Valencia, July 14th, 2018

Independent Assurance Report

To the management of AC Camerfirma SA. ("Camerfirma"):

Scope

We have been engaged, in a reasonable assurance engagement, to report on Camerfirma management's assertion that for its Certification Authority (CA) operations at Avila and Madrid, SPAIN, throughout the period 14th of April 2017 to the 13th of April 2018 for the root Certification Authority "Chambers of Commerce Root", "Chambers of Commerce Root - 2008" and "CHAMBERS OF COMMERCE ROOT - 2016" as detailed in Appendix 1, Camerfirma has:

- disclosed its SSL certificate lifecycle management business practices in its:
    - DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN CERTIFICADOS DIGITALES AC CAMERFIRMA SA EIDAS-2016 – Version 1.2.3 http://docs.camerfirma.com/publico/DocumentosWeb/politicas/CPS_eidas_v_1_2_3.pdf
    - DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN CERTIFICADOS DIGITALES AC CAMERFIRMA SA - Versión 3.3 http://docs.camerfirma.com/publico/DocumentosWeb/politicas/CPS_v_3_3.pdf
    - POLÍTICA DE CERTIFICACIÓN CHAMBERS OF COMMERCE ROOT – Version 1.0.1 http://docs.camerfirma.com/publico/DocumentosWeb/politicas/PC_Chambers_of_Commerce_Root_1_0_1.pdf
    - CERTIFICATION POLICY FOR WEBSITES – Version 2.0 http://docs.camerfirma.com/publico/DocumentosWeb/politicas/PC_Camerfirma_For_Websites.pdf
    - POLÍTICA DE CERTIFICACIÓN CAMERFIRMA EXPRESS CORPORATE SERVER – Version 1.1.1 http://docs.camerfirma.com/publico/DocumentosWeb/politicas/PC_Camerfirma_Corporate_Server_1_1_1.pdf

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Camerfirma website, and provided such services in accordance with its disclosed practices

- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles; and
  - SSL subscriber information is properly authenticated (for the registration activities performed by Camerfirma)

- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2.

Certification authority's responsibilities

Camerfirma's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2.

Our independence and quality control

We have complied with the independence and other ethical requirements of the Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

Auren applies International Standard on Quality Control 1, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Auditor's responsibilities

Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, Assurance Engagements Other than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion is fairly stated, and, accordingly, included:

(1) obtaining an understanding of Camerfirma's SSL certificate lifecycle management business practices including its relevant controls over the issuance, renewal, and revocation of SSL certificates and obtaining an understanding of Camerfirma's network and certificate system security to meet the requirements set forth by the CA/Browser Forum
(2) selectively testing transactions executed in accordance with disclosed SSL certificate lifecycle management practices;
(3) testing and evaluating the operating effectiveness of the controls; and
(4) performing such other procedures as we considered necessary in the circumstances.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Relative effectiveness of controls

The relative effectiveness and significance of specific controls at Camerfirma and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Inherent limitations

Because of the nature and inherent limitations of controls, Camerfirma's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

Basis for qualified opinion

During our procedures, we noted that sufficient controls to ensure that the CA CP and CPS describes how the CA implements the latest version of the Baseline Requirements were not implemented.

This caused WebTrust Criterion 4 of Principle 1 which reads:

The Certificate Authority has controls to provide reasonable assurance that the CA CP and/or CPS that describes how the CA implements the latest version of the Baseline Requirements are updated annually.

to not be met.

