Bugzilla ID: 986854
Bugzilla Summary: Add Renewed AC Camerfirma root certificate.

CAs wishing to have their certificates included in Mozilla products must

1) Comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/)
2) Supply all of the information listed in http://wiki.mozilla.org/CA:Information_checklist.
    a. Review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices
    b. Review the Potentially Problematic Practices at https://wiki.mozilla.org/CA:Problematic_Practices

General information about the CA's associated organization

CA Company Name	Camerfirma
Website URL (English version)	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.
Inclusion in other major browsers	Yes, IE
CA Primary Point of Contact (POC)	POC direct email: ramirom@camerfirma.com Email Alias: gestion_soporte@camerfirma.com CA Phone Number: 349 13 443743

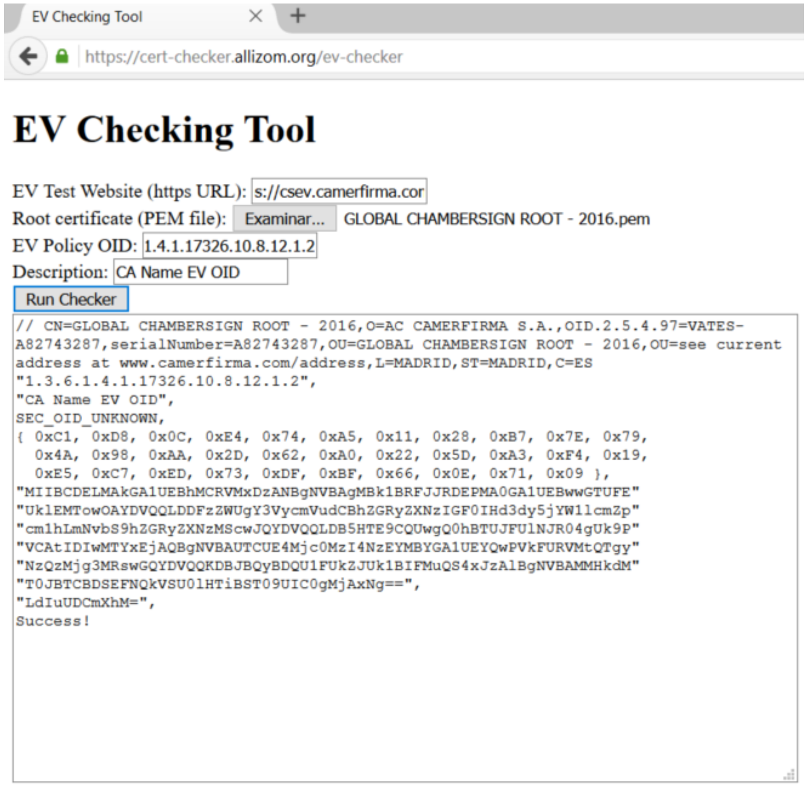
Technical Information about each root certificate

Certificate Name	Chambers of Commerce Root - 2016	Global Chambersign Root - 2016

Certificate Issuer Field	C=ES
	ST=MADRID
	L=MADRID
	OU=see current address at www.camerfirma.com/address
	OU=CHAMBERS OF COMMERCE ROOT - 2016
	serialNumber=A82743287
	2.5.4.97=VATES-A82743287
	O=AC CAMERFIRMA S.A.
	CN=CHAMBERS OF COMMERCE ROOT - 2016
		C=ES
		ST=MADRID
		L=MADRID
		OU=see current address at www.camerfirma.com/address
		OU=GLOBAL CHAMBERSIGN ROOT - 2016
		serialNumber=A82743287
		2.5.4.97=VATES-A82743287
		O=AC CAMERFIRMA S.A.
		CN=GLOBAL CHAMBERSIGN ROOT - 2016

Certificate Summary	There is a "Chambers of Commerce Root - 2008" root certificate currently included in NSS, which is SHA-1 4096-bit. This new root is	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

