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_eidas_v_1_2_1_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_eidas_v_1_2_1_EN.pdf 1.5.5 Registration Authority (RA)	RA Contract and RA Audits.
2.1. Repositories Provide the direct URLs to the CA's repositories	CPS_eidas_v_1_2_1_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_eidas_v_1_2_1_EN.pdf 1.2. General Overview.	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: - ETSI EN 319 401 v2.1.1 General Policy Requirements for Trust Service Providers - ETSI EN 319 411-1 v1.1.1 General Policy Requirements for Trust Service Providers - ETSI EN 319 411-2 v2.1.1 Policy and security requirements for TSP issuing certificates-Part 2 Requirements for trust service providers issuing EU qualified certificates - ETSI EN 319 412-1 v1.1.1 Certificate Profiles-Part 1 Overview and common data structures - ETSI EN 319 412-2 v1.1.1 Certificate Profiles-Part 2 Certificate profile for certificates issued to natural persons - ETSI EN 319 412-3 v1.1.1 Certificate Profiles-Part 3 Certificate profile for certificates issued to legal persons - ETSI EN 319 412-4 v1.1.1 Certificate Profiles-Part 4 Certificate profile for web site certificates - ETSI EN 319 412-5 v1.1.1 Certificate Profiles-Part 5 QCStatements

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.	[ROOT 1] CHAMBERS OF COMMERCE ROOT - 2016 - VALID: https://cevok.camerfirma.com - EXPIRED: https://cev.camerfirma.com - REVOKED: https://cevrv.camerfirma.com [ROOT 2] GLOBAL CHAMBERSIGN ROOT - 2016 - VALID: https://csevok.camerfirma.com - EXPIRED: https://csev.camerfirma.com - REVOKED: https://csevrv.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_eidas_v_1_2_1_EN.pdf 8.2. Procedures for specifying changes.	8.2.2.2 Notification method Any proposed changes to this policy are published immediately on Camerfirma's website 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 to this document are expressly communicated to third party entities and companies 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_eidas_v_1_2_1_EN.pdf 8.2.2.2 Notification method	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_eidas_v_1_2_1_EN.pdf 3.1.8.2.1 Subject/Signatory Identification.	3.1.8.2.1 Subject/Signatory Identification. The Subject or Signatory natural person (or alternatives as described in the eIDAS) when this person is also the Applicant, or the Applicant's representative when it is a legal entity, is required to present one of the following documents: - National Identity Document. - Residence card. - Passport. - Apostille for identification documents of applicants outside of Spanish territory. Physical presence is not required for these certificates in the cases established in eIDAS. http://www.camerfirma.com/index/buscador-documentos.php In the case of a representative of the Subject/Signatory, submission of an authorisation signed by a representative of the entity, who will act as the Applicant. For entities outside of Spanish territory, the document accrediting the representative capacity of the person signing the authorisation shall be issued duly apostilled, to verify the accuracy of the documentation.

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_eidas_v_1_2_1_EN.pdf 3.1.8.2.3 Entity’s ID. 3.1.6 Recognition, authentication and function of registered trademarks and other distinctive symbols 3.1.8.2.4 Proof of relationship.	3.1.8.2.3 Entity’s ID. Prior to the issuance and delivery of an organisation certificate, data relating to the incorporation and legal status of the entity must be authenticated. 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 website. http://www.camerfirma.com/index/buscador-documentos.php For entities outside of Spanish territory, the documentation that must be provided is that of the Official Registrar of the country concerned, duly apostilled where the existence of the entity in that country is indicated. In the issuance of OV/EV SSL component certificates, the existence of the entity can be checked by accessing the following public registries (www.registradores.org; www.rmc.es), Camerdata (www.camerdata.es), Informa (www.informa.es) or the Spanish Tax Office databases (www.aeat.es). EV must incontrovertibly verify the entity’s activity. This is checked by accessing the commercial registry or other business activity registers. For entities outside of Spanish territory, the documentation that must be provided is that of the Official Registrar of the country concerned, duly apostilled where the existence of the entity in that country is indicated. In addition: - It must be checked that the submitted data or documents are not older than one year. - That the organisation has legally existed for a minimum of one year. - Certificates cannot be issued for eliminated companies in countries where there is a government ban on doing business. In Public administrations: The documentation proving that the public administration, public body or public entity exists is not required because this identity is part of the General State Administration or other State Public Administration’s corporate scope. 3.1.6 Recognition, authentication and function of registered trademarks and other distinctive symbols Camerfirma does not assume any obligations regarding issuing certificates in relation to the use of trademarks or other distinctive symbols. Camerfirma deliberately does not allow the use of a distinctive sign on the Subject/Signatory that does not hold usage rights. However, Camerfirma is not required to seek evidence about the rights to use trademarks or other distinctive signs prior to issuing certificates. 