During our procedures, we noted that Camerfirma had issued certificates with errors according to the CA/B Forum requirements. Specifically:

- Duplicate SAN entry
- Certificates with organizationName but without countryName
- DNSName is not FQDN

- Certificates with organizationName but without localityName or stateOrProvinceName
- Wildcard to immediate left of public suffix in SAN
- Certificates with rfc822Name or directoryName type in alternative name

This caused WebTrust Criterion 2.5 of Principle 2 which reads:

The CA maintains controls to provide reasonable assurance that the extensions, key sizes, and certificate policy identifiers (including Reserved Certificate Policy Identifiers) of Subscriber certificates generated after the Effective Date (1 July 2012) conform to the Baseline Requirements.

and WebTrust Criterion 2.6 of Principle 2 which reads:

The CA maintains controls to provide reasonable assurance that with exception to the requirements stipulated in the Baseline Requirements Sections 7.1.2.1, 7.1.2.2, and 7.1.2.3, all other fields and extensions of certificates generated after the Effective Date (1 July 2012) are set in accordance with RFC 5280.

and WebTrust Criterion 2.12 of Principle 2 which reads:

The CA maintains controls to provide reasonable assurance that for Subscriber certificates issued:

- *The subjectAltName extension is present and contains at least one entry*
- *Each entry MUST be either:*
  - *A dNSName containing the Fully-Qualified Domain Name (Wildcard FQDNs permitted); or*
  - *An iPAddress containing the IP address of a server.*

and WebTrust Criterion 2.14 of Principle 2 which reads:

The CA maintains controls to provide reasonable assurance that Subject information of Certificates conforms to the Baseline Requirements, including:

- *subject:commonName*
- *subject:organizationName*
- *subject:givenName*
- *subject:surname*
- *subject:streetAddress*
- *subject:localityName*
- *subject:stateOrProvinceName*
- *subject:postalCode*
- *subject:countryName*
- *subject:organizationalUnitName*
- *Other Subject Attributes*
- *Subject field requirements if Reserved Certificate Policy Identifiers are asserted*
- *Subject Information for Subordinate CA certificates*

to not be met.

During our procedures, we noted that for some problem communications has not begun investigation of Certificate Problem Reports within 24 hours.

This caused WebTrust Criterion 5.2 of Principle 2 which reads:

The CA maintains controls to provide reasonable assurance that it:

- *has the capability to accept and acknowledge Certificate Problem Reports on a 24x7 basis;*
- *identifies high priority Certificate Problem Reports;*
- *begin investigation of Certificate Problem Reports within 24 hours:*
- *decides whether revocation or other appropriate action is warranted; and*
- *where appropriate, forwards such complaints to law enforcement.*

to not be met.

During our procedures, we noted that for some revocation requests the subscriber Certificates were not revoked within 24 hours.

This caused WebTrust Criterion 5.3 of principle 2 which reads:

The CA maintains controls to provide reasonable assurance that Subscriber Certificates are revoked within 24 hours if any of the following events occurs:

1. *The Subscriber requests in writing that the CA revoke the Certificate;*
2. *The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization;*
3. *The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of SSL Baseline Requirements Sections 6.1.5 and 6.1.6;*
4. *The CA obtains evidence that the Certificate was misused;*
5. *The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;*
6. *The CA is made aware of any circumstance indicating that use of a FullyQualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);*
7. *The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;*
8. *The CA is made aware of a material change in the information contained in the Certificate;*
9. *The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement;*
10. *The CA determines that any of the information appearing in the Certificate is inaccurate or misleading;*
11. *The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;*

12. *The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;*
13. *The CA is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate;*
14. *Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement; or*
15. *The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time).*

to not be met.

During our procedures, we could not evidence self-assessments on at least a quarterly basis against a randomly selected sample of at least three percent of the Certificates issued.

This caused WebTrust Criterion 8.4 of Principle 2 which reads:

The CA maintains controls to provide reasonable assurance that:

- *it performs ongoing self-assessments on at least a quarterly basis against a randomly selected sample of at least three percent (3%) of the Certificates issued during the period commencing immediately after the previous selfassessment samples was taken,*
- *Except for Delegated Third Parties that undergo an annual audit that meets the criteria specified in the Baseline Requirements, the CA performs ongoing quarterly assessments against a randomly selected sample of at least three percent (3%) of the Certificates verified by the Delegated Third Party in the period beginning immediately after the last samples was taken*
- *The CA reviews each Delegated Third Party's practices and procedures to assess that the Delegated Third Party is in compliance with these Requirements and the relevant Certificate Policy and/or Certification Practice Statement.*

to not be met.