	SHA-256 4096-bit. This root will have internally-operated subordinate CAs that issue certificates for Spanish companies and representatives. Chambers of Commerce act as RAs	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.
Number of Included Roots	Can the “Chambers of Commerce Root” SHA-1 2048-bit root certificate be removed now? No SHA1 Fingerprint: 6E:3A:55:A4:19:0C:19:5C:93:84:3C:C0:DB:72:2E:31:30:61:F0:B1 Can the “Chambers of Commerce Root - 2008” SHA-1 4096-bit root certificate be removed now? No SHA1 Fingerprint: 78:6A:74:AC:76:AB:14:7F:9C:6A:30:50:BA:9E:A8:7E:FE:9A:CE:3C	Can the “Global Chambersign Root” SHA-1 2048-bit root certificate be removed now? No SHA1 Fingerprint: 33:9B:6B:14:50:24:9B:55:7A:01:87:72:84:D9:E0:2F:C3:D2:D8:E9 Can the “Global Chambersign Root - 2008” SHA-1 4096-bit root certificate be removed now? No SHA1 Fingerprint: 4A:BD:EE:EC:95:0D:35:9C:89:AE:C7:52:A1:2C:5B:29:F6:D6:AA:0C
Root Cert URL	http://www.camerfirma.com/certs/chambersofcommerceroot-2016.crt	http://www.camerfirma.com/certs/globalchambersignroot-2016.crt
SHA1 Fingerprint	2D:E1:6A:56:77:BA:CA:39:E1:D6:8C:30:DC:B1:4A:BE:22:A6:17:9B	11:39:A4:9E:84:84:AA:F2:D9:0D:98:5E:C4:74:1A:65:DD:5D:94:E2
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.
Valid from	14 apr 2016 7:35:48 gmt	14 apr 2016 7:50:06 gmt
Valid to	8 apr 2040 7:35:48 gmt	8 apr 2040 7:50:06 gmt
Certificate Version	3	3
Certificate Signature Algorithm	sha256WithRSAEncryption	sha256WithRSAEncryption
Signing key parameters	4.096	4.096
Test Website URL (SSL)	https://cev.camerfirma.com https://cov.camerfirma.com	https://csev.camerfirma.com https://csov.camerfirma.com
CRL URL	http://crl.camerfirma.com/chambersofcommerceroot-2016.crl	http://crl.camerfirma.com/globalchambersignroot-2016.crl
OCSP URL	http://ocsp.camerfirma.com	http://ocsp.camerfirma.com

Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing Timestamping	Websites (SSL/TLS) Email (S/MIME) Code Signing Timestamping
SSL Validation Type	OV and EV	OV and EV
EV Policy OID(s)	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	1.3.6.1.4.1.17326.10.8.12.1.2 1.3.6.1.4.1.17326.10.8.12.1.1 

EV Checking Tool

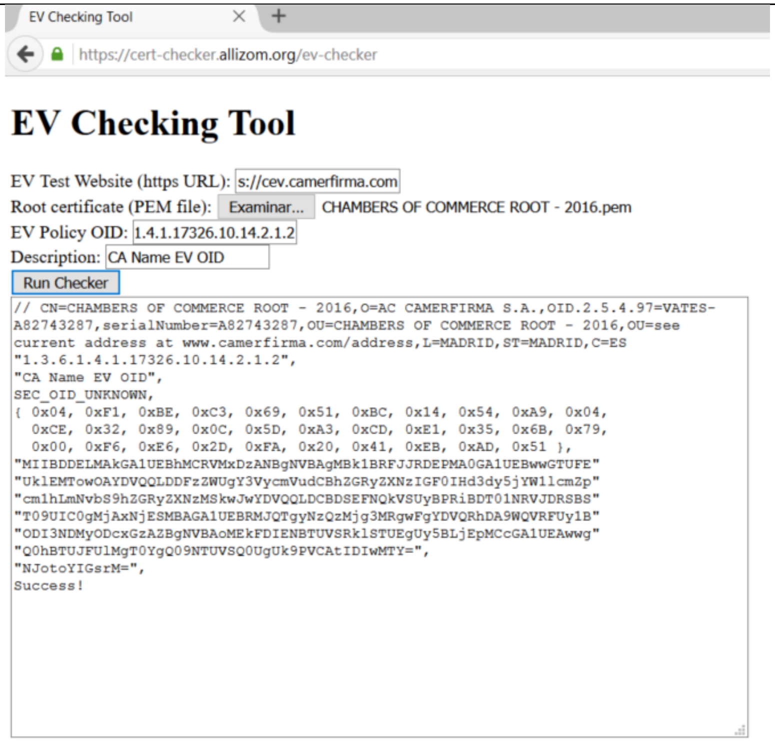
EV Test Website (https URL): s://csev.camerfirma.cor