3.1.8.2.4 Proof of relationship. - Certificate type: - Legal Entity Representative with general powers of representation - Representative of an entity without legal status with general powers of representation. - Legal Entity Representative for procedures with the Public Administrations - Representative of a Non-legal Entity for procedures with the Public Administrations - Legal Entity Representative for Legal Representatives - Representative of a Non-Legal Entity for Legal Representatives Documentation: Evidence on the Subject/Signatory’s representation powers with respect to the entity, by providing documentation showing their powers of representation depending on the type of entity. This information is published in the RA’s operating manuals and on Camerfirma’s website. - Certificate type: Corporate Documentation: Usually, an authorisation signed by the entity's Legal Representative. - Certificate type: Digital Seal Documentation: Authorisation to request the certificate by someone with sufficient power of representation for the signing entity. Certificate or query from the Companies Registry to check the incorporation and legal status of the entity and the appointment and term of office of the authorising person. - Certificate type: Public employee/Office and Seal Documentation: The identity document of the person who is acting on behalf of the Public Administration, public body or entity is required. The responsible Applicant/person shall be identified by the RA with his/her ID and authorisation from the responsible person, indicating that it is a public employee or appointment in the Official State Gazette where this person’s Tax ID No. appears. - Certificate type: Server Documentation: Domain control by the Signatory entity. Camerfirma checks that the data found in the WHOIS Internet service search match the entity’s information submitted in the request. It may be that the domain is assigned in the registrar’s database to a third party responsible for its management. In this case, the following is required so that the data of the last owner of the domain appears in the certificate: 1. An authorisation for issuing the certificate. 2. A communication from the organisation or person who controls the domain registration indicating this circumstance. For EV certificates, the certificate issuance guidelines require a distinction to 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 that the information is accurate. The certificate includes this information as defined in the reference certification policies. The certificates issued with SAN (Subject Alternative Name) extension. The above procedures should be carried out for each of the domains included in the certificate. The certificate cannot be issued if any of them do not meet established requirements. - Certificate type: CodeSign Documentation: Authorisation to request the certificate by someone with sufficient power of representation for the signing entity. Certificate or query from the Companies Registry to check the incorporation and legal status of the entity and the appointment and term of office of the authorising person. - Certificate type: TSU Documentation: Authorisation to request the certificate by someone with sufficient power of representation for the signing entity. Certificate or query from the Companies Registry to check the incorporation and legal status of the entity and the appointment and term of office of the authorising person.
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.	CPS_eidas_v_1_2_1_EN.pdf 3.1.8.2.3 Entity’s ID.	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.	CPS_eidas_v_1_2_1_EN.pdf 3.1.8.2.2 Service or machine identity 3.1.8.2.4 Proof of relationship.	3.1.8.2.2 Service or machine identity The existence of the domain or IP address. This is checked by accessing the WHOIS Internet domains. The use of a domain name or private IP addresses is allowed but obsolete (and will be prohibited after October 2016, which is why Camerfirma stopped issuing certificates of this kind from 1 November 2016. In any case, issued certificates of this type are revoked if their expiry date is after October 2016). The customer is notified of this before the certificate is issued. The existence of the domain or IP address. This is checked by accessing the WHOIS Internet domains. The use of a domain name or private IP addresses is allowed but obsolete (and will be prohibited after October 2016, which is why Camerfirma stopped issuing certificates of this kind from 1 November 2016. In any case, issued certificates of this type are revoked if their expiry date is after October 2016). The customer is 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 ccTLD or gTLD are applied. Checked by accessing the WHOIS Internet domains: - 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/ When the request for issuance is for a secure server or digital office certificate, Camerfirma will examine the registration of the authorised CAs, CAA, pursuant to RFC 6844, and if those CAA records are present and do not allow Camerfirma to issue those certificates because they are not registered, Camerfirma will not issue such a certificate but will allow applicants to re-submit the application once this situation has been remedied. The customer must modify his/her domain's data to allow Camerfirma to issue such a certificate. The tool used to check the provider’s assignment to the domain is https://toolbox.googleapps.com/apps/dig/#ANY/ This last procedure will not be necessary if the certificate issuance uses “Certificate Transparency” as indicated in the CABFORUM BRs. CA-Browser Forum BR 1.4.4. 3.1.8.2.4 Proof of relationship. - Certificate type: Server Documentation: Domain control by the Signatory entity. Camerfirma checks that the data found in the WHOIS Internet service search match the entity’s information submitted in the request. It may be that the domain is assigned in the registrar’s database to a third party responsible for its management. In this case, the following is required so that the data of the last owner of the domain appears in the certificate: 1. An authorisation for issuing the certificate. 2. A communication from the organisation or person who controls the domain registration indicating this circumstance. For EV certificates, the certificate issuance guidelines require a distinction to 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 that the information is accurate. The certificate includes this information as defined in the reference certification policies. The certificates issued with SAN (Subject Alternative Name) extension. The above procedures should be carried out for each of the domains included in the certificate. The certificate cannot be issued if any of them do not meet established requirements.
