint Test</b>	ERROR: CA certificates must set keyUsage extension as critical ERROR: Invalid country in countryName WARNING: - CA certificates should not have a validity period greater than 25 years	Verified?	Need Clarification From CA
<b>Test Website Lint Test</b>	No Error	Verified?	Verified
<b>EV Tested</b>	// CN=CHAMBERS OF COMMERCE ROOT - 2016,O=AC CAMERFIRMA S.A.,OID.2.5.4.97=VATES-A82743287,serialNumber=A82743287,OU=CHAMBERS OF COMMERCE ROOT - 2016,OU=see current address at <a href="http://www.camerfirma.com/address,L=MADRID,ST=MADRID,C=ES">www.camerfirma.com/address,L=MADRID,ST=MADRID,C=ES</a> "1.3.6.1.4.1.17326.10.14.2.1.2", "Camerfirma EV OID", SEC_OID_UNKNOWN, { 0x04, 0xF1, 0xBE, 0xC3, 0x69, 0x51, 0xBC, 0x14, 0x54, 0xA9, 0x04, 0xCE, 0x32, 0x89, 0x0C, 0x5D, 0xA3, 0xCD, 0xE1, 0x35, 0x6B, 0x79, 0x00, 0xF6, 0xE6, 0x2D, 0xFA, 0x20, 0x41, 0xEB, 0xAD, 0x51 }, "MIIBDELMAKGA1UEBhMCRVMxDzANBgNVBAMk1BRFJJRDEPMA0GA1UEBwwGTUFE" "UkiEMTowOAYDVQQLDDFzZWUgY3VyemVudCBhZGRyZXNzIGF0IHd3dy5jYW1lcmZp" "cm1hLmNvbS9hZGRyZXNzMSkwJwYDVQLDCESEFNQkVSUyBPRiBBDT01NRVJDRSBS" "T09UIC0gMjAxNjESMBAGA1UEBRMJQTYgNzQzMjg3MRgwFgYDVQRhDA9WQVRFUy1B" "ODI3NDMyODcxGzAZBgNVBAoMEkFDIENBTUVSRkiSTUEgUy5BLjEpMCCGA1UEAwg" "Q0hBTUJFUIMgT0YgQ09NTUVSQ0UgUk9PVCAtdiDwMTY=", "NJotoYIGsrM=", Success!  <a href="https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version">https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version</a>	Verified?	Verified

### Digital Fingerprint Information

<b>SHA-1 Fingerprint</b>	78:6A:74:AC:76:AB:14:7F:9C:6A:30:50:BA:9E:A8:7E:FE:9A:CE:3C	Verified?	Verified
<b>SHA-256 Fingerprint</b>	04:F1:BE:C3:69:51:BC:14:54:A9:04:CE:32:89:0C:5D:A3:CD:E1:35:6B:79:00:F6:E6:2D:FA:20:41:EB:AD:51	Verified?	Verified

### CA Hierarchy Information

<b>CA Hierarchy</b>	CPS document: 1.2.1.3 Hierarchy Chambers of Commerce Root  <a href="http://docs.camerfirma.com/publico/DocumentosWeb/politicas/CPS_V_3_2_7_EN.pdf">http://docs.camerfirma.com/publico/DocumentosWeb/politicas/CPS_V_3_2_7_EN.pdf</a>	Verified?	Verified
<b>Externally Operated SubCAs</b>	In-House subCAs	Verified?	Verified
<b>Cross Signing</b>	N/A	Verified?	Verified
<b>Technical Constraint on 3rd party Issuer</b>	Registration Authorities: CPS sections 1.5.4 and 2.1.2  URL with a list of publicly disclosed subordinate CA: <a href="http://www.camerfirma.com/area-de-usuario/jerarquia-politicas-ypractic-as-de-certificacion/">http://www.camerfirma.com/area-de-usuario/jerarquia-politicas-ypractic-as-de-certificacion/</a>	Verified?	Verified

