Print this page

Mozilla - CA Program

Case Information

Case Number	00000080	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Camerfirma	**Request Status**	Ready for Public Discussion

Additional Case Information

Subject	Include renewed Camerfirma Root Certs	**Case Reason**	New Owner/Root inclusion requested

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org/show_bug.cgi?id=986854

General information about CA's associated organization

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

Response to Mozilla's list of Recommended Practices

Recommended Practices	https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices	**Recommended Practices Statement**	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.
CA's Response to Recommended Practices	1) Publicly Available CP and CPS: Yes 2) CA Hierarchy: Yes 3) Audit Criteria: Yes 4) Document Handling of IDNs in CP/CPS: No 5) Revocation of Compromised Certificates: Yes (CPS section 4.8.2) 6) Verifying Domain Name Ownership: Yes 7) Verifying Email Address Control: Yes 8) Verifying Identity of Code Signing Certificate Subscriber: Not applicable. Mozilla is no longer enabling the Code Signing trust bit for root certificates. 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 10) Domain owned by a Natural Person: No SSL certificates have been issued to natural persons 11) OCSP: Confirm OCSP responds according to expected 12) Network Security Controls: Yes	**Verified?**	Verified

Response to Mozilla's list of Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices	**Problematic Practices Statement**	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	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).	**Verified?**	Verified

Root Case Record # 1

Root Case Information

Root Certificate Name	CHAMBERS OF COMMERCE ROOT - 2016	**Root Case No**	R00000116
Request Status	Ready for Public Discussion	**Case Number**	00000080

Certificate Data

Certificate Issuer Common Name	CHAMBERS OF COMMERCE ROOT - 2016
O From Issuer Field	AC CAMERFIRMA S.A.
OU From Issuer Field	see current address at www.camerfirma.com/address
Valid From	2016 Apr 14
Valid To	2040 Apr 08
Certificate Serial Number	349a2da18206b2b3
Subject	CN=CHAMBERS OF COMMERCE ROOT - 2016, OU=see current address at www.camerfirma.com/address, O=AC CAMERFIRMA S.A., C=ES
Signature Hash Algorithm	sha256WithRSAEncryption
Public Key Algorithm	RSA 4096 bits
SHA-1 Fingerprint	2D:E1:6A:56:77:BA:CA:39:E1:D6:8C:30:DC:B1:4A:BE:22:A6:17:9B
SHA-256 Fingerprint	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
Certificate Fingerprint	C9:0F:BC:26:64:48:5F:6D:31:75:05:5A:45:EF:10:D2:EB:6E:6C:7E:02:7D:F1:A1:D5:26:45:8C:42:F4:26:96
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	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.	**Verified?**	Verified

Root Certificate Download URL	http://www.camerfirma.com/certs/chambersofcommerceroot-2016.crt	**Verified?**	Verified
CRL URL(s)	http://crl.camerfirma.com/chambersofcommerceroot-2016.crl	**Verified?**	Verified
OCSP URL(s)	http://ocsp.camerfirma.com	**Verified?**	Verified
Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	OV; EV	**Verified?**	Verified
EV Policy OID(s)	2.23.140.1.1	**Verified?**	Verified
Root Stores Included In	Microsoft; Mozilla	**Verified?**	Verified
Mozilla Applied Constraints	No	**Verified?**	Verified

Test Websites or Example Cert

Test Website URL (SSL) or Example Cert	https://cev.camerfirma.com/ https://cov.camerfirma.com/	**Verified?**	Verified
Test Website - Expired	N/A		
Test Website - Revoked	N/A		

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

Revocation Tested	No Error	**Verified?**	Verified
CA/Browser Forum Lint Test	No Error	**Verified?**	Verified
Test Website Lint Test	No Error	**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" "ODI3NDMyODcxGzAZBgNVBAoMEkFDIENBTUVSRkISTUEgUy5BLjEpMCcGA1UEAwwg" "Q0hBTUJFUIMgT0YgQ09NTUVSQ0UgUk9PVCAtIDIwMTY=", "NJotoYIGsrM=", Success! https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	CPS document: 1.2.1.3 Hierarchy Chambers of Commerce Root http://docs.camerfirma.com/publico/DocumentosWeb/politicas/CPS_V_3_2_7_EN.pdf	**Verified?**	Verified
Externally Operated SubCAs	In-House subCAs	**Verified?**	Verified
Cross Signing	N/A	**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/	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Language(s) that the documents are in: Spanish (The CPS are also translated into English)	**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: ☐	**Verified?**	Verified
CP Doc Language	Spanish		
CP	http://docs.camerfirma.com/publico/DocumentosWeb/politicas/PC_Chambers_of_Commerce_Root_1_0_1.pdf	**Verified?**	Verified
CP Doc Language	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	**Verified?**	Verified
Other Relevant Documents		**Verified?**	Verified
Auditor Name	AUREN	**Verified?**	Verified
Auditor Website	http://www.auren.com	**Verified?**	Verified
Auditor Qualifications		**Verified?**	Verified
Standard Audit	https://bug986854.bmoattachments.org/attachment.cgi?id=8775118	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	6/17/2016	**Verified?**	Verified
BR Audit	https://bugzilla.mozilla.org/attachment.cgi?id=8800807	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	8/5/2016	**Verified?**	Verified
EV Audit	https://bugzilla.mozilla.org/attachment.cgi?id=8800811	**Verified?**	Verified
EV Audit Type	WebTrust	**Verified?**	Verified
EV Audit Statement Date	8/5/2016	**Verified?**	Verified
BR Commitment to Comply	Audit Report both in Spanish and English: (Included in W4CA report) https://cert.webtrust.org/SealFile?seal=1925&file=pdf	**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.	**Verified?**	Verified
EV SSL Verification Procedures	URL (SSL) https://cev.camerfirma.com	**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.	**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	**Verified?**	Verified
Code Signing Subscriber	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable