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 3.1.8.2.4 Proof of relationship.	
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 3.1.8.2.4 Proof of relationship.	
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_eidas_v_1_2_1_EN.pdf 3.1.8.2.2 Service or machine identity	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_eidas_v_1_2_1_EN.pdf 3.1.8.2.2 Service or machine identity 3.1.8.2.4 Proof of relationship.	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_eidas_v_1_2_1_EN.pdf 3.1. Initial record	
3.2.3. Authentication of Individual Identity	CPS_eidas_v_1_2_1_EN.pdf 3.1.8.2.1 Subject/Signatory Identification.	The Subject or Signatory natural person (or alternatives as described in the eIDAS) when this person is also the Applicant, or the Applicant's representative when it is a legal entity, is required to present one of the following documents: - National Identity Document. - Residence card. - Passport. - Apostille for identification documents of applicants outside of Spanish territory.

3.2.5. Validation of Authority	CPS_eidas_v_1_2_1_EN.pdf 3.1.8.2.4 Proof of relationship.	3.1.8.2.4 Proof of relationship. Certificate type: - Legal Entity Representative with general powers of representation - Representative of an entity without legal status with general powers of representation. - Legal Entity Representative for procedures with the Public Administrations - Representative of a Non-legal Entity for procedures with the Public Administrations - Legal Entity Representative for Legal Representatives - Representative of a Non-Legal Entity for Legal Representatives Documentation: Evidence on the Subject/Signatory's representation powers with respect to the entity, by providing documentation showing their powers of representation depending on the type of entity. This information is published in the RA's operating manuals and on Camerfirma's website. - Certificate type: Corporate Documentation: Usually, an authorisation signed by the entity's Legal Representative. - Certificate type: Digital Seal Documentation: Authorisation to request the certificate by someone with sufficient power of representation for the signing entity. Certificate or query from the Companies Registry to check the incorporation and legal status of the entity and the appointment and term of office of the authorising person. - Certificate type: Public employee/Office and Seal Documentation: The identity document of the person who is acting on behalf of the Public Administration, public body or entity is required. The responsible Applicant/person shall be identified by the RA with his/her ID and authorisation from the responsible person, indicating that it is a public employee or appointment in the Official State Gazette where this person's Tax ID No. appears. - Certificate type: Server Documentation: Domain control by the Signatory entity. Camerfirma checks that the data found in the WHOIS Internet service search match the entity's information submitted in the request. It may be that the domain is assigned in the registrar's database to a third party responsible for its management. In this case, the following is required so that the data of the last owner of the domain appears in the certificate: 1. An authorisation for issuing the certificate. 2. A communication from the organisation or person who controls the domain registration indicating this circumstance. For EV certificates, the certificate issuance guidelines require a distinction to 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 that the information is accurate. The certificate includes this information as defined in the reference certification policies. The certificates issued with SAN (Subject Alternative Name) extension. The above procedures should be carried out for each of the domains included in the certificate. The certificate cannot be issued if any of them do not meet established requirements. - Certificate type: CodeSign Documentation: Authorisation to request the certificate by someone with sufficient power of representation for the signing entity. Certificate or query from the Companies Registry to check the incorporation and legal status of the entity and the appointment and term of office of the authorising person. - Certificate type: TSU Documentation: Authorisation to request the certificate by someone with sufficient power of representation for the signing entity. Certificate or query from the Companies Registry to check the incorporation and legal status of the entity and the appointment and term of office of the authorising person.
