CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs)

INTRODUCTION
1) CA's Legal Name: AC Camerfirma S.A.

2)
[ROOT 1] CHAMBERS OF COMMERCE ROOT - 2016 (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)
[SUBCA 1.1] AC CAMERFIRMA FOR LEGAL PERSONS - 2016 (3A:80:66:26:6D:28:BD:28:CC:D0:F5:64:C8:FB:C1:21:9B:4F:FA:E4:03:E0:1E:50:39:D3:0F:24:00:F0:EB:09)
[SUBCA 1.2] AC CAMERFIRMA FOR NATURAL PERSONS - 2016 (EE:DD:45:7A:F1:35:3D:76:F4:8E:7C:61:23:F3:91:40:E5:F9:A0:69:CA:51:B4:3E:EA:86:15:C9:CE:C0:D4:BB)
[SUBCA 1.3] AC CAMERFIRMA FOR WEBSITES - 2016 (93:7D:7D:5D:0B:7F:B7:DB:03:93:99:BC:0B:67:0C:C2:03:C7:AB:4E:33:2F:AE:45:3C:C3:8E:C1:88:DD:EA:2B)
[SUBCA 1.4] AC CAMERFIRMA TSA - 2016 (BA:AE:2C:63:38:85:7D:50:20:0F:6F:73:DD:45:E6:5A:A2:D8:95:BE:D4:67:5B:6E:39:6B:72:22:E0:18:A9:B8)
[SUBCA 1.5] AC CAMERFIRMA CODESIGN - 2016 (49:08:F2:33:75:67:BE:50:5C:26:CC:01:A7:F0:7C:4B:80:21:32:A0:95:B2:BA:EE:EE:6D:E2:08:83:08:8A:56)

[ROOT 2] GLOBAL CHAMBERSIGN ROOT - 2016 (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)
[SUBCA 2.1] AC CAMERFIRMA - 2016 (37:1C:57:98:2C:F5:43:FB:F9:04:1E:DC:34:8A:2E:0A:CD:CD:E4:B6:EC:25:EC:24:2B:AC:84:F0:1D:AB:18:1C)
[SUBCA 2.1.1] AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016 (4D:20:C9:51:E1:34:89:3B:C5:90:1B:FA:F8:E2:40:A5:BE:7D:00:59:6D:D3:1C:40:42:92:52:F2:E0:4F:8B:46)
[SUBCA 2.1.2] AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016 (EF:41:1C:83:7A:C3:30:41:85:E5:39:13:FE:36:9B:F8:FF:65:98:C2:A5:2B:DB:1B:6E:2D:EA:B5:DC:C7:F0:6F)

3) BR version 1.4.4, with the exception of the Domain Validation section 3.2.2.4 for which we used BR version 1.4.1.

4) http://docs.camerfirma.com/publico/DocumentosWeb/politicas/CPS_V_3_2_7_EN.pdf

BR Section Number	List the specific documents and section numbers of those documents which meet the requirements of each BR section	Explain how the CA's listed documents meet the requirements of each BR section.
1.2.1. Revisions Note the Effective Date for each item in the table. Certificates created after each Effective Date are expected to be in compliance with the item. Make sure your CA is in compliance with each of these items. After careful consideration, indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.	Compliance for any SSL certificate issued by AC Camerfirma SA.	
1.2.2. Relevant Dates Note the Compliance date for eachitem in the table. Those are the dates by which your CP/CPS and practices are expected to be updated to comply with the item. Make sure your CA is in compliance with each of these items. After careful consideration, indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.	Compliance for any SSL certificate issued by AC Camerfirma SA.	
1.3.2. Registration Authorities Indicate whether your CA allows for Delegated Third Parties, or not. Indicate which sections of your CP/CPS specify such requirements, and how the CP/CPS meets the BR requirements for RAs.	CPS_V_3_2_7_EN.pdf 1.5.4 Registration Authority (RA)	RA Contract and RA Audits.