## Verification Policies and Practices

<b>Policy Documentation</b>	Language(s) that the documents are in: Spanish (The CPS are also translated into English)	Verified?	Verified
<b>CA Document Repository</b>	Spanish: <a href="http://www.camerfirma.com/area-de-usuario/jerarquia-politicas-y-practicas-de-certificacion/">http://www.camerfirma.com/area-de-usuario/jerarquia-politicas-y-practicas-de-certificacion/</a> English: <a href="http://www.camerfirma.com/en/area-de-usuario/jerarquia-politicas-y-practicas-de-certificacion/">http://www.camerfirma.com/en/area-de-usuario/jerarquia-politicas-y-practicas-de-certificacion/</a> CP: <input type="checkbox"/>	Verified?	Verified
<b>CP Doc Language</b>	Spanish		
<b>CP</b>	<a href="http://docs.camerfirma.com/publico/DocumentosWeb/politicas/PC_Chambres_of_Commerce_Root_1_0_1.pdf">http://docs.camerfirma.com/publico/DocumentosWeb/politicas/PC_Chambres_of_Commerce_Root_1_0_1.pdf</a>	Verified?	Verified
<b>CP Doc Language</b>	Spanish		
<b>CPS</b>	Spanish: <a href="https://servicios.camerfirma.com/publicacioncertificada2/ver/pdf/publicacion10122614">https://servicios.camerfirma.com/publicacioncertificada2/ver/pdf/publicacion10122614</a> English: <a href="http://docs.camerfirma.com/publico/DocumentosWeb/politicas/CPS_V_3_2_7_EN.pdf">http://docs.camerfirma.com/publico/DocumentosWeb/politicas/CPS_V_3_2_7_EN.pdf</a>	Verified?	Verified
<b>Other Relevant Documents</b>		Verified?	Verified
<b>Auditor Name</b>	AUREN	Verified?	Verified
<b>Auditor Website</b>	<a href="http://www.auren.com">http://www.auren.com</a>	Verified?	Verified
<b>Auditor Qualifications</b>		Verified?	Verified
<b>Standard Audit</b>	AUREN	Verified?	Verified
<b>Standard Audit Type</b>	WebTrust	Verified?	Verified
<b>Standard Audit Statement Date</b>	6/17/2015	Verified?	Verified
<b>BR Audit</b>	<a href="https://cert.webtrust.org/SealFile?seal=1925&amp;file=pdf">https://cert.webtrust.org/SealFile?seal=1925&amp;file=pdf</a>	Verified?	Verified
<b>BR Audit Type</b>	WebTrust	Verified?	Verified
<b>BR Audit Statement Date</b>	6/17/2015	Verified?	Verified
<b>EV Audit</b>	<a href="https://cert.webtrust.org/SealFile?seal=1926&amp;file=pdf">https://cert.webtrust.org/SealFile?seal=1926&amp;file=pdf</a>	Verified?	Verified
<b>EV Audit Type</b>	WebTrust	Verified?	Verified
<b>EV Audit Statement Date</b>	6/17/2015	Verified?	Verified
<b>BR Commitment to Comply</b>	Audit Report both in Spanish and English: (Included in W4CA report) <a href="https://cert.webtrust.org/SealFile?seal=1925&amp;file=pdf">https://cert.webtrust.org/SealFile?seal=1925&amp;file=pdf</a>	Verified?	Verified
<b>SSL Verification Procedures</b>	CPS Section 3.1.8.3.1: In order to validate an application for an OV (Organisation Validation) secure server certificate the following is checked: 1. The entity's existence by accessing public registers ( <a href="http://www.registradores.org">www.registradores.org</a> ; <a href="http://www.rmc.es">www.rmc.es</a> ), Camerdata ( <a href="http://www.camerdata.es">www.camerdata.es</a> ), Informa ( <a href="http://www.informa.es">www.informa.es</a> ) or the databases of the Spanish Tax Agency ( <a href="http://www.aeat.es">www.aeat.es</a> ). The entity is described in the Organisation field of the certificate and matches the domain owner. 2. The existence of the domain or ID address and the subscriber's right to use it. This is checked by accessing the WHOIS Internet domains. The use of a domain name or private IP addresses is allowed but is obsolete (and will be prohibited after October 2016, meaning that Camerfirma will stop issuing certificates of this kind from 1 November 2015. In any case, issued certificates of this type are revoked if their expiry date is later than October 2015. The customer will be notified of this before the certificate is issued.	Verified?	Verified
<b>EV SSL Verification Procedures</b>	URL (SSL) <a href="https://cev.camerfirma.com">https://cev.camerfirma.com</a>	Verified?	Verified
<b>Organization Verification Procedures</b>	CPS Section 3.1.8.3.1 (For OV Certificates): In order to validate an application for an OV (Organisation Validation) secure server certificate the following is checked: The entity's existence by accessing public registers ( <a href="http://www.registradores.org">www.registradores.org</a> ; <a href="http://www.rmc.es">www.rmc.es</a> ), Camerdata ( <a href="http://www.camerdata.es">www.camerdata.es</a> ), Informa ( <a href="http://www.informa.es">www.informa.es</a> ) or the databases of the Spanish Tax Agency ( <a href="http://www.aeat.es">www.aeat.es</a> ). The entity is described in the Organisation field of the certificate and matches the domain owner. The circumstances may arise in which a certificate is issued for this type of self-employed person, in this case, an entity does not exist, which is identified by means of an up-to-date receipt from the IAE tax in addition to their Identification Document. For entities outside of Spanish territory, the documentation that must be provided is the Official Registry of the corresponding country, duly apostilled, where the existence of the entity in the said country is indicated.	Verified?	Verified
<b>Email Address Verification Procedures</b>	CPS Section 3.1.8.2.1: The Signatories/Subscribers are required to appear in person when they are also the Applicant, or the Applicant's representative when this is a legal entity, and they as well as presenting the following: - National Identification Document. - Residency card. - Passport	Verified?	Verified
<b>Code Signing</b>	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	Verified?	Not