3.2.6. Criteria for Interoperation or Certification Disclose all cross-certificates in the CA hierarchies under evaluation.	CPS_eidas_v_1_2_1_EN.pdf 4.2. Cross certification request.	Camerfirma does not have any cross certification process established at this time.
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_eidas_v_1_2_1_EN.pdf 3.1. Initial record	
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_eidas_v_1_2_1_EN.pdf 3.1.8.2.2 Service or machine identity 3.1.8.2.4 Proof of relationship.	3.1.8.2.2 Service or machine identity The existence of the domain or IP address. This is checked by accessing the WHOIS Internet domains. The use of a domain name or private IP addresses is allowed but obsolete (and will be prohibited after October 2016, which is why Camerfirma stopped issuing certificates of this kind from 1 November 2016. In any case, issued certificates of this type are revoked if their expiry date is after October 2016). The customer is notified of this before the certificate is issued. The existence of the domain or IP address. This is checked by accessing the WHOIS Internet domains. The use of a domain name or private IP addresses is allowed but obsolete (and will be prohibited after October 2016, which is why Camerfirma stopped issuing certificates of this kind from 1 November 2016. In any case, issued certificates of this type are revoked if their expiry date is after October 2016). The customer is 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 ccTLD or gTLD are applied. Checked by accessing the WHOIS Internet domains: - 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/ When the request for issuance is for a secure server or digital office certificate, Camerfirma will examine the registration of the authorised CAs, CAA, pursuant to RFC 6844, and if those CAA records are present and do not allow Camerfirma to issue those certificates because they are not registered, Camerfirma will not issue such a certificate but will allow applicants to re-submit the application once this situation has been remedied. The customer must modify his/her domain's data to allow Camerfirma to issue such a certificate. The tool used to check the provider’s assignment to the domain is https://toolbox.googleapps.com/apps/dig/#ANY/ This last procedure will not be necessary if the certificate issuance uses “Certificate Transparency” as indicated in the CABFORUM BRs. CA-Browser Forum BR 1.4.4. 3.1.8.2.4 Proof of relationship. Certificate type: - Server Documentation: Domain control by the Signatory entity. Camerfirma checks that the data found in the WHOIS Internet service search match the entity’s information submitted in the request. It may be that the domain is assigned in the registrar’s database to a third party responsible for its management. In this case, the following is required so that the data of the last owner of the domain appears in the certificate: 1. An authorisation for issuing the certificate. 2. A communication from the organisation or person who controls the domain registration indicating this circumstance. For EV certificates, the certificate issuance guidelines require a distinction to 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 that the information is accurate. The certificate includes this information as defined in the reference certification policies. The certificates issued with SAN (Subject Alternative Name) extension. The above procedures should be carried out for each of the domains included in the certificate. The certificate cannot be issued if any of them do not meet established requirements.
4.3.1. CA Actions during Certificate Issuance	CPS_eidas_v_1_2_1_EN.pdf 4.1.3 Applications for final-entity certificates in HSM, TSU and Subordinate CA.	
4.9.1.1 Reasons for Revoking a Subscriber Certificate Reasons for revoking certificates must be listed in the CA's CP/CPS.	CPS_eidas_v_1_2_1_EN.pdf 4.8.2 Causes for revocation and documentary proof	
4.9.1.2 Reasons for Revoking a Subordinate CA Certificate	CPS_eidas_v_1_2_1_EN.pdf 4.8.2 Causes for revocation and documentary proof	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_eidas_v_1_2_1_EN.pdf 4.8.3 Who can request revocation	
4.9.3. Procedure for Revocation Request	CPS_eidas_v_1_2_1_EN.pdf 4.8.4 Revocation request procedure.	
4.9.5. Time within which CA Must Process the Revocation Request	CPS_eidas_v_1_2_1_EN.pdf 4.8.5 Revocation period	For final-entity certificates. The revocation period, from the moment Camerfirma or an RA has reliable knowledge of a certificate revocation, takes place immediately, and is included in the next CRL issued and based on the data from the management platform from which the OCSP responder is fed.
