salesforce.com

- Close Window
- Print This Page
- Expand All | Collapse All

R00000117

Information

Case No	00000080	**Owner**	Kathleen Wilson
Root Case No	R00000117	**Request Status**	Initial Request Received
Root Certificate Name	GLOBAL CHAMBERSIGN ROOT - 2016		
All Fields Verified?	No		

Fill this section when changing a currently included Root Certificate

Included CA Owner Name		**Included Certificate**	

Additional Root Case Information

Subject	Include GLOBAL CHAMBERSIGN ROOT - 2016	**Date/Time Opened**	5/23/2016 4:09 PM
		Date/Time Closed	

Technical Information about Root Certificate

O From Issuer Field	AC CAMERFIRMA S.A.	**O From Issuer Field (Verified?)**	Verified
OU From Issuer Field	GLOBAL CHAMBERSIGN ROOT - 2016	**OU from Issuer Field (Verified?)**	Verified
Certificate Summary	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	**Certificate Summary (Verified?)**	Verified
Root Certificate Download URL	http://www.camerfirma.com/certs/globalchambersignroot-2016.crt	**Root Certificate Download URL (Verified?**	Verified
SHA-1 Fingerprint	11:39:A4:9E:84:84:AA:F2:D9:0D:98:5E:C4:74:1A:65:DD:5D:94:E2	**SHA-1 Fingerprint (Verified?)**	Verified
SHA-256 Fingerprint	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	**SHA-256 Fingerprint (Verified?)**	Verified
Valid From	4/14/2016	**Valid From (Verified?)**	Verified
Valid To	8/4/2040	**Valid To (Verified?)**	Verified
Certificate Version	3	**Certificate Version (Verified?)**	Verified
Certificate Signature Algorithm	SHA-256	**Cert Signature Algorithm (Verified?)**	Verified
Signing Key Parameters	4096	**Signing Key Parameters (Verified?)**	Verified
Test Website URL (SSL) or Example Cert	https://csev.camerfirma.com/	**TestWebsiteURL(SSL)orExCert (Verified?)**	Verified
CRL URL(s)	http://crl.camerfirma.com/globalchambersignroot-2016.crl	**CRL URL (Verified?)**	Verified
OCSP URL(s)	http://ocsp.camerfirma.com/	**OCSP URL (Verified?)**	Verified
Trust Bits	Email; Websites	**Trust Bits (Verified?)**	Verified
SSL Validation Type	OV; EV	**SSL Validation Type (Verified?)**	Verified
EV Policy OID(s)	1.3.6.1.4.1.17326.10.8.12.1.2	**EV Policy OID(s) (Verified?)**	Verified
Root Stores Included In	Microsoft	**Root Stores Included In (Verified?)**	Verified
Mozilla Applied Constraints	No	**Mozilla Applied Constraints (Verified?)**	Verified

Test Results (When Requesting the Websites Trust Bit)

Revocation Tested	ERROR: - OCSP signing certificate does not contain the OCSP No Check extension - NextUpdate not set (RFC 5019, section 2.2.4)	**Revocation Tested (Verified?)**	Need Response From CA
CA/Browser Forum Lint Test	ERROR: - Invalid country in countryName WARNING: - CA certificates should not have a validity period greater than 25 years	**CA/Browser Forum Lint Test (Verified?)**	Need Response From CA
Test Website Lint Test	No Error	**Test Website Lint Test (Verified?)**	Verified
EV Tested	// 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 www.camerfirma.com/address,L=MADRID,ST=MADRID,C=ES "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 }, "MIIBDDELMAkGA1UEBhMCRVMxDzANBgNVBAgMBk1BRFJJRDEPMA0GA1UEBwwGTUFE" "UklEMTowOAYDVQQLDDFzZWUgY3VycmVudCBhZGRyZXNzIGF0IHd3dy5jYW1lcmZp" "cm1hLmNvbS9hZGRyZXNzMSkwJwYDVQQLDCBDSEFNQkVSUyBPRiBDT01NRVJDRSBS" "T09UIC0gMjAxNjESMBAGA1UEBRMJQTgyNzQzMjg3MRgwFgYDVQRhDA9WQVRFUy1B" "ODI3NDMyODcxGzAZBgNVBAoMEkFDIENBTUVSRklSTUEgUy5BLjEpMCcGA1UEAwwg" "Q0hBTUJFUlMgT0YgQ09NTUVSQ0UgUk9PVCAtIDIwMTY=", "NJotoYIGsrM=", Success!	**EV Tested (Verified?)**	Verified