Qualified Opinion

In our opinion, except for the matters described in the basis for qualified section above, throughout the period 14th of April 2017 to the 13th of April 2018, Camerfirma management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3.

This report does not include any representation as to the quality of Camerfirma's services beyond those covered by the WebTrust Principles and Criteria for

Certification Authorities – SSL Baseline with Network Security v2.2, nor the suitability of any of Camerfirma's services for any customer's intended purpose.

F. Mondragon, Auditor
auren
Valencia, SPAIN
July 14th, 2018

APPENDIX 1 List of CAs in Scope

Root CAs
1 - CHAMBERS OF COMMERCE ROOT – 2016 2 - GLOBAL CHAMBERSIGN ROOT – 2016 3 - Chambers of Commerce Root – 2008 4 - Global Chambersign Root – 2008 5 - Chambers of Commerce Root 6 - Global Chambersign Root
OV SSL Issuing CAs
1.3 - AC CAMERFIRMA FOR WEBSITES – 2016 3.2 - Camerfirma Corporate Server II – 2015 3.3 - Camerfirma AAPP II – 2014 5.2 - AC Camerfirma Express Corporate Server v3 5.3 - AC CAMERFIRMA AAPP
EV SSL Issuing Cas
1.3 - AC CAMERFIRMA FOR WEBSITES – 2016 2.1.3 - AC CAMERFIRMA GLOBAL FOR WEBSITES – 2016 3.2 - Camerfirma Corporate Server II – 2015 3.3 - Camerfirma AAPP II – 2014
Other CAs
1.1 - AC CAMERFIRMA FOR LEGAL PERSONS – 2016 1.2 - AC CAMERFIRMA FOR NATURAL PERSONS – 2016 1.4 - AC CAMERFIRMA CODESIGN – 2016 1.5 - AC CAMERFIRMA TSA – 2016 2.1 - AC CAMERFIRMA – 2016 2.1.1 - AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS – 2016 2.1.2 - AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS – 2016, 3.5 - Camerfirma TSA II - 2014 4.1 - AC Camerfirma – 2009 4.1.1 - RACER – 2009 5.1 - AC Camerfirma Certificados Camerales 6.1 - AC Camerfirma, O=AC Camerfirma SA 6.1.1 - RACER
Legacy Inactive Cas
3.1 - Camerfirma Certificados Camerales – 2009 (revoked 01/29/2018) 3.4 - Camerfirma TSA – 2009 (revoked 01/29/2018) 5.4 - AC Camerfirma TSA (revoked 12/04/2017) 5.5 - AC Camerfirma Codesign v2 (revoked 11/27/2017)