4.9.7. CRL Issuance Frequency	CPS_eidas_v_1_2_1_EN.pdf 4.8.8 CRL issuance frequency	
4.9.9. On-line Revocation/Status Checking Availability	CPS_eidas_v_1_2_1_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_eidas_v_1_2_1_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_eidas_v_1_2_1_EN.pdf 4.8.1 Previous clarifications	AC Camerfirma keeps, in its OCSP service, information of a revoked certificate beyond its validity period.
4.10.2. Service Availability	CPS_eidas_v_1_2_1_EN.pdf 4.8.10 Availability of online service to check revocation	The OCSP service is fed from the CRLs issued by the various certification authorities (CA) or by access to the platform's database (EE). 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 per day, seven days per week, 365 days per year. Camerfirma makes every effort to ensure service is not down for more than 24 hours. This service is critical for Camerfirma's activities and is therefore considered in the contingency and business continuity plans.
5. MANAGEMENT, OPERATIONAL, and Physical CONTROLS	CPS_eidas_v_1_2_1_EN.pdf 5. Physical, Procedural and Personnel Security Controls	Camerfirma is subject to the annual validations established by the UNE-ISO/IEC 27001 standard, which regulates the establishment of suitable processes to ensure proper security management in information systems. Camerfirma has established physical and environmental security controls to protect resources in the buildings where the systems and equipment used for the transactions are stored. The physical and environmental security policy applicable to the certificate creation services provides protection against: - Unauthorised physical access - Natural disasters - Fires - Failure in supporting systems (electricity, telecommunications, etc.). - Building collapse - Flooding - Theft - Unauthorised withdrawal of equipment, information, devices and applications related to the components used for the Certification Service Provider's services The facilities have preventive and corrective maintenance services with 24h/365 day per year assistance and assistance during the 24 hours following the notice.
5.2.2. Number of Individuals Required per Task	CPS_eidas_v_1_2_1_EN.pdf 5.2.2 Number of people required per task	Camerfirma guarantees that at least two people will carry out tasks classified as sensitive. Mainly handling the Root CA and intermediate CA key storage device.
5.3.1. Qualifications, Experience, and Clearance Requirements	CPS_eidas_v_1_2_1_EN.pdf 5.3.1 Background, qualifications, experience and accreditation requirements	All personnel undertaking tasks classified as duties of trust must have worked at the workplace for at least one year and have a fixed employment contract. All personnel are qualified and have been trained in the procedures to which they have been assigned. Personnel in positions of trust must have no personal interests that conflict with undertaking the role to which they are entrusted. 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 request validation request duties. In general, Camerfirma removes an employee's trust roles if it discovers that person has committed any criminal act that could affect the performance of his/her duties. Camerfirma shall not assign a trusted or managed site to a person who is not suitable for the position, especially for having been convicted of a crime or misdemeanour affecting their suitability for the position. For this reason, an investigation will first be carried out, to the extent permitted by applicable law, on the following aspects: • Studies, including alleged degree. • Previous work, up to five years, including professional references and checking that the alleged work was actually performed. • Delinquency
5.3.3. Training Requirements and Procedures	CPS_eidas_v_1_2_1_EN.pdf 5.3.3 Training requirements	Personnel undertaking duties of trust must have been trained in accordance with Certification Policies. There is a training plan that is part of the UNE-ISO/IEC 27001 controls. Registration operators who validate EV secure server certificates receive specific training in accordance with special regulations on issuing these certificates. Training includes the following content: • Security principles and mechanisms of the public certification hierarchy. • Versions of hardware and applications in use. • Tasks to be carried out by the person. • Management and processing of incidents and security compromises. • Business continuity and emergency procedures. • Management and security procedure related to processing personal data.
5.3.4. Retraining Frequency and Requirements	CPS_eidas_v_1_2_1_EN.pdf 5.3.4 Information updating requirements and frequency	Camerfirma undertakes the required updating procedures to ensure certification duties are undertaken properly, especially when they are modified substantially.
5.3.7. Independent Contractor Controls	CPS_eidas_v_1_2_1_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_eidas_v_1_2_1_EN.pdf 4.10.1 Type of recorded files.	