Root certificate (PEM file): GLOBAL CHAMBERSIGN ROOT - 2016.pem

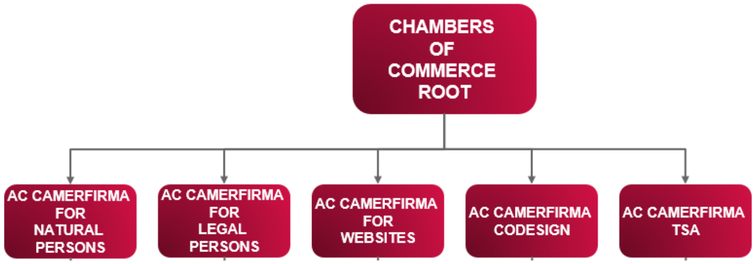
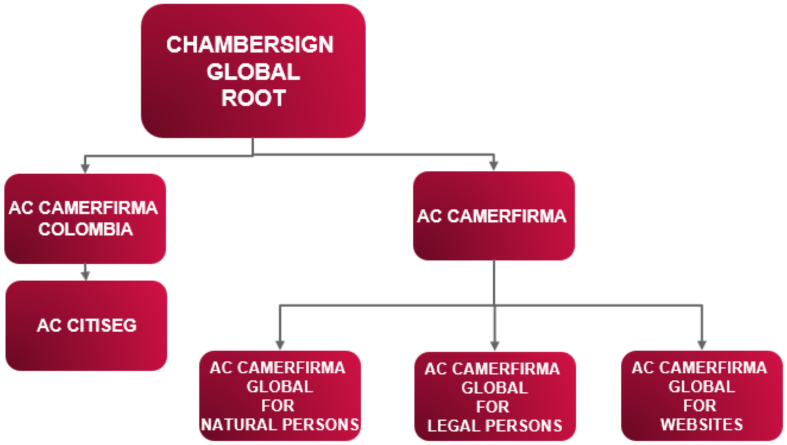
EV Policy OID: 1.4.1.17326.10.8.12.1.2

Description: CA Name EV OID

```
// CN=GLOBAL CHAMBERSIGN ROOT - 2016,O=AC CAMERFIRMA S.A.,OID.2.5.4.97=VATES-
A82743287,serialNumber=A82743287,OU=GLOBAL CHAMBERSIGN ROOT - 2016,OU=see current
address at www.camerfirma.com/address,L=MADRID,ST=MADRID,C=ES
"1.3.6.1.4.1.17326.10.8.12.1.2",
"CA Name EV OID",
SEC_OID_UNKNOWN,
{ 0xC1, 0xD8, 0x0C, 0xE4, 0x74, 0xA5, 0x11, 0x28, 0xB7, 0x7E, 0x79,
  0x4A, 0x98, 0xAA, 0x2D, 0x62, 0xA0, 0x22, 0x5D, 0xA3, 0xF4, 0x19,
  0xE5, 0xC7, 0xED, 0x73, 0xDF, 0xBF, 0x66, 0x0E, 0x71, 0x09 },
"MIIBCDELMAkGA1UEBhMCRVMxDzANBgNVBAgMBk1BRFJJRDEPMA0GA1UEBwwGTUFE"
"UklEMTowOAYDVQQLDDFzZWUgY3VycmVudCBhZGRyZXNzIGF0IHd3dy5jYW1lcmZp"
"cm1hLmNvbS9hZGRyZXNzMScwJQYDVQQLDB5HTE9CQUwgQ0hBTUJFUlNJR04gUk9P"
"VCAtIDIwMTYxEjAQBgNVBAUTCUE4Mjc0MzI4NzEYMBYGA1UEYQwPVkFURVMtQTgy"
"NzQzMjg3MRswGQYDVQQKDBJBQyBDQU1FUkZJUk1BIFMuQS4xJzAlBgNVBAMMHkdM"
"T0JBTCBDSEFNQkVSU0lHTiBST09UIC0gMjAxNg==",
"LdIuUDCmXhM=",
Success!
```

	 EV Checking Tool https://cert-checker.allizom.org/ev-checker EV Checking Tool EV Test Website (https URL): s://cev.camerfirma.com Root certificate (PEM file): Examinar... CHAMBERS OF COMMERCE ROOT - 2016.pem EV Policy OID: 1.4.1.17326.10.14.2.1.2 Description: CA Name EV OID Run Checker // 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", "CA Name 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!	
Non-sequential serial numbers and entropy in cert	All new end-entity certificates contains at least 20 bits of unpredictable random data in the serial number.	All new end-entity certificates contains at least 20 bits of unpredictable random data in the serial number.