2.1. Repositories Provide the direct URLs to the CA's repositories	CPS_V_3_2_7_EN.pdf 4.8.10 Availability of online service to check revocation	CA provides an online service to check revocations via HTTP at: http://www.camerfirma.com/area-de-usuario/consulta-de-certificados/ Also by means of OCSP queries at: http://www.camerfirma.com/servicios/respondedor-ocsp/
2.2. Publication of information "The CA SHALL publicly give effect to these Requirements and represent that it will adhere to the latest published version." --> Copy the specific text that is used into the explanation in this row. (in English)	CPS_V_3_2_7_EN.pdf 1.2. General Overview. AC Camerfirma will add the version of EV and BR in a new version of the CPS.	This document specifies the Certification Practice Statement (hereinafter, CPS) that AC Camerfirma SA (hereinafter, Camerfirma) has established for issuing certificates and is based on the following standards specification: □ RCF 3647 – Internet X. 509 Public Key Infrastructure Certificate Policy, by IETF, □ RFC 3739 3039 IETF Internet X.509 Public Key Infrastructure:Qualified Certificates Profile. □ RFC 5280, RFC 3280: Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL). □ RFC 6960 Online Certificate Status Protocol – OCSP □ ETSI TS 101 456 V1.2.1 Policy requirements for certification authorities issuing qualified certificates □ ETSI TS 102 042 V1.1.1 Policy requirements for certification authorities issuing public key certificates □ ETSI TS 102 023 V1.2.1 Policy requirements for time-stamping authorities technically equivalent to RFC 3628 □ CA/Browser Forum Baseline Requirements for issuing and managing Publicly Trusted Certificates. □ CA/Browser Forum EV SSL Certificate Guidelines.

2.2. Publication of information "The CA SHALL host test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. At a minimum, the CA SHALL host separate Web pages using Subscriber Certificates that are (i) valid, (ii) revoked, and (iii) expired." --> List the URLs to the three test websites (valid, revoked, expired) for each root certificate under consideration. If you are requesting EV treatment, then the TLS cert for each test website must be EV.	we have these URL used for Microsoft acreditation with active certificates. We will arrange the other ones before july 2017. https://cov.camerfirma.com https://cev.camerfirma.com https://csov.camerfirma.com https://csev.camerfirma.com	
2.3. Time or frequency of publication Indicate your CA's policies/practices to ensure that the BRs are reviewed regularly, and that the CA's CP/CPS is updated annually.	CPS_V_3_2_7_EN.pdf 8.2. Procedures for specifying changes.	8.2.2.2 Notice system Any proposed changes to this policy are published immediately on Camerfirma's web site http://www.camerfirma.com/area-de-usuario/politicas-y-practicas-de-certificacion/ This document contains a section on changes and versions, specifying the changes that occurred since it was created and the dates of those changes. Changes made to this document are expressly communicated to those agencies and third party companies and organisations that issue certificates under this CPS.
2.4. Access controls on repositories Acknowledge that all Audit, CP, CPS documents required by Mozilla's CA Certificate Policy and the BRs will continue to be made publicly available.	CPS_V_3_2_7_EN.pdf 8.2.2.2 Notice system	previous point
3.2.2.1 Identity If the Subject Identity Information in certificates is to include the name or address of an organization, indicate how your CP/CPS meets the requirements in this section of the BRs.	CPS_V_3_2_7_EN.pdf 3.1. Initial registration	3.1.8.2.1 Identification of the Applicant. 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. 3.1.8.2.2 Identification of the Entity. Prior to the issuing and delivering a certificate for an organisation, the information must be authenticated with regards to the formation and legal nature of the entity. The RA requests the required documentation depending on the type of entity in order to identify it. This information is published in the RA's operating manuals and on Camerfirma's web site. Documentation proving that the public administration, public body or public entity exists is not required, because the said identity forms part of corporate scope of the General State Administration or other State Public Administrations. The documentation necessary to issue a certificate is published at: http://www.camerfirma.com/index/buscador-documentos.php 3.1.8.2.3 Identification of the relationship. For the Special Power of Attorney Certificate and Power of Representation Certificate, the notary deeds must be submitted to prove the Signatory/Subscriber's powers of representation in relation to the entity. A certificate issued by the public register at least 10 days previously is submitted. The RA can also check the status and level of the applicant's powers of representation online.