<b>Subscriber Verification Pro</b>			
<b>Multi-Factor Authentication</b>	Regarding CA certificates' controls: CPS Section 6.3.1 Multi-person control is required for activation of the CA's private key. Pursuant to this CPS, there is a policy of two of four people to activate keys.	<b>Verified?</b>	Verified
<b>Network Security</b>	The Webtrust Baseline requirements audit was conducted in accordance with the "WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2" which includes also the CA/B Forum Network and Certificate Systems Security Requirements – Version 1.0:  <a href="https://cert.webtrust.org/SealFile?seal=1925&amp;file=pdf">https://cert.webtrust.org/SealFile?seal=1925&amp;file=pdf</a>	<b>Verified?</b>	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates			
<b>Publicly Disclosed &amp; Audited subCAs</b>	URL with a list of publicly disclosed subordinate CA: <a href="http://www.camerfirma.com/area-de-usuario/jerarquia-politicas-ypracticas-de-certificacion/">http://www.camerfirma.com/area-de-usuario/jerarquia-politicas-ypracticas-de-certificacion/</a>	<b>Verified?</b>	Need Response From CA

## Root Case Record # 2

Root Case Information			
<b>Root Certificate Name</b>	GLOBAL CHAMBERSIGN ROOT - 2016	<b>Root Case No</b>	R00000117
<b>Request Status</b>	Initial Request Received	<b>Case Number</b>	00000080

Additional Root Case Information	
<b>Subject</b>	Include GLOBAL CHAMBERSIGN ROOT - 2016

Technical Information about Root Certificate			
<b>O From Issuer Field</b>	AC CAMERFIRMA S.A.	<b>Verified?</b>	Verified
<b>OU From Issuer Field</b>	GLOBAL CHAMBERSIGN ROOT - 2016	<b>Verified?</b>	Verified
<b>Certificate Summary</b>	There is a "Global Chambersign Root - 2008" root certificate currently included in NSS, which is SHA-1 4096-bit. This new root is SHA-256. This root will have internally-operated subordinateCAs that issue certificates for Spanish com	<b>Verified?</b>	Verified
<b>Root Certificate Download URL</b>	<a href="http://www.camerfirma.com/certs/globalchambersignroot-2016.crt">http://www.camerfirma.com/certs/globalchambersignroot-2016.crt</a>	<b>Verified?</b>	Verified
<b>Valid From</b>	2016 Apr 14	<b>Verified?</b>	Verified
<b>Valid To</b>	2040 Aug 04	<b>Verified?</b>	Verified
<b>Certificate Version</b>	3	<b>Verified?</b>	Verified
<b>Certificate Signature Algorithm</b>	SHA-256	<b>Verified?</b>	Verified
<b>Signing Key Parameters</b>	4096	<b>Verified?</b>	Verified
<b>Test Website URL (SSL) or Example Cert</b>	<a href="https://csev.camerfirma.com/">https://csev.camerfirma.com/</a>	<b>Verified?</b>	Verified
<b>CRL URL(s)</b>	<a href="http://crl.camerfirma.com/globalchambersignroot-2016.crl">http://crl.camerfirma.com/globalchambersignroot-2016.crl</a>	<b>Verified?</b>	Verified
<b>OCSP URL(s)</b>	<a href="http://ocsp.camerfirma.com/">http://ocsp.camerfirma.com/</a>	<b>Verified?</b>	Verified
<b>Trust Bits</b>	Email; Websites	<b>Verified?</b>	Verified
<b>SSL Validation Type</b>	OV; EV	<b>Verified?</b>	Verified
<b>EV Policy OID(s)</b>	1.3.6.1.4.1.17326.10.8.12.1.2	<b>Verified?</b>	Verified
<b>Root Stores Included In</b>	Microsoft	<b>Verified?</b>	Verified
<b>Mozilla Applied</b>	No	<b>Verified?</b>	Verified