CA Hierarchy information for each root certificate

CA Hierarchy	 CHAMBERS OF COMMERCE ROOT AC CAMERFIRMA FOR NATURAL PERSONS AC CAMERFIRMA FOR LEGAL PERSONS AC CAMERFIRMA FOR WEBSITES AC CAMERFIRMA CODESIGN AC CAMERFIRMA TSA	 CHAMBERSIGN GLOBAL ROOT AC CAMERFIRMA COLOMBIA AC CITISEG AC CAMERFIRMA AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS AC CAMERFIRMA GLOBAL FOR WEBSITES
Externally Operated SubCAs	In-House subCAs	- In-House subCAs
Cross Signing	N/A	N/A
Technical Constraints on Third-party Issuers	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-y-practicas-de-certificacion/	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-y-practicas-de-certificacion/

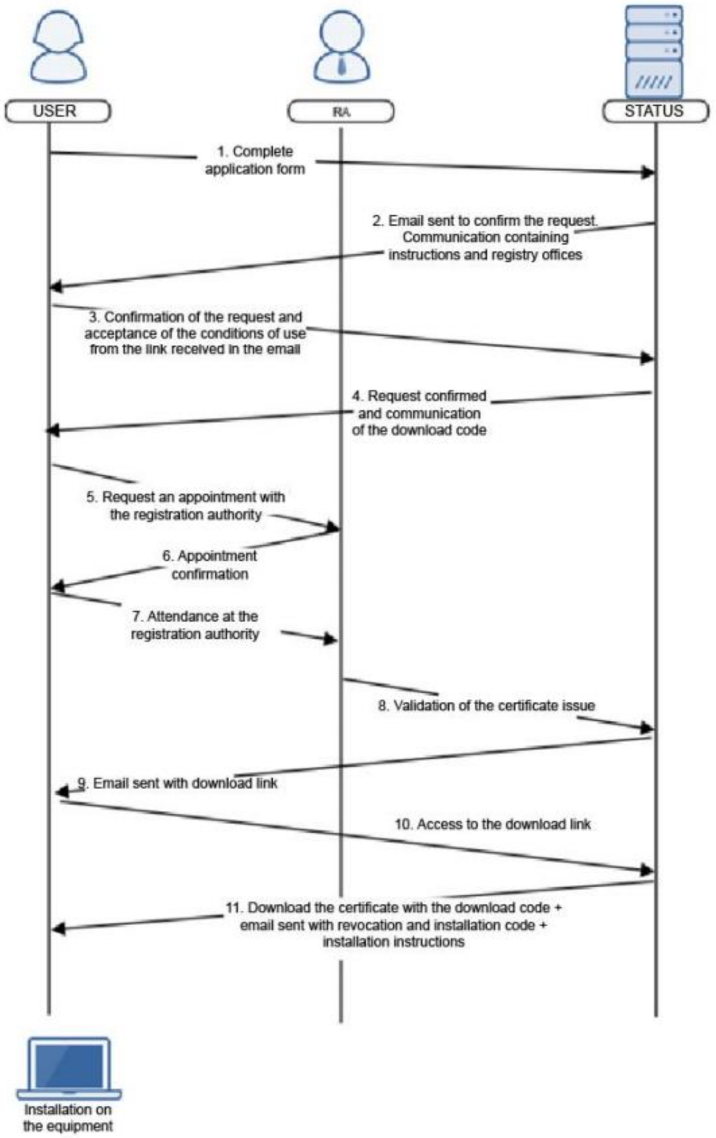
Verification Policies and Practices

Policy Documentation	Language(s) that the documents are in: Spanish (The CPS are also translated into English) 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: ● Chambersign Global ROOT hierarchy: http://docs.camerfirma.com/publico/DocumentosWeb/politicas/PC_Global_Chambersign_Root_1.0.pdf