3.2.2.2 DBA/Tradename If the Subject Identity Information in certificates is to include a DBA or tradename, indicate how your CP/CPS meets the requirements in this section of the BRs.	CPS_V_3_2_7_EN.pdf 3.1.8.2.2 Identification of the Entity. 3.1.6 Recognition, authentication and function of registered trademarks 3.1.8.2.3 Identification of the relationship.	3.1.6 Recognition, authentication and function of registered trademarks Camerfirma does not assume any obligations regarding the issue of certificates in relation to the use of a trademark. Camerfirma does not purposefully allow the use of a name for which the Signatory/Subscriber does not own the right to use. Nevertheless, Camerfirma is not obliged to search for proof of ownership of trademarks for issuing certificates. 3.1.8.2.2 Identification of the Entity. Prior to the issuing and delivering a certificate for an organisation, the information must be authenticated with regards to the formation and legal nature of the entity. The RA requests the required documentation depending on the type of entity in order to identify it. This information is published in the RA's operating manuals and on Camerfirma's web site. Documentation proving that the public administration, public body or public entity exists is not required, because the said identity forms part of corporate scope of the General State Administration or other State Public Administrations. The documentation necessary to issue a certificate is published at: http://www.camerfirma.com/index/buscador-documentos.php 3.1.8.2.3 Identification of the relationship. For the Special Power of Attorney Certificate and Power of Representation Certificate, the notary deeds must be submitted to prove the Signatory/Subscriber's powers of representation in relation to the entity. A certificate issued by the public register at least 10 days previously is submitted. The RA can also check the status and level of the applicant's powers of representation online.
3.2.2.3 Verification of Country If the subject:countryName field is present in certificates, indicate how your CP/CPS meets the requirements in this section of the BRs.	3.1.8.2.2 Identification of the Entity.	RA Operator check the Organization documentation that is linked with the country name.

3.2.2.4 Validation of Domain Authorization or Control Indicate which of the methods of domain validation your CA uses, and where this is described in your CP/CPS. The CA's CP/CPS must clearly describe the acceptable methods of domain validation. It is *not* sufficient for the CP/CPS to merely reference the BRs. Enough information must be directly provided in the CP/CPS for the reader to be able to understand how the CA performs domain validation.	3.1.8.3.5 In EV secure server certificates. 3.1.8.3.1 For OV (Organisation Validation) secure server certificates.	AC Camerfrima send a email to the administrative contact and the technical contact (webmaster, admin..etc) . In the email a ramdom code is included. Contacts must go to a links and type this ramdom code.
3.2.2.4.1 Validating the Applicant as a Domain Contact If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	NO	
3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	YES	
3.2.2.4.3 Phone Contact with Domain Contact If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	NO	
3.2.2.4.4 Constructed Email to Domain Contact If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	YES	
3.2.2.4.5 Domain Authorization Document If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	NO	
3.2.2.4.6 Agreed-Upon Change to Website If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	NO	
3.2.2.4.7 DNS Change If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	NO	
3.2.2.4.8 IP Address If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	NO	
3.2.2.4.9 Test Certificate If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	NO	
3.2.2.4.10. TLS Using a Random Number If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	NO	
3.2.2.5 Authentication for an IP Address If your CA allows IP Addresss to be listed in certificates, indicate how your CA meets the requirements in this section of the BRs.	CPS_V_3_2_7_EN.pdf 3.1.8.3.1 For OV (Organisation Validation) secure server certificates.	AC Camerfirma do not issue certificates for IP addesses

3.2.2.6 Wildcard Domain Validation If your CA allows certificates with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, then indicate how your CA meets the requirements in this seciton of the BRs.	CPS_V_3_2_7_EN.pdf 3.1.8.3.1 For OV (Organisation Validation) secure server certificates. 3.1.8.3.5 In EV secure server certificates.	AC Camerfirma validate the full control of the organization over the second level domain
3.2.2.7 Data Source Accuracy Indicate how your CA meets the requirements in this section of the BRs.	CPS_V_3_2_7_EN.pdf 3.1. Initial registration	AC Camerfirma validate that all documentas and data received is up todate.