CA Identifying Information for in Scope CAs

CHAMBERS OF COMMERCE ROOT – 2016

CA#	Subject	Issuer	serialNumber	Key Type	Sig Algorithm	notBefore	NotAfter	SKI	SHA256 Fingerprint
1	CN=CHAMBERS OF COMMERCE ROOT – 2016, O=AC CAMERFIRMA S.A, C=ES	CN=CHAMBERS OF COMMERCE ROOT – 2016, O=AC CAMERFIRMA S.A, C=ES	349A2DA18206B2B3	rsaEncryption – 4096 bit	sha256WithRSA Encryption	April 14 09:35:48 2016 GMT	April 08 09:35:48 2040 GMT	9E:2E:65:4F:3E:57:F5:AB:7D:96:C6:8B:DF:B3:35:6D:4A:E8:9E:8B	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
1.1	CN=AC CAMERFIRMA FOR LEGAL PERSONS – 2016, O=AC CAMERFIRMA S.A., C=ES	CN=CHAMBERS OF COMMERCE ROOT – 2016, O=AC CAMERFIRMA S.A, C=ES	54B16EE111245A42	rsaEncryption – 4096 bit	sha256WithRSA Encryption	April 14 10:33:07 2016 GMT	March 09 10:33:07 2040 GMT	C3:27:85:93:D7:2F:96:C5:1B:AC:76:33:D9:86:A2:4A:7D:68:14:42	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
1.2	CN = AC CAMERFIRMA FOR NATURAL PERSONS – 2016, O=AC CAMERFIRMA S.A., C=ES	CN=CHAMBERS OF COMMERCE ROOT – 2016, O=AC CAMERFIRMA S.A, C=ES	51514CB44FA454F5	rsaEncryption – 4096 bit	sha256WithRSA Encryption	April 14 10:48:09 2016 GMT	March 09 10:48:09 2040 GMT	70:B8:F8:24:C7:51:CA:CE:22:80:92:08:C9:C0:68:2F:C1:47:58:51	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
1.3	CN=AC CAMERFIRMA FOR WEBSITES – 2016, O=AC CAMERFIRMA S.A., C=ES	CN=CHAMBERS OF COMMERCE ROOT – 2016, O=AC CAMERFIRMA S.A, C=ES	23CDF491B343480B	rsaEncryption – 4096 bit	sha256WithRSA Encryption	Apr 18 17:43:54 2016 GMT	March 13 17:43:54 2040 GMT	EC:95:33:3B:71:C0:D2:B1:9C:58:23:0B:36:41:BC:54:9E:2C:92:1D	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
1.4	CN=AC CAMERFIRMA CODESIGN – 2016, O=AC CAMERFIRMA S.A., C=ES	CN=CHAMBERS OF COMMERCE ROOT – 2016, O=AC CAMERFIRMA S.A, C=ES	454A8B11B4E135F2	rsaEncryption – 4096 bit	sha256WithRSA Encryption	Apr 14 10:17:54 2016 GMT	March 09 10:17:54 2040 GMT	A7:25:4A:06:4E:E5:60:90:40:E4:9E:72:25:98:85:EA:3C:DF:FA:92	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
1.5	CN=AC CAMERFIRMA TSA – 2016, O=AC CAMERFIRMA S.A., C=ES	CN=CHAMBERS OF COMMERCE ROOT – 2016, O=AC CAMERFIRMA S.A, C=ES	15B7A58A54FF0282	rsaEncryption – 4096 bit	sha256WithRSA Encryption	Apr 14 12:42:09 2016 GMT	March 09 12:12:09 2040 GMT	1E:6D:B5:C6:3F:EF:92:55:5E:37:FA:DB:FD:10:AA:BA:D9:3B:4E:2C	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