**Constraints**

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

<b>Revocation Tested</b>	No Error	<b>Verified?</b>	Verified
<b>CA/Browser Forum Lint Test</b>	ERROR: CA certificates must set keyUsage extension as critical ERROR: Invalid country in countryName WARNING: CA certificates should not have a validity period greater than 25 years	<b>Verified?</b>	Need Response From CA
<b>Test Website Lint Test</b>	No Error	<b>Verified?</b>	Verified
<b>EV Tested</b>	// CN=CHAMBERS OF COMMERCE ROOT - 2016,O=AC CAMERFIRMA S.A.,OID.2.5.4.97=VATES-A82743287,serialNumber=A82743287,OU=CHAMBERS OF COMMERCE ROOT - 2016,OU=see current address at <a href="http://www.camerfirma.com/address.L=MADRID.ST=MADRID.C=ES">www.camerfirma.com/address.L=MADRID.ST=MADRID.C=ES</a> "1.3.6.1.4.1.17326.10.14.2.1.2", "Camerfirma EV OID", SEC_OID_UNKNOWN, { 0x04, 0xF1, 0xBE, 0xC3, 0x69, 0x51, 0xBC, 0x14, 0x54, 0xA9, 0x04, 0xCE, 0x32, 0x89, 0x0C, 0x5D, 0xA3, 0xCD, 0xE1, 0x35, 0x6B, 0x79, 0x00, 0xF6, 0xE6, 0x2D, 0xFA, 0x20, 0x41, 0xEB, 0xAD, 0x51 }, "MIIBDDELMaKGA1UEBhMCRVMxZzANBGNVBAgMBk1BRFJJRDEPMA0GA1UEBwwGTUFE" "UkIEMTowOAYDVQQLDDFzZWUgY3VycmVudCBhZGRyZXRzIGF0IHd3dy5jYW1lcmZp" "cm1hLmNvbS9hZGRyZXRzMSkwJwYDVQLDCBSEFNQkVSUyBPRiBBDT01NRVJDRSBS" "T09UIC0gMjAxNjESMBAGA1UEBRMJQTYyZzQzMjg3MRgwFgYDVQRhDA9WQVRFUy1B" "ODI3NDMyODcxZzAZBgNVBAoMEkFDIENBTUVSRkISTUEgUy5BLjEpMCCGA1UEAwwg" "Q0hBTUJFUjUgT0YgQ09NTUVSQ0UgUk9PVCAiIDlwMTY=", "NJotoYIGsrM=", Success!	<b>Verified?</b>	Verified

**Digital Fingerprint Information**

<b>SHA-1 Fingerprint</b>	4A:BD:EE:EC:95:0D:35:9C:89:AE:C7:52:A1:2C:5B:29:F6:D6:AA:0C	<b>Verified?</b>	Verified
<b>SHA-256 Fingerprint</b>	C1:D8:0C:E4:74:A5:11:28:B7:7E:79:4A:98:AA:2D:62:A0:22:5D:A3:F4:19:E5:C7:ED:73:DF:BF:66:0E:71:09	<b>Verified?</b>	Verified