3.2.3. Authentication of Individual Identity	CPS_V_3_2_7_EN.pdf 3.1.8.2.1 Identification of the Applicant.	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.
3.2.5. Validation of Authority	CPS_V_3_2_7_EN.pdf 3.1.8.2.3 Identification of the relationship.	3.1.8.2.3 Identification of the relationship. For the Special Power of Attorney Certificate and Power of Representation Certificate, the notary deeds must be submitted to prove the Signatory/Subscriber's powers of representation in relation to the entity. A certificate issued by the public register at least 10 days previously is submitted. The RA can also check the status and level of the applicant's powers of representation online. In the Special Powers of Representation Certificates, the different powers are described in a table of sections, which are included in the certificate in two ways: one, placing the sections of the powers of representation in the TITLE field, and two, by means of a link in the USER NOTICE that forwards the deeds that have been scanned and signed by the RA operator. The list of powers of attorney can be found at: https://www.camerfirma.com/apoderado/poderes.php.
3.2.6. Criteria for Interoperation or Certification Disclose all cross-certificates in the CA hierarchies under evaluation.	CPS_V_3_2_7_EN.pdf 4.2. Cross certification application.	AC Camerfirma do not issue cross-certification certificates
4.1.1. Who Can Submit a Certificate Application Indicate how your CA identifies suspicious certificate requests.		AC Camerfirma AR Operators have an access to a list of rejected and high risk certificates to be checked before validates a request.
4.1.2. Enrollment Process and Responsibilities	CPS_V_3_2_7_EN.pdf 3.1. Initial registration	
4.2. Certificate application processing		
4.2.1. Performing Identification and Authentication Functions Indicate how your CA identifies high risk certificate requests.		AC Camerfirma AR Operators have an access to a list of rejected and high risk certificates to be checked before validates a request.

4.2.2. Approval or Rejection of Certificate Applications	CPS_V_3_2_7_EN.pdf 3.1.8.3.1 For OV (Organisation Validation) secure server certificates. 3.1.8.3.5 In EV secure server certificates.	3.1.8.3.1 For OV (Organisation Validation) secure server 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. 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. 3.1.8.3.5 In EV secure server certificates. For “extended validation” Secure Server Certificates (EV) that follow the “CA/Browser Forum Guidelines for Issuance and Management of extended validation certificates”, the same procedures apply as for a Recognised contractual relationship certificate, i.e.: 1. The Signatories/Subscribers, or an Applicant's representative if it is an entity, must introduce themselves in person and present an identity document or passport. In the event of entities outside of the Spanish territory, the passport of specific, duly apostilled document attesting to the country must be presented. 2. The RA requests the required documentation depending on the type of entity in order to identify it. The entity's business activity must be proven. This is checked by accessing the commercial registry or other business activity registers. In the event of entities outside of the 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 appears. 3. Submission of authorisation signed by an entity's representative, who acts as the Applicant. In the event of entities outside of the Spanish territory, the documentary accreditation for the representation powers of the person signing the authorisation must be provided, duly apostilled, in order to check the authenticity of the documentation provided. For these certificates, the RA must also check: 1. The entity's existence: By accessing public registrars (www.registradores.org; www.rmc.es), (www.registradores.org; www.rmc.es), Camerdata (www.camerdata.es), Informa (www.informa.es) or the databases if the Spanish Tax Agency (www.aeat.es). If the RA operators require further information on the organisation than appears on the certificate, they can access a corporate risk management database Camerfirma SA https://www.camerfirma.com. This database provides commercial registry information on companies and their representatives, including risk information. In the event of entities outside of the 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 appears. - It must be checked that the submitted data or documents are not older than one year. - That the organisation has legally existed for the minimum of one year. - Certificates cannot be issued for eradicated companies in countries where there is a government ban on doing business. 