GLOBAL CHAMBERSIGN ROOT - 2016

CA#	Subject	Issuer	serialNumber	Key Type	Sig Algorithm	notBefore	NotAfter	SKI	SHA256 Fingerprint
2	CN=GLOBAL CHAMBERSIGN ROOT – 2016, O=AC CAMERFIRMA S.A, C=ES	CN=GLOBAL CHAMBERSIGN ROOT – 2016, O=AC CAMERFIRMA S.A, C=ES	2DD22E5030A65E13	rsaEncryption – 4096 bit	sha256WithRSA Encryption	Apr 14 09:50:06 2016 GMT	Apr 08 09:50:06 2040 GMT	E8:9B:CD:7E:86:62:9B:7A:4D:8C:00:97:39:85:CF:1C:78:90:70:3A	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
2.1	CN=AC CAMERFIRMA – 2016, O=AC CAMERFIRMA S.A., C=ES	CN=GLOBAL CHAMBERSIGN ROOT – 2016, O=AC CAMERFIRMA S.A, C=ES	1108715A574BA44D	rsaEncryption – 4096 bit	sha256WithRSA Encryption	Apr 14 13:23:49 2016 GMT	March 09 13:23:49 2040 GMT	D2:84:97:44:4D:D9:88:EE:7C:25:BF:52:80:B3:29:48:9B:8B:18:84	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
2.1.1	CN=AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS – 2016	CN=AC CAMERFIRMA – 2016, O=AC CAMERFIRMA S.A., C=ES	11087A21EF4A8102	rsaEncryption – 4096 bit	sha256WithRSA Encryption	Apr 14 17:13:34 2016 GMT	Feb 08 17:13:34 2040 GMT	4E:36:56:A8:58:CE:1B:83:85:60:4C:D4:1B:A1:DF:72:3D:AF:7B:5F	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
2.1.2	CN=AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS – 2016, O=AC CAMERFIRMA S.A, C=ES	CN=AC CAMERFIRMA – 2016, O=AC CAMERFIRMA S.A., C=ES	3487D16B4118D1A2	rsaEncryption – 4096 bit	sha256WithRSA Encryption	Apr 14 16:58:36 2016 GMT	Feb 08 16:58:36 2040 GMT	80:21:DF:71:F1:EF:D4:6B:DA:33:86:D1:0F:BE:C5:DD:65:4C:84:5E	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
2.1.3	CN = AC CAMERFIRMA GLOBAL FOR WEBSITES – 2016, O=AC CAMERFIRMA S.A, C=ES	CN=AC CAMERFIRMA – 2016, O=AC CAMERFIRMA S.A., C=ES	2EE38417DD54AF32	rsaEncryption – 4096 bit	sha256WithRSA Encryption	Apr 18 17:57:56 2016 GMT	Feb 12 17:57:56 2040 GMT	F4:35:D1:DA:FD:FE:A4:11:06:C6:2C:3C:C2:FF:9C:FA:89:91:0F:6A	99:BD:A6:79:2D:CA:ED:71:45:BF:9B:7F:46:68:31:05:18:21:AE:F0:32:16:97:11:76:24:1A:FC:21:23:AB:84