CA Hierarchy Information

CA Hierarchy	CPS document:1.2.1.3 http://docs.camerfirma.com/publico/DocumentosWeb/politicas/CPS_V_3_2_7_EN.pdf	**CA Hierarchy (Verified?)**	Verified
Externally Operated SubCAs	In-House subCAs	**Externally Operated SubCAs (Verified?)**	Verified
Cross Signing	N/A	**Cross Signing (Verified?)**	Verified
Technical Constraint on 3rd party Issuer	Registration Authorities: CPS sections 1.5.4 and 2.1.2 URL with a list of publicly disclosed subordinate CA: http://www.camerfirma.com/area-de-usuario/jerarquia-politicas-ypracticas-de-certificacion/	**Tech Cons on 3rd party Iss (Verified?)**	Verified

Verification Policies and Practices

Policy Documentation	Language(s) that the documents are in: Spanish (The CPS are also translated into English)	**Policy Documentation (Verified?)**	Verified
CA Document Repository	Spanish: http://www.camerfirma.com/area-de-usuario/jerarquia-politicas-y-practicas-de-certificacion/ English: http://www.camerfirma.com/en/area-de-usuario/jerarquia-politicas-y-practicas-de-certificacion/ CP: □	**CA Document Repository (Verified?)**	Verified
CP Doc Language	Spanish		
CP	http://docs.camerfirma.com/publico/DocumentosWeb/politicas/PC_Chambers_of_Commerce_Root_1_0_1.pdf	**CP (Verified?)**	Verified
CPS Doc Language	English, Spanish		
CPS	Spanish: https://servicios.camerfirma.com/publicacioncertificada2/ver/pdf/publicacion10122614 English: http://docs.camerfirma.com/publico/DocumentosWeb/politicas/CPS_V_3_2_7_EN.pdf	**CPS (Verified?)**	Verified
Other Relevant Documents		**Other Relevant Documents (Verified?)**	Verified
Auditor Name	AUREN	**Auditor Name (Verified?)**	Verified
Auditor Website	http://www.auren.com	**Auditor Website (Verified?)**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitioners-international/item64419.aspx	**Auditor Qualifications (Verified?)**	Verified
Standard Audit	https://bug986854.bmoattachments.org/attachment.cgi?id=8775118	**Standard Audit (Verified?)**	Verified
Standard Audit Type	WebTrust	**Standard Audit Type (Verified?)**	Verified
Standard Audit Statement Date	6/17/2015	**Standard Audit Statement Dt (Verified?)**	Verified
BR Audit	NEED BR Audit Statement	**BR Audit (Verified?)**	Need Response From CA