2. The existence of the domain and the subscriber's right to use it is checked by accessing the WHOIS domain databases: - http://www.internic.net/whois.html - http://www.networksolutions.com - http://en.gandi.net - http://www.interdomain.es - https://www.nic.es/ (.es) - http://www.eurid.eu/ (.eu) - http://www.nic.coop/whoissearch.aspx (.coop) - http://www.nominalia.com/ - http://www.arsys.es/ 3. That the entity has control over the Internet domain for which the certificate has been issued. In other words, the entity described in the internet domain database access service is clearly identified and matches the entity that the certificate applicant is representing. The certificate issue guidelines require that a distinction be made between different types of organisations (private, government, business). In these cases, the applicant specifies the type of entity to which he/she belongs on the application form. The registration authority checks the information is accurate. The certificate includes this information as defined in the reference certification policies. In the certificates issued with the SAN extension (Subject Alternative Name). 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.
4.3.1. CA Actions during Certificate Issuance	CPS_V_3_2_7_EN.pdf 4.1.3 Final entity certificate application in HSM, TSU and SubCA.	
4.9.1.1 Reasons for Revoking a Subscriber Certificate Reasons for revoking certificates must be listed in the CA's CP/CPS.	CPS_V_3_2_7_EN.pdf 4.8.2 Causes for revocation and documentary proof	
4.9.1.2 Reasons for Revoking a Subordinate CA Certificate		AC Camerfirma SA could at any moment to revoke any SUBCA under its hierarchies, because security, political or contractual reasons in a discretionary maner.
4.9.2. Who Can Request Revocation	CPS_V_3_2_7_EN.pdf 4.8.3 Who can request revocation?	

4.9.3. Procedure for Revocation Request	CPS_V_3_2_7_EN.pdf 4.8.4 Revocation request procedure.	
4.9.5. Time within which CA Must Process the Revocation Request	CPS_V_3_2_7_EN.pdf 4.8.5 Revocation period	The revocation period, from the moment Camerfirma or an RA has reliable knowledge of a certificate revocation, happens immediately, and is included in the next CRL issued as well as in the database of the management platform, which supplies the OCSP respondent.
4.9.7. CRL Issuance Frequency	CPS_V_3_2_7_EN.pdf 4.8.8 CRL issue frequency	
4.9.9. On-line Revocation/Status Checking Availability	CPS_V_3_2_7_EN.pdf 4.8.10 Availability of online service to check revocation	
4.9.10. On-line Revocation Checking Requirements Indicate how your CA meets all of the requirements listed in this section, including support of GET, update frequency, preventing errounious return of "good" status.	CPS_V_3_2_7_EN.pdf 4.8.5 Revocation period	AC Camerfirma OCSP services support GET method at this moment.
4.9.11. Other Forms of Revocation Advertisements Available Indicate if your CA supports OCSP stapling.	N/A	
4.10.1. Operational Characteristics	CPS_V_3_2_7_EN.pdf 4.8.1 Preliminary clarifications	AC Camerfirma keeps, in its OCSP service, information of a revoked certificate beyond its validity period.
4.10.2. Service Availability	CPS_V_3_2_7_EN.pdf 4.8.10 Availability of online service to check revocation	The OCSP service is based on CRLs issued by the various certification authorities (CAs) or by access to the database of the platform (EE). The technical access data and the OCSP response validation certificates are published on the Camerfirma website http://www.camerfirma.com/servicios/respondedor-ocsp/ These services are available 24 hours a day, seven days a week, 365 days a year. Camerfirma will make every effort to ensure that the service is not down for more than 24 hours. This service is critical for Camerfirma's activities and is therefore covered in detail in the contingency and business continuity plans.