Chambers of Commerce Root – 2008

CA#	Subject	Issuer	serialNumber	Key Type	Sig Algorithm	notBefore	NotAfter	SKI	SHA256 Fingerprint
3	CN=Chambers of Commerce Root - 2008, O=AC Camerfirma S.A., C=ES	CN=Chambers of Commerce Root - 2008, O=AC Camerfirma S.A., C=ES	00A3DA427EA4B1AEDA	rsaEncryption - 4096 bit	sha1WithRSAEncryption	August 01 14:29:50 2008 GMT	July 31 14:29:50 2038 GMT	F9:24:AC:0F:B2:B5:F8:79:C0:FA:60:88:1B:C4:D9:4D:02:9E:17:19	06:3E:4A:FA:C4:91:DF:D3:32:F3:08:9B:85:42:E9:46:17:D8:93:D7:FE:94:4E:10:A7:93:7E:E2:9D:96:93:C0
3.1	CN=Camerfirma Certificados Camerales - 2009, O=AC Camerfirma S.A., C=ES	CN=Chambers of Commerce Root - 2008, O=AC Camerfirma S.A., C=ES	02	rsaEncryption - 4096 bit	sha1WithRSAEncryption	March 16 19:40:20 2009 GMT	March 14 19:40:20 2019 GMT	1E:C4:5A:8A:84:6F:11:90:58:B3:E2:09:D7:16:E6:EA:C3:24:E6:8D	2F:2B:32:E7:8F:C6:9D:2F:FC:64:5E:B6:06:8E:07:4E:74:97:74:49:5F:DC:25:10:93:B0:EE:E0:4E:FA:FD:17
3.2	CN = Camerfirma Corporate Server II - 2015, O=AC Camerfirma S.A., C=ES	CN=Chambers of Commerce Root - 2008, O=AC Camerfirma S.A., C=ES	621FF31C489BA136	rsaEncryption - 4096 bit	sha256WithRSA Encryption	January 15 11:21:16 2015 GMT	December 15 11:21:16 2037 GMT	63:E9:F0:F0:56:00:68:65:B0:21:6C:0E:5C:D7:19:08:9D:08:34:65	66:EA:E2:70:9B:54:CD:D1:69:31:77:B1:33:2F:F0:36:CD:D0:F7:23:DB:30:39:ED:31:15:55:A6:CB:F5:FF:3E
3.3	CN=Camerfirma AAPP II - 2014, O=AC Camerfirma S.A., C=EU	CN=Chambers of Commerce Root - 2008, O=AC Camerfirma S.A., C=ES	1548D054B8A842BA	rsaEncryption - 4096 bit	sha256WithRSA Encryption	Dec 16 13:59:01 2017 GMT	Dec 15 13:59:01 2037 GMT	5D:A1:55:A4:DC:4A:AC:83:11:F9:AA:38:E5:F7:68:4A:FE:15:15:4C	72:39:D2:F7:70:FA:FF:3B:1C:F8:BE:2A:05:EC:03:ED:EA:AC:05:3B:55:4F:90:D3:69:21:15:5B:A8:05:19:81
3.4	CN=Camerfirma TSA - 2009, O=AC Camerfirma S.A., C=ES	CN=Chambers of Commerce Root - 2008, O=AC Camerfirma S.A., C=ES	05	rsaEncryption - 4096 bit	sha1WithRSAEncryption	March 16 19:45:26 2009 GMT	March 14 19:45:26 2019 GMT	0E:31:4D:5D:E9:E1:C2:5C:5B:BC:F5:2B:05:BA:AF:47:0D:16:AB:DC	4C:25:12:B5:DB:C0:D3:54:C7:21:42:50:B8:25:6D:4B:FB:60:89:41:96:9B:8D:89:C4:21:50:21:E0:B2:B9:05
3.5	CN=Camerfirma TSA II - 2014, O=AC Camerfirma S.A., C=ES	CN=Chambers of Commerce Root - 2008, O=AC Camerfirma S.A., C=ES	25A454BC34551238	rsaEncryption - 4096 bit	sha256WithRSA Encryption	Dec 16 16:45:33 2014 GMT	Dec 15 16:45:33 2037 GMT	17:C5:40:BC:2A:F8:45:B8:AB:33:BF:F8:6F:49:6C:F6:17:CA:B7:D4	65:69:5D:50:01:17:FD:72:70:F1:02:7E:D1:21:F0:59:42:67:00:75:46:1D:33:7E:EE:C7:F6:A5:B7:57:A4:7A