BR Audit Type	WebTrust	**BR Audit Type (Verified?)**	Need Response From CA
BR Audit Statement Date	6/17/2015	**BR Audit Statement Date (Verified?)**	Need Response From CA
EV Audit	NEED EV Audit Statement	**EV Audit (Verified?)**	Need Response From CA
EV Audit Type	WebTrust	**EV Audit Type (Verified?)**	Need Response From CA
EV Audit Statement Date	6/17/2015	**EV Audit Statement Date (Verified?)**	Need Response From CA
BR Commitment to Comply	Audit Report both in Spanish and English: (Included in W4CA report) https://cert.webtrust.org/SealFile?seal=1925&file=pdf	**BR Commitment to Comply (Verified?)**	Verified
SSL Verification Procedures	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 (www.registradores.org; www.rmc.es), Camerdata (www.camerdata.es), Informa (www.informa.es) or the databases of the Spanish Tax Agency (www.aeat.es). 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.	**SSL Verification Procedures (Verified?)**	Verified
EV SSL Verification Procedures	URL (SSL) https://cev.camerfirma.com	**EV SSL Verification Proc (Verified?)**	Verified
Organization Verification Procedures	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 (www.registradores.org; www.rmc.es), Camerdata (www.camerdata.es), Informa (www.informa.es) or the databases of the Spanish Tax Agency (www.aeat.es). 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.	**Org Verification Procedure (Verified?)**	Verified
Email Address Verification Procedures	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	**Email Addr Verification Proc (Verified?)**	Verified
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Code Signing Subs Verif Proc (Verified?)**	Not Applicable
Multi-Factor Authentication	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.	**Multi-Factor Authentication (Verified?)**	Verified
Network Security	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: https://cert.webtrust.org/SealFile?seal=1925&file=pdf	**Network Security (Verified?)**	Verified

Software Release Information

NSS Release When First Included		**Firefox Release When First Included**	

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	URL with a list of publicly disclosed subordinate CA: http://www.camerfirma.com/area-de-usuario/jerarquia-politicas-ypracticas-de-certificacion/	**Publ Discl & Audited subCAs (Verified?)**	Need Response From CA

Internal Comments

Comments by Mozilla on Root Case

Public Comments

Comments

System Information

Created By	Kathleen Wilson, 5/23/2016 4:09 PM	Last Sync Date/Time	
Last Modified By	Aaron Wu, 8/29/2016 5:48 PM		

Root Case History

8/29/2016 5:47 PM

User	**Kathleen Wilson**
Action	**Changed BR Audit from AUREN to NEED BR Audit Statement.**

8/29/2016 8:15 AM

User	**Aaron Wu**
Action	**Changed Test Website Lint Test from NEED: Browse to https://cert-checker.allizom.org/ and enter the test website and click on the 'Browse' button to provide the PEM file for the root certificate. Then click on 'run certlint'. All errors must be resolved/fixed. to No Error. Changed CA/Browser Forum Lint Test from NEED: Browse to https://crt.sh/ and enter the SHA-1 Fingerprint for the root certificate. Then click on the 'Search' button. Then click on the 'Run cablint' link. All errors must be resolved/fixed. to ERROR: - Invalid country in countryName WARNING: - CA certificates should not have a validity period greater than 25 years. Changed Trust Bits. Changed Test Website URL (SSL) or Example Cert from NEED: - If requesting Websites trust bit: URL to a website whose SSL cert chains up to this root. Note that this can be a test site. - If requesting Email trust bit: attach an example cert to the bug. to https://csev.camerfirma.com/. Changed SSL Verification Procedures (Verified?) from Need Response From CA to Verified. Changed Revocation Tested. Changed Email Addr Verification Proc (Verified?) from Need Response From CA to Verified. Changed EV Tested. Changed EV SSL Verification Proc (Verified?) from Need Response From CA to Verified. Changed CA Document Repository to Spanish: http://www.camerfirma.com/area-de-usuario/jerarquia-politicas-y-practicas-de-certificacion/ English: http://www.camerfirma.com/en/area-de-usuario/jerarquia-politicas-y-practicas-de-certificacion/ CP: □. Changed BR Audit from NEED: If requesting Websites trust bit, then also need a BR audit as described here: https://wiki.mozilla.org/CA:BaselineRequirements to AUREN.**

8/29/2016 3:27 AM

User	**Aaron Wu**
Action	**Changed Certificate Summary to 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.**

5/23/2016 4:09 PM

User	**Kathleen Wilson**
Action	**Created.**