5.4.3. Retention Period for Audit Logs	CPS_eidas_v_1_2_1_EN.pdf 4.10.2 File storage period	
5.4.8. Vulnerability Assessments	CPS_eidas_v_1_2_1_EN.pdf 4.9.7 Vulnerability analysis	The analysis of vulnerabilities is covered by the Camerfirma audit processes. Risk and vulnerability management processes are reviewed once a year in accordance with the UNE-ISO/IEC 27001 certificate and included in the Risk analysis document, code CONF-2005-05-01. This document specifies the controls implemented to guarantee required security objectives. The system audit data is stored so that it can be used to investigate any incident and locate vulnerabilities. Camerfirma runs a monthly systems analysis with the aim of detecting suspicious activities. This report is executed by an external company and includes: • Intrusion Detection - IDS (HIDS) • OSSEC Integrity Control System • SPLUNK. Operations intelligence. • Event correlation report. Camerfirma corrects any problem reported and registered by the systems department.
5.5.2. Retention Period for Archive	CPS_eidas_v_1_2_1_EN.pdf 4.10.2 File storage period	Certificates, contracts with Subjects/Signatories and any information relating to the Subject/Signatory's identification and authentication must be kept for at least 15 years. Older versions of documents are also kept for a period of at least fifteen (15) years by AC Camerfirma and may be consulted by stakeholders with reasonable cause.

5.7.1. Incident and Compromise Handling Procedures	CPS_eidas_v_1_2_1_EN.pdf 4.12. Retrieval in the event of compromised key security or natural disaster	Camerfirma has developed a Contingency plan to retrieve critical systems, if an alternative data centre were necessary as part of the UNE-ISO/IEC 27001 certification. The continuity and contingency plan is drafted in document CONF-2003-00-01 Continuity and Availability. If root key security is compromised, this must be considered a specific case in the contingency and business continuity document. If the keys are replaced, this incident affects recognition by the various private and public sector applications. Recovering the validity of keys in business terms mainly depends on the duration of these recognised processes. The contingency and business continuity document include these purely technical and operational terms to ensure that new keys are available, which is not the case for recognition by third parties. The commitment of algorithms or associated parameters used for generating digital certificates or associated services is also incorporated into the contingency and business continuity plan. Any failure to meet the targets set by this contingency plan is considered reasonably unavoidable unless there is a breach of obligations on Camerfirma's part in implementing these processes. A part of the implementation of its ISO27001 and ISO20000 systems, Camerfirma has developed plans and procedures for continuous improvement in a way that systematically reinforces all experiences covered in the management of incidents and avoids their repetition. Related Document IN-2007-02-08 Continuous Improvement Procedure 4.12.1 An entity's key is compromised The contingency plan encompassed in Camerfirma's UNE-ISO/IEC 27001 certification considers that compromised security of the CA's private key is a disaster. If the security of a root key is compromised: - All Subjects/Signatories, User Parties and other CAs with which agreements or other relationships have been established must be informed. - They are informed that the certificates and information relating to the revocation status that are signed using this key are not valid. 4.12.2 Security installation following a natural or other type of disaster Camerfirma will reinstate critical services (revocation and publication of revocations) in accordance with the contingency and business continuity plan encompassed in the UNE-ISO/IEC 27001 certification, indicating restoration within 24 hours. Camerfirma has an alternative centre if required to start up the certification systems, which is described in the business continuity plan.
6.1.1. Key Pair Generation	CPS_eidas_v_1_2_1_EN.pdf 6.1. Key pair creation and installation	The computers used by Camerfirma to store root keys and are certified in accordance with FIPS 140-2, level 3. The root keys are generated and managed on an off-line computer in a cryptographic room. Reference document CONF-00-2012-02-Script of CA ROOT generation xxxx where "xxxx" is the year corresponding to the creation of the key. The creation of Subordinate CAs keys is generated in HSM equipment certified FIPS 140-2, level 3, where it is hosted for its corresponding use. The certificate issued by the root key is made in a secure cryptographic room.
6.1.2. Private Key Delivery to Subscriber	CPS_eidas_v_1_2_1_EN.pdf 6.1.2 Delivering the public key to the certificate issuer	The public key is sent to Camerfirma to create the certificate when the circuit so requires. It is sent in standard PKCS#10 format.
6.1.5. Key Sizes	CPS_eidas_v_1_2_1_EN.pdf 6.1.4 Size and validity of issuer's keys	
6.1.6. Public Key Parameters Generation and Quality Checking	CPS_eidas_v_1_2_1_EN.pdf 6.1.1 Public key creation parameters.	The public key for the Root CA and Subordinate CA and for Signatories' certificates is encrypted pursuant to RFC 3280 and PKCS#1. RSA is the key generation algorithm.