Verification Pro			
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.	**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	**Verified?**	Verified

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/	**Verified?**	Need Response From CA

Root Case Record # 2

Root Case Information

Root Certificate Name	Global Chambersign Root	**Root Case No**	R00000117
Request Status	Ready for Public Discussion	**Case Number**	00000080

Certificate Data

Certificate Issuer Common Name	Global Chambersign Root
O From Issuer Field	AC Camerfirma SA CIF A82743287
OU From Issuer Field	http://www.chambersign.org
Valid From	2003 Sep 30
Valid To	2037 Sep 30
Certificate Serial Number	00
Subject	CN=Global Chambersign Root, OU=http://www.chambersign.org, O=AC Camerfirma SA CIF A82743287, C=EU
Signature Hash Algorithm	sha1WithRSAEncryption
Public Key Algorithm	RSA 2048 bits
SHA-1 Fingerprint	33:9B:6B:14:50:24:9B:55:7A:01:87:72:84:D9:E0:2F:C3:D2:D8:E9
SHA-256 Fingerprint	EF:3C:B4:17:FC:8E:BF:6F:97:87:6C:9E:4E:CE:39:DE:1E:A5:FE:64:91:41:D1:02:8B:7D:11:C0:B2:29:8C:ED
Certificate Fingerprint	F3:3B:D6:DD:C7:57:6A:7A:C9:BB:A4:64:D7:42:5F:26:D5:8F:D2:C5:1A:3A:1F:89:87:8D:52:62:BD:D4:85:E0
Certificate Version	3

Technical Information about Root Certificate

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	**Verified?**	Verified
Root Certificate Download URL	http://www.camerfirma.com/certs/globalchambersignroot-2016.crt	**Verified?**	Verified
CRL URL(s)	http://crl.camerfirma.com/globalchambersignroot-2016.crl	**Verified?**	Verified
OCSP URL(s)	http://ocsp.camerfirma.com/	**Verified?**	Verified
Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	OV; EV	**Verified?**	Verified
EV Policy OID(s)	2.23.140.1.1	**Verified?**	Verified
Root Stores Included	Microsoft	**Verified?**	Verified

In			
Mozilla Applied Constraints	No	**Verified?**	Verified

Test Websites or Example Cert

Test Website URL (SSL) or Example Cert	https://csev.camerfirma.com/	**Verified?**	Verified
Test Website - Expired	N/A		
Test Website - Revoked	N/A		

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

Revocation Tested	No Error	**Verified?**	Verified
CA/Browser Forum Lint Test	No Error	**Verified?**	Verified
Test Website Lint Test	No Error	**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!	**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	**Verified?**	Verified
Externally Operated SubCAs	In-House subCAs	**Verified?**	Verified
Cross Signing	N/A	**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/	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Language(s) that the documents are in: Spanish (The CPS are also translated into English)	**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: □	**Verified?**	Verified
CP Doc Language	Spanish		
CP	http://docs.camerfirma.com/publico/DocumentosWeb/politicas/PC_Chambers_of_Commerce_Root_1_0_1.pdf	**Verified?**	Verified
CP Doc Language	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	**Verified?**	Verified

Other Relevant Documents		**Verified?**	Verified
Auditor Name	AUREN	**Verified?**	Verified
Auditor Website	http://www.auren.com	**Verified?**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitioners-international/item64419.aspx	**Verified?**	Verified
Standard Audit	https://bug986854.bmoattachments.org/attachment.cgi?id=8775118	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	6/17/2016	**Verified?**	Verified
BR Audit	https://bugzilla.mozilla.org/attachment.cgi?id=8800807	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	8/5/2016	**Verified?**	Verified
EV Audit	https://bugzilla.mozilla.org/attachment.cgi?id=8800811	**Verified?**	Verified
EV Audit Type	WebTrust	**Verified?**	Verified
EV Audit Statement Date	8/5/2016	**Verified?**	Verified
BR Commitment to Comply	Audit Report both in Spanish and English: (Included in W4CA report) https://cert.webtrust.org/SealFile?seal=1925&file=pdf	**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.	**Verified?**	Verified
EV SSL Verification Procedures	URL (SSL) https://cev.camerfirma.com	**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.	**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	**Verified?**	Verified
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**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.	**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	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	URL with a list of publicly disclosed subordinate CA:	**Verified?**	Need Response From CA

	http://www.camerfirma.com/area-de-usuario/jerarquia-politicas-ypracticas-de-certificacion/