**CA Hierarchy Information**

<b>CA Hierarchy</b>	CPS document:1.2.1.3 <a href="http://docs.camerfirma.com/publico/DocumentosWeb/politicas/CPS_V_3_2_7_EN.pdf">http://docs.camerfirma.com/publico/DocumentosWeb/politicas/CPS_V_3_2_7_EN.pdf</a>	<b>Verified?</b>	Verified
<b>Externally Operated SubCAs</b>	In-House subCAs	<b>Verified?</b>	Verified
<b>Cross Signing</b>	N/A	<b>Verified?</b>	Verified
<b>Technical Constraint on 3rd party Issuer</b>	Registration Authorities: CPS sections 1.5.4 and 2.1.2  URL with a list of publicly disclosed subordinate CA: <a href="http://www.camerfirma.com/area-de-usuario/jerarquia-politicas-y-practicas-de-certificacion/">http://www.camerfirma.com/area-de-usuario/jerarquia-politicas-y-practicas-de-certificacion/</a>	<b>Verified?</b>	Verified

**Verification Policies and Practices**

<b>Policy Documentation</b>	Language(s) that the documents are in: Spanish (The CPS are also translated into English)	<b>Verified?</b>	Verified
<b>CA Document Repository</b>	Spanish: <a href="http://www.camerfirma.com/area-de-usuario/jerarquia-politicas-y-practicas-de-certificacion/">http://www.camerfirma.com/area-de-usuario/jerarquia-politicas-y-practicas-de-certificacion/</a> English: <a href="http://www.camerfirma.com/en/area-de-usuario/jerarquia-politicas-y-practicas-de-certificacion/">http://www.camerfirma.com/en/area-de-usuario/jerarquia-politicas-y-practicas-de-certificacion/</a> CP: <input type="checkbox"/>	<b>Verified?</b>	Verified
<b>CP Doc Language</b>	Spanish		
<b>CP</b>	<a href="http://docs.camerfirma.com/publico/DocumentosWeb/politicas/PC_Chambres_of_Commerce_Root_1_0_1.pdf">http://docs.camerfirma.com/publico/DocumentosWeb/politicas/PC_Chambres_of_Commerce_Root_1_0_1.pdf</a>	<b>Verified?</b>	Verified
<b>CP Doc Language</b>	Spanish		
<b>CPS</b>	Spanish: <a href="https://servicios.camerfirma.com/publicacioncertificada2/ver/pdf/publicacion10122614">https://servicios.camerfirma.com/publicacioncertificada2/ver/pdf/publicacion10122614</a> English: <a href="http://docs.camerfirma.com/publico/DocumentosWeb/politicas/CPS_V_3_2_7_EN.pdf">http://docs.camerfirma.com/publico/DocumentosWeb/politicas/CPS_V_3_2_7_EN.pdf</a>	<b>Verified?</b>	Verified
<b>Other Relevant Documents</b>		<b>Verified?</b>	Verified
<b>Auditor Name</b>	AUREN	<b>Verified?</b>	Verified