5. MANAGEMENT, OPERATIONAL, and Physical CONTROLS	CPS_V_3_2_7_EN.pdf 5. Physical, Procedural and Personnel Security Controls	Camerfirma is subject to the annual validations established by the UNE-ISO/IEC 27001:2007 standard, which regulates the establishment of suitable processes to ensure proper security management in information systems.
5.2.2. Number of Individuals Required per Task	CPS_V_3_2_7_EN.pdf 5.2.2 Number of people required per task	Camerfirma guarantees that at least two people will carry out the tasks described in the Certification Policies, Mainly handling the Root CA and intermediate CA key storage device.
5.3.1. Qualifications, Experience, and Clearance Requirements	CPS_V_3_2_7_EN.pdf 5.3.1 Background, qualifications, experience and accreditation requirements	All personnel undertaking tasks classified as duties of trust must have worked in the production centre for at least one year and have a permanent employment contract. All personnel are qualified and have been suitably trained in the procedures to which they have been assigned. The personnel working in positions of trust are not found to have personal interests that come into conflict with the performance of the role that they are appointed. Camerfirma ensures that registration personnel or RA Administrators are trustworthy and belong to a Chamber of Commerce or the body delegated to undertake registration work. RA Administrators must have taken a training course for application validation duties. In general, Camerfirma removes an employee's trust roles if it discovers that the person has committed any criminal act that could affect the performance of his/her duties. Camerfirma will not assign a trusted or management role to a person who is not suitable for the position, especially if he/she has been convicted for theft or if there is any doubt about their suitability for the position. For this reason, an investigation is previously carried out, to the extent that applicable legislation allows it, in relation to the following aspects: • Studies, including alleged qualifications. • Previous work experience, up to five years, including professional references and checking that they did actually perform the alleged role. • Delinquency
5.3.3. Training Requirements and Procedures	CPS_V_3_2_7_EN.pdf 5.3.3 Training requirements	Personnel undertaking duties of trust must have been trained pursuant to the Certification Policies. There is a training plan that is part of the UNE-ISO/IEC 27001:2007 controls. Registration operators who validate EV secure server certificates receive specific training pursuant to the special regulations on the issue of these certificates. The training includes the following content: • Security principles and mechanisms of the public hierarchy of certification. • Hardware versions and applications in use. • Tasks that the person must undertake. • Management and processing of security incidents and obligations. • Business continuity and emergency procedures. • Management and security procedure in relation to the management of personal information.
5.3.4. Retraining Frequency and Requirements	CPS_V_3_2_7_EN.pdf 5.3.4 Information updating requirements and frequency	Camerfirma undertakes the required updating procedures to ensure certification duties are undertaken correctly, especially when they are modified substantially.
5.3.7. Independent Contractor Controls	CPS_V_3_2_7_EN.pdf 5.3.1 Background, qualifications, experience and accreditation requirements	This paragraph cover third party personnal duties.
5.4.1. Types of Events Recorded	CPS_V_3_2_7_EN.pdf 4.10.1 Type of recorded files.	
5.4.3. Retention Period for Audit Logs	CPS_V_3_2_7_EN.pdf 4.10.2 File storage period	
5.4.8. Vulnerability Assessments	CPS_V_3_2_7_EN.pdf 2.7. Audits.	AC Camerfirma undertake 3 Vulnerability test in an annual base.
5.5.2. Retention Period for Archive	CPS_V_3_2_7_EN.pdf 4.10.2 File storage period	The certificates, contracts with the Signatories/Subscribers and any information related to the identification and authentication of the Signatory/Subscriber are kept for at least 15 years.

5.7.1. Incident and Compromise Handling Procedures	CPS_V_3_2_7_EN.pdf 4.12. Retrieval in the event of compromised key security or natural disaster	Camerfirma is subject to the annual validations established by the UNE-ISO/IEC 27001:2007 standard, which regulates the establishment of suitable processes to ensure proper security management in information systems. UNE-ISO/IEC 27001:2007 require a Risk Management Assessment.