6.1.7. Key Usage Purposes	CPS_eidas_v_1_2_1_EN.pdf 6.1.4 Purposes of key use	The keys must only be used for the purposes stated in the "Key usage purposes" section of the certification policies for each of the certificates issued. The CA makes all reasonable efforts to confirm that the CA's signature keys are used only for the purposes of generating certificates and signing CRLs. The key usage limitation is defined in the certificate content in the extensions: keyUsage, extendedKeyUsage and basicConstraints
6.2. Private Key Protection and Cryptographic Module Engineering Controls	CPS_eidas_v_1_2_1_EN.pdf 6.2. Protecting the private key	The CA's private key The private signature key of the root CAs and Subordinate CAs are maintained in a cryptographic device that meets FIPS 140-2 level 3 specifications. When the CA's 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's private key backups are stored securely. This procedure is described in detail in the Camerfirma security policies. Subordinate CAs' keys are kept on devices that comply with at least FIPS 140-1 Level 3. The Signatory's private key The Signatory's private key can be stored in a software or hardware device. When it is stored in software format, Camerfirma provides configuration instructions for secure use. Cryptographic devices distributed by Camerfirma to host qualified certificates must meet all requirements of qualified secure signature creation devices and therefore are suitable for generating qualified signatures. Information regarding the key creation and custody process that Camerfirma uses is included in the digital certificate itself, in the corresponding OID, allowing the User Party to act in consequence.
6.2.5. Private Key Archival	CPS_eidas_v_1_2_1_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 Signatory'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 Signatory's keys created on hardware cannot be copied because they cannot be taken out of the cryptographic device. Camerfirma keeps records on CA private key management processes.
6.2.6. Private Key Transfer into or from a Cryptographic Module	CPS_eidas_v_1_2_1_EN.pdf 6.3.2 Entering the private key in the cryptographic module.	At least two people are required to enter the key in the cryptographic module. Keys associated with Signatories cannot be transferred. Camerfirma keeps records on CA private key management processes.
6.2.7. Private Key Storage on Cryptographic Module	CPS_eidas_v_1_2_1_EN.pdf 6.2. Protecting the private key	The CA's private key The private signature key of the root CAs and Subordinate CAs are maintained in a cryptographic device that meets FIPS 140-2 level 3 specifications. When the CA's 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's private key backups are stored securely. This procedure is described in detail in the Camerfirma security policies. Subordinate CAs' keys are kept on devices that comply with at least FIPS 140-1 Level 3.
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. AC Camerfirma pass 3 vulnerability tests and a penetration test yearly.
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.
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_eidas_v_1_2_1_EN.pdf 2.7 Audits	OK
8.1. Frequency or circumstances of assessment	CPS_eidas_v_1_2_1_EN.pdf 2.7.1 Audit frequency	OK
8.2. Identity/qualifications of assessor	CPS_eidas_v_1_2_1_EN.pdf 2.7.2 Auditor identification and rating	
8.4. Topics covered by assessment	CPS_eidas_v_1_2_1_EN.pdf 2.7.4 Topics covered in the audit	
8.6. Communication of results	CPS_eidas_v_1_2_1_EN.pdf 2.7.7 Processing the audit report	
8.7. Self-Audits	CPS_eidas_v_1_2_1_EN.pdf 2.7.6 Auditing the Registration Authorities	OK
9.6.1. CA Representations and Warranties	CPS_eidas_v_1_2_1_EN.pdf 2.1. Obligations 2.1.1 External Subordinate CA. 2.1.2 RA 2.6.1.2 Terms and conditions.	OK
9.6.3. Subscriber Representations and Warranties	CPS_eidas_v_1_2_1_EN.pdf 2.1.3 Signatory 2.1.4 Subject/Certificate holder. 2.6.1.2 Terms and conditions.	
9.8. Limitations of liability	CPS_eidas_v_1_2_1_EN.pdf 2.2. Liability.	OK
9.9.1. Indemnification by CAs	CPS_eidas_v_1_2_1_EN.pdf 2.3. Financial responsibility	OK
9.16.3. Severability	CPS_eidas_v_1_2_1_EN.pdf 2.4.4 Dispute resolution procedure.	