	• Chambers of Commerce Root hierarchy: http://docs.camerfirma.com/publico/DocumentosWeb/politicas/PC_Chambers_of_Commerce_Root_1_0_1.pdf 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
Audits	Audit Type: WebTrust for CA Auditor: AUREN (http://www.auren.com/) Audit Report both in Spanish and English: https://cert.webtrust.org/SealFile?seal=1925&file=pdf (2015.06.17) Audit Type: WebTrust Baseline Requirements with Network Security Auditor: AUREN (http://www.auren.com/) Audit Report both in Spanish and English: (Included in W4CA report) https://cert.webtrust.org/SealFile?seal=1925&file=pdf (2015.06.17) Audit Type: WebTrust for EV Auditor: AUREN (http://www.auren.com/es-ES) Audit Report both in Spanish and English: https://cert.webtrust.org/SealFile?seal=1926&file=pdf (2015.06.17)
Baseline Requirements (SSL)	URL to BR audit statement: (Included in W4CA report) https://cert.webtrust.org/SealFile?seal=1925&file=pdf (2015.06.17) The document(s) and section number(s) where the "Commitment to Comply" with the CA/Browser Forum Baseline Requirements may be found, as per BR #8.3: CPS Section 1.2.1.3.1 and 1.2.1.3.4.
SSL Verification Procedures	If you are requesting to enable the Websites Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #3 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices 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. 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.

	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. Domain information is taken from the WHOIS service of the registrar of the domain for which the rules established in the corresponding ccTLD or gTLD shall be applied 3. The subscriber's control over the domain, checking that the information found in the WHOIS Internet service search matches the entity's information submitted in the application. It may occur that the domain is assigned in the registrar's database to a third parry responsible for its management. In such circumstances, in order for the last domain owner's details to appear in the certificate, the following is needed: a. An authorisation of this for issuing the certificate. b. Communication indicating these circumstances from the organisation or person that controls the domain record. The certificate is delivered via email to at least the administrative and technical supervisors who appear in the domain databases. The STATUS management application does not allow the validation of certificates without entering the administrative and technical contact details, which are automatically notified. In the certificates issued with a SAN extension (SubjectAltName). The aforementioned procedures must be executed for each of the domains included in the certificate. The certificate cannot be issued if any of them do not comply with the indicated requirements.
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: 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. 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. CPS Section 3.1.8.3.2 (For corporate seal certificates): The issuing of the corporate digital seal certificates is supported with documents in the following way: an enquiry into the existence of the company/entity is checked in the AEAT, Camerdata, Informa or public registry databases, in the same way as for the issuing of the aforementioned OV secure server certificates. The applicant's email address must come from an account with a domain related to the company or body that made the application.

Email Address Verification Procedures	If you are requesting to enable the Email Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #4 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices 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. All other communications are made by means of email. CPS Section 4.1 The user receives an e-mail, after confirmation of the application data, at the address associated with the certificate application, with a link to confirm the application and accept the conditions of use. CPS Section 4.3.1 Following there is a diagram of the certification via software process in order to clarify the process:

USER
RA
STATUS
1. Complete application form
2. Email sent to confirm the request. Communication containing instructions and registry offices
3. Confirmation of the request and acceptance of the conditions of use from the link received in the email
4. Request confirmed and communication of the download code
5. Request an appointment with the registration authority
6. Appointment confirmation
7. Attendance at the registration authority
8. Validation of the certificate issue
9. Email sent with download link
10. Access to the download link
11. Download the certificate with the download code + email sent with revocation and installation code + installation instructions
Installation on the equipment

Code Signing Subscriber Verification Procedures	If you are requesting to enable the Code Signing Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #5 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices CPS Section 3.1.8.3.3 For code signing certificates, the same checking system is used as for the issuing of OV secure server certificates. For signing code physical presence is required in a RA and an authorization of an enterprise representative is needed
Multi-factor Authentication	Confirm that multi-factor authentication is required for all accounts capable of directly causing certificate issuance. See # 6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices 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. Regarding RA's access controls: CPS Section 1.2.1: Camerfirma has developed a special certification authority for issuing operator certificates for entity registration. With this certificate an operator can oversee his/her own management tasks in accordance with his/her role on the Camerfirma STATUS® management platform.
Network Security	Confirm that you have performed the actions listed in #7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices 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: Audit Type: WebTrust Baeline Requirements with Network Security Auditor: AUREN (http://www.auren.com/) Audit Report both in Spanish and English: (Included in W4CA report) https://cert.webtrust.org/SealFile?seal=1925&file=pdf