Global Chambersign Root – 2008

CA#	Subject	Issuer	serialNumber	Key Type	Sig Algorithm	notBefore	NotAfter	SKI	SHA256 Fingerprint
4	CN=Global Chambersign Root - 2008, O=AC Camerfirma S.A., C=ES	CN=Global Chambersign Root - 2008, O=AC Camerfirma S.A., C=ES	00C9CDD3E9D57D23CE	rsaEncryption - 4096 bit	sha1WithRSAEncryption	Aug 01 14:31:40 2008 GMT	July 31 14:31:40 2038 GMT	B9:09:CA:9C:1E:DB:D3:6C:3A:6B:AE:ED:54:F1:5B:93:06:35:2E:5E	13:63:35:43:93:34:A7:69:80:16:A0:D3:24:DE:72:28:4E:07:9D:7B:52:20:BB:8F:BD:74:78:16:EE:BE:BA:CA
4.1	CN=AC Camerfirma - 2009, O=AC Camerfirma S.A., C=ES	CN=Global Chambersign Root - 2008, O=AC Camerfirma S.A., C=ES	02	rsaEncryption - 4096 bit	sha1WithRSAEncryption	March 16 19:16:25 2009 GMT	March 11 19:16:25 2029 GMT	C8:00:0F:FC:C6:52:FC:9F:DB:3B:64:2E:32:B9:6E:2E:71:F3:65:79	B6:8D:5D:9B:4E:A6:35:95:7C:0C:32:15:C2:0D:35:B2:21:7B:69:E3:49:C7:A3:04:C4:F9:7F:20:C4:08:1F:88
4.1.1	CN=RACER - 2009, O=AC Camerfirma S.A., C=ES	CN=AC Camerfirma - 2009, O=AC Camerfirma S.A., C=ES	03	rsaEncryption - 4096 bit	sha1WithRSAEncryption	March 25 12:47:09 2009 GMT	March 23 12:47:09 2019 GMT	AC:16:D7:10:D1:6F:75:F6:84:88:68:E6:44:25:11:72:CA:B3:1B:80	47:CF:DE:E3:76:09:72:5C:FF:03:7B:56:A0:71:C4:3A:A0:58:69:A8:44:28:A5:D8:61:FF:92:B9:45:02:92:AA

Chambers of Commerce Root

CA#	Subject	Issuer	serialNumber	Key Type	Sig Algorithm	notBefore	NotAfter	SKI	SHA256 Fingerprint
5	CN = Chambers of Commerce Root, O=AC Camerfirma SA CIF A82743287, C=EU	CN = Chambers of Commerce Root, O=AC Camerfirma SA CIF A82743287, C=EU	00	rsaEncryption - 2048 bit	sha1WithRSAEncryption	Sep 30 18:13:43 2003 GMT	Sep 30 18:13:44 2037 GMT	E3:94:F5:B1:4D:E9:DB:A1:29:5B:57:8B:4D:76:06:76:E1:D1:A2:8A	0C:25:8A:12:A5:67:4A:EF:25:F2:8B:A7:DC:FA:EC:EE:A3:48:E5:41:E6:F5:CC:4E:E6:3B:71:B3:61:60:6A:C3
5.1	CN=AC Camerfirma Certificados Camerales, O=AC Camerfirma SA, C=ES	CN = Chambers of Commerce Root, O=AC Camerfirma SA CIF A82743287, C=EU	05	rsaEncryption - 2048 bit	sha1WithRSAEncryption	Feb 09 17:42:47 2004 GMT	Feb 09 17:42:47 2034 GMT	B6:1F:4E:9D:1C:68:91:2E:37:72:60:E1:46:8F:5A:A5:2A:31:31:B9	C7:D8:43:81:E1:1F:7C:57:46:77:1A:F5:B0:50:DC:51:FC:6F:DA:D6:F6:F3:5B:B5:3A:3D:E9:13:82:2E:A0:9E
5.2	CN=AC Camerfirma Express Corporate Server v3, O=AC Camerfirma SA, C=ES	CN = Chambers of Commerce Root, O=AC Camerfirma SA CIF A82743287, C=EU	0A	rsaEncryption - 2048 bit	sha1WithRSAEncryption	Jan 20 12:18:12 2009 GMT	Jan 18 12:18:12 2019 GMT	0A:4A:C0:CA:98:12:EF:97:59:DD:F7:A4:AF:B0:14:A4:39:AE:AE:4A	F3:A9:74:1B:86:72:38:87:5E:0A:3B:55:98:A3:BC:91:1D:87:56:3A:C6:EA:47:CE:F8:50:32:FF:94:8B:EA:31
5.3	CN=AC CAMERFIRMA AAPP, O=AC Camerfirma SA, C=ES	CN = Chambers of Commerce Root, O=AC Camerfirma SA CIF A82743287, C=EU	0D	rsaEncryption - 2048 bit	sha1WithRSAEncryption	Feb 23 10:46:37 2010 GMT	Feb 20 10:46:37 2022 GMT	E5:46:50:E8:43:A0:B2:F7:1C:E4:B6:FF:D8:00:04:20:F7:1F:A4:0B	83:90:E7:03:57:E9:B5:73:CA:3D:D2:9D:BD:DC:23:7E:CA:F9:36:78:2C:A3:38:9C:79:43:FB:C2:B7:FA:A0:B6
5.4	CN=AC Camerfirma TSA CA, O=AC Camerfirma SA, C=ES	CN = Chambers of Commerce Root, O=AC Camerfirma SA CIF A82743287, C=EU	12	rsaEncryption - 2048 bit	sha1WithRSAEncryption	May 19 09:20:50 2005 GMT	May 20 09:20:50 2035 GMT	BF:FA:7E:AE:B9:9D:AA:65:69:72:C6:32:16:8D:E0:10:2E:A5:9B:22	BE:A3:BC:AC:53:71:13:18:7D:05:BD:39:24:40:8F:60:00:5D:85:08:DF:F4:83:28:BC:06:E7:9A:14:B8:E4:9A
5.5	CN=AC Camerfirma Codesign v2, O=AC Camerfirma SA, C=ES	CN = Chambers of Commerce Root, O=AC Camerfirma SA CIF A82743287, C=EU	0C	rsaEncryption - 2048 bit	sha1WithRSAEncryption	Jan 20 12:20:19 2009 GMT	Jan 18 12:20:19 2019 GMT	69:1A:94:72:A0:D1:96:FF:3D:56:2A:D8:FE:2B:47:18:15:9D:B0:EE	9B:C4:F1:71:FF:9A:A2:24:F0:0C:79:9E:80:49:0E:31:01:0E:34:75:A0:8F:E6:4D:C9:A9:C4:19:2E:B0:C0:B1