6.1.1. Key Pair Generation	CPS_V_3_2_7_EN.pdf 6.1. Key pair creation and installation	The systems used by Camerfirma are nCipher. These devices house root keys and are certified Level 3 FIPS 140-2. The root keys are created and managed in a offline system in a cryptographic room. Reference document CONF-00-2012-02-CA creation script root 2008 SubCA keys are created in HSM systems, where they are housed for their corresponding use. The certificate issued by the root key is created in a secure cryptographic room.
6.1.2. Private Key Delivery to Subscriber	CPS_V_3_2_7_EN.pdf 6.1.2 Delivering the public key to the certificate issuer	The public key is given to Camerfirma to create the certificate when the circuit requires in a standard format, preferably self-signed PKCS#10 or X509 format.
6.1.5. Key Sizes	CPS_V_3_2_7_EN.pdf 6.1.4 Size and validity of issuer's keys	
6.1.6. Public Key Parameters Generation and Quality Checking	CPS_V_3_2_7_EN.pdf 6.1.6 Public key creation parameters.	The public key for the Root CA and Subordinate CA and for subscriber certificates is encrypted pursuant to RFC 3280 and PKCS#1. The algorithm for creating keys is the RSA.
6.1.7. Key Usage Purposes	CPS_V_3_2_7_EN.pdf 6.1.9 Purpose of key use	The keys are only used for the purposes indicated in the section "Purpose of key use" of the certification policies of each one of the certificates issued. The CA makes every possible effort that is in within their scope to confirm that the CA signature keys are only used for certificate creation purposes and for the signing of CRLs. Despite the fact that the encryption of information is technically possible with the certificates, Camerfirma shall not be held responsible for the damages caused due to the holder's loss of control of the private key needed to decipher the information, except in the certificate exclusively issued for this use. For certificates that are not exclusively for encryption, Camerfirma does not copy or store private keys associated with them.
6.2. Private Key Protection and Cryptographic Module Engineering Controls	CPS_V_3_2_7_EN.pdf 6.2. Protecting the private key	6.2. Protecting the private key The CA's private key The Root signature private key and the CAs are kept in an nCipher cryptographic device. This device complies with the specifications FIPS 140-2 level two and level three. An Eracom device pursuant to certificate FIPS 140-1 level three is used for OCSP and TSA authorities. When the CA private key is outside the device it is kept encrypted. A backup is made of the CA private key which is stored and only retrieved by authorised personnel in accordance with the roles of trust, using at least dual control on a secure physical device. The CA private key backups are stored securely. This procedure is described in detail in the Camerfirma security policies. The external SubCA keys are kept in devices that comply with at least FIPS 140-1 level 3. The subscriber's private key The subscriber's private key can be stored in a software or hardware device. When it is stored in software format, Camerfirma provides the configuration instructions for secure use in recognised applications. As regards cryptographic devices with certificates for advanced electronic signing, suitable as secure signature creation devices, these comply with security level CC EAL4+ and support the PKCS#11 and CSP standards. Camerfirma uses the cryptographic means allowed in its registration application and which guarantee the creation of recognised electronic signatures. Information on the type of key creation and safekeeping is included in the digital certificate itself, allowing the Trusting Third Party to act accordingly. Notes on the centralised key management system: If a centralised key management system is implemented, a storage device is used for the user keys, which must comply with at least FIPS-140-2 level 3. The key is activated remotely by means of a personal and secret key sent to the certificate holder or the person responsible for the keys from the management platform, guaranteeing the unique control of the private key on their behalf.
6.2.5. Private Key Archival	CPS_V_3_2_7_EN.pdf 6.3.3 Private key backup	Camerfirma makes backups of CA private keys to allow their retrieval in the event of natural disaster, loss or damage. At least two people are required to create the copy and retrieve it. These retrieval files are stored in fireproof cabinets and in an external custody centre. The subscriber's keys created on software can be stored for retrieval in the event of a contingency in an external storage device separately from the installation key, as specified in the software key installation manual. The subscriber's keys created on hardware cannot be copied because they cannot be taken out of the cryptographic device. Camerfirma keeps minutes on CA private key management processes.