Response to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_Practices)

Publicly Available CP and CPS	See "Verification Policies and Practices" section Spanish: http://www.camerfirma.com/area-de-usuario/jerarquia-politicas-y-practicas-de-certificacion/ English (only CPS): http://www.camerfirma.com/en/area-de-usuario/jerarquia-politicas-y-practicas-de-certificacion/

CA Hierarchy	See “CA Hierarchy information for each root certificate” section of this document.
Audit Criteria	See “Verification Policies and Practices” section, audits subsection of this document: Audit Type: WebTrust for CA Auditor: AUREN (http://www.auren.com/) Audit Report both in Spanish and English: https://cert.webtrust.org/SealFile?seal=1925&file=pdf (2015.06.17) Audit Type: WebTrust Baeline Requirements with Network Security Auditor: AUREN (http://www.auren.com/) Audit Report both in Spanish and English: (Included in W4CA report) https://cert.webtrust.org/SealFile?seal=1925&file=pdf (2015.06.17) Audit Type: WebTrust for EV Auditor: AUREN (http://www.auren.com/es-ES) Audit Report both in Spanish and English: https://cert.webtrust.org/SealFile?seal=1926&file=pdf (2015.06.17)
Document Handling of IDNs in CP/CPS	IDN not supported.
Revocation of Compromised Certificates	CPS section 4.8.2: A certificate is revoked where: • Any of the details contained in the certificate are amended. • Errors are detected in the data submitted in the certificate application or there are changes to the verified circumstances for the issue of the certificate • The security of the key or certificate belonging to the subscriber or certificate manager is compromised or suspected of being compromised. • Etc.
Verifying Domain Name Ownership	See “SSL Verification Procedures” subsection of this document.
Verifying Email Address Control	See “Email Address Verification Procedures” subsection of this document. Use challenge-response mechanism.
Verifying Identity of Code Signing Certificate Subscriber	See “Code Signing Subscriber Verification Procedures” subsection of this document. For code signing certificates, the same checking system is used as for the issuing of OV secure server certificates.
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. (Webtrust BR audit confirms it).
Domain owned by a Natural Person	No SSL certificates have been issued to natural persons. In this case we follow the recommended practices.

OCSP	Confirm OCSP responds according to expected.

Response to Mozilla's list of Potentially Problematic Practices (https://wiki.mozilla.org/CA:Problematic_Practices)

Long-lived DV certificates	SSL certs are OV. CP 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.
Wildcard DV SSL certificates	SSL certs are OV, so we only issue wildcard certificates to subscribers whose actual identity has been validated with organizational validation (OV).
Email Address Prefixes for DV Certs	SSL certs are OV and the email used for verification should be in WHOIS administration or technical contact.
Delegation of Domain / Email validation to third parties	The verifications can only be performed for RA. Each RA is internally audited by the CA auditors (See CPS section 2.2) "Of course, it is not Camerfirma's intention to burden the RAs with the entire weight of responsibility for any damages due to a breach of the duties delegated to the RAs. For this reason, the same as for the CAs, the RA is subject to a control system imposed by Camerfirma, not only by means of the file and safe-keeping procedure controls for the files received by the RA using audits to evaluate, among others, the resources used and the knowledge and control over the operational procedures used to provide the RA services."
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
Allowing external entities to operate subordinate CAs	
Distributing generated private keys in PKCS#12 files	No. AC Camerfirma only accept PKCS10 request for SSL certificates.
Certificates referencing hostnames or private IP addresses	We do not issue certificates referencing hostnames or private IP addresses
Issuing SSL Certificates for Internal Domains	We do not issue certificates for internal domains.
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.
CRL with critical CIDP Extension	CRL not including CIDP extension
Generic names for CAs	No generic names are used for root certificates.

Lack of Communication With End Users	Anyone can contact with Camerfirma via contact info in section 1.7 of the CPS.
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).