<b>Auditor Website</b>	<a href="http://www.auren.com">http://www.auren.com</a>	Verified?	Verified
<b>Auditor Qualifications</b>	<a href="http://www.webtrust.org/licensed-webtrust-practitioners-international/item64419.aspx">http://www.webtrust.org/licensed-webtrust-practitioners-international/item64419.aspx</a>	Verified?	Verified
<b>Standard Audit</b>	<a href="https://bug986854.bmoattachments.org/attachment.cgi?id=8775118">https://bug986854.bmoattachments.org/attachment.cgi?id=8775118</a>	Verified?	Verified
<b>Standard Audit Type</b>	WebTrust	Verified?	Verified
<b>Standard Audit Statement Date</b>	6/17/2015	Verified?	Verified
<b>BR Audit</b>	<a href="https://cert.webtrust.org/SealFile?seal=1925&amp;file=pdf">https://cert.webtrust.org/SealFile?seal=1925&amp;file=pdf</a>	Verified?	Verified
<b>BR Audit Type</b>	WebTrust	Verified?	Verified
<b>BR Audit Statement Date</b>	6/17/2015	Verified?	Verified
<b>EV Audit</b>	<a href="https://cert.webtrust.org/SealFile?seal=1926&amp;file=pdf">https://cert.webtrust.org/SealFile?seal=1926&amp;file=pdf</a>	Verified?	Verified
<b>EV Audit Type</b>	WebTrust	Verified?	Verified
<b>EV Audit Statement Date</b>	6/17/2015	Verified?	Verified
<b>BR Commitment to Comply</b>	Audit Report both in Spanish and English: (Included in W4CA report) <a href="https://cert.webtrust.org/SealFile?seal=1925&amp;file=pdf">https://cert.webtrust.org/SealFile?seal=1925&amp;file=pdf</a>	Verified?	Verified
<b>SSL Verification Procedures</b>	CPS Section 3.1.8.3.1: In order to validate an application for an OV (Organisation Validation) secure server certificate the following is checked: 1. The entity's existence by accessing public registers ( <a href="http://www.registradores.org">www.registradores.org</a> ; <a href="http://www.rmc.es">www.rmc.es</a> ), Camerdata ( <a href="http://www.camerdata.es">www.camerdata.es</a> ), Informa ( <a href="http://www.informa.es">www.informa.es</a> ) or the databases of the Spanish Tax Agency ( <a href="http://www.aeat.es">www.aeat.es</a> ). The entity is described in the Organisation field of the certificate and matches the domain owner. 2. The existence of the domain or ID address and the subscriber's right to use it. This is checked by accessing the WHOIS Internet domains. The use of a domain name or private IP addresses is allowed but is obsolete (and will be prohibited after October 2016, meaning that Camerfirma will stop issuing certificates of this kind from 1 November 2015. In any case, issued certificates of this type are revoked if their expiry date is later than October 2015. The customer will be notified of this before the certificate is issued.	Verified?	Verified
<b>EV SSL Verification Procedures</b>	URL (SSL) <a href="https://cev.camerfirma.com">https://cev.camerfirma.com</a>	Verified?	Verified
<b>Organization Verification Procedures</b>	CPS Section 3.1.8.3.1 (For OV Certificates): In order to validate an application for an OV (Organisation Validation) secure server certificate the following is checked: The entity's existence by accessing public registers ( <a href="http://www.registradores.org">www.registradores.org</a> ; <a href="http://www.rmc.es">www.rmc.es</a> ), Camerdata ( <a href="http://www.camerdata.es">www.camerdata.es</a> ), Informa ( <a href="http://www.informa.es">www.informa.es</a> ) or the databases of the Spanish Tax Agency ( <a href="http://www.aeat.es">www.aeat.es</a> ). The entity is described in the Organisation field of the certificate and matches the domain owner. The circumstances may arise in which a certificate is issued for this type of self-employed person, in this case, an entity does not exist, which is identified by means of an up-to-date receipt from the IAE tax in addition to their Identification Document. For entities outside of Spanish territory, the documentation that must be provided is the Official Registry of the corresponding country, duly apostilled, where the existence of the entity in the said country is indicated.	Verified?	Verified
<b>Email Address Verification Procedures</b>	CPS Section 3.1.8.2.1: The Signatories/Subscribers are required to appear in person when they are also the Applicant, or the Applicant's representative when this is a legal entity, and they as well as presenting the following: - National Identification Document. - Residency card. - Passport	Verified?	Verified
<b>Code Signing Subscriber Verification Pro</b>	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	Verified?	Not Applicable
<b>Multi-Factor Authentication</b>	Regarding CA certificates' controls: CPS Section 6.3.1 Multi-person control is required for activation of the CA's private key. Pursuant to this CPS, there is a policy of two of four people to activate keys.	Verified?	Verified
<b>Network Security</b>	The Webtrust Baseline requirements audit was conducted in accordance with the "WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2" which includes also the CA/B Forum Network and Certificate Systems Security Requirements – Version 1.0:  <a href="https://cert.webtrust.org/SealFile?seal=1925&amp;file=pdf">https://cert.webtrust.org/SealFile?seal=1925&amp;file=pdf</a>	Verified?	Verified

### Link to Publicly Disclosed and Audited subordinate CA Certificates

<b>Publicly Disclosed &amp; Audited subCAs</b>	URL with a list of publicly disclosed subordinate CA: <a href="http://www.camerfirma.com/area-de-usuario/jerarquia-politicas-ypracticass-de-certificacion/">http://www.camerfirma.com/area-de-usuario/jerarquia-politicas-ypracticass-de-certificacion/</a>	Verified?	Need Response From CA
--	--	-----------	-----------------------