6.2.6. Private Key Transfer into or from a Cryptographic Module	CPS_V_3_2_7_EN.pdf 6.3.5 Entering the private key in the cryptographic module	At least two people are required to enter the key in the cryptographic module. Keys linked to subscribers cannot be transferred. Camerfirma keeps minutes on CA private key management processes.
6.2.7. Private Key Storage on Cryptographic Module	CPS_V_3_2_7_EN.pdf 6.2. Protecting the private key	6.2. Protecting the private key The CA's private key The Root signature private key and the CAs are kept in an nCipher cryptographic device. This device complies with the specifications FIPS 140-2 level three.
6.3.2. Certificate Operational Periods and Key Pair Usage Periods		AC Camerfirma do not issue end user certificate beyond 39 month period for SSL certificates.
6.5.1. Specific Computer Security Technical Requirements		Camerfirma is subject to the annual validations established by the UNE-ISO/IEC 27001:2007 standard, which regulates the establishment of suitable processes to ensure proper security management in information systems.
7.1. Certificate profile		OK
7.1.1. Version Number(s)		Every certificate issued by Camerfirma is X.509 v3

7.1.2. Certificate Content and Extensions; Application of RFC 5280		OK
7.1.2.1 Root CA Certificate		OK
7.1.2.2 Subordinate CA Certificate		OK
7.1.2.3 Subscriber Certificate		OK
7.1.2.4 All Certificates		OK
7.1.2.5 Application of RFC 5280		OK
7.1.3. Algorithm Object Identifiers		OK (no SSL certs with sha1)
7.1.4. Name Forms		
7.1.4.1 Issuer Information		OK
7.1.4.2 Subject Information		OK. We issued 4 certificates with a organization field but without Locality or stateorprovince. All of them are located and in revocation process.
7.1.4.3 Subject Information - Subordinate CA Certificates		OK
7.1.5. Name Constraints		OK
7.1.6. Certificate Policy Object Identifier		
7.1.6.1 Reserved Certificate Policy Identifiers		OK
7.1.6.2 Root CA Certificates		OK
7.1.6.3 Subordinate CA Certificates		OK
7.1.6.4 Subscriber Certificates		OK
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS	CPS_V_3_2_7_EN.pdf 2..7 Audits	OK
8.1. Frequency or circumstances of assessment	CPS_V_3_2_7_EN.pdf 2.7.1 Audit frequencies	OK
8.2. Identity/qualifications of assessor	CPS_V_3_2_7_EN.pdf 2.7.2 Auditor identification and rating	
8.4. Topics covered by assessment	CPS_V_3_2_7_EN.pdf 2.7.4 Topics covered in the audit	
8.6. Communication of results	CPS_V_3_2_7_EN.pdf 2.7.7 Audit report handling	
8.7. Self-Audits	CPS_V_3_2_7_EN.pdf 2.7.6 Auditing the Registration Authorities	OK
9.6.1. CA Representations and Warranties	CPS_V_3_2_7_EN.pdf 2.1. CA Obligations 2.1.2 RA Obligations 2.6.1.2 Terms and conditions.	OK
9.6.3. Subscriber Representations and Warranties	CPS_V_3_2_7_EN.pdf 2.1.3 Certificate applicant. 2.1.4 Signatory/Subscriber. 2.6.1.2 Terms and conditions.	
9.8. Limitations of liability	CPS_V_3_2_7_EN.pdf 2.2. Responsibility.	OK
9.9.1. Indemnification by CAs	CPS_V_3_2_7_EN.pdf 2.3. Financial responsibility	OK
9.16.3. Severability	CPS_V_3_2_7_EN.pdf 2.4.4 Dispute settlement procedure.	