Global Chambersign Root

CA#	Subject	Issuer	serialNumber	Key Type	Sig Algorithm	notBefore	NotAfter	SKI	SHA256 Fingerprint
6	CN=Global Chambersign Root, O=AC Camerfirma SA CIF A82743287, C=EU	CN=Global Chambersign Root, O=AC Camerfirma SA CIF A82743287, C=EU	00	rsaEncryption - 2048 bit	sha1WithRSAEncryption	Sep 30 18:14:18 2003 GMT	Sep 30 18:14:18 2037 GMT	43:9C:36:9F:B0:9E:30:4D:C6:CE:5F:AD:10:AB:E5:03:A5:FA:A9:14	EF:3C:B4:17:FC:8E:BF:6F:97:87:6C:9E:4E:CE:39:DE:1E:A5:FE:64:91:41:D1:02:8B:7D:11:C0:B2:29:8C:ED
6.1	CN=AC Camerfirma, O=AC Camerfirma SA, C=ES	CN=Global Chambersign Root, O=AC Camerfirma SA CIF A82743287, C=EU	02	rsaEncryption - 2048 bit	sha1WithRSAEncryption	Nov 14 15:49:08 2003 GMT	Nov 14 15:49:08 2033 GMT	70:C1:95:FA:5D:A5:16:BE:62:E8:A4:7D:E3:D4:64:5F:C4:E1:3E:9D	EF:3D:71:12:DD:3C:3C:46:A3:DC:4D:2E:01:29:21:EA:D8:3E:FC:91:5C:A6:DE:3A:CE:72:F3:91:37:5B:F0:6A
6.1.1	CN=RACER, O=AC Camerfirma SA, C=ES	CN=AC Camerfirma, O=AC Camerfirma SA, C=ES	01	rsaEncryption - 2048 bit	sha1WithRSAEncryption	Dec 04 19:26:41 2003 GMT	Dec 04 19:26:41 2023 GMT	BE:BC:08:D4:2E:BA:00:4C:80:DC:26:67:B4:A5:D8:DD:C3:4A:1A:F9	F1:71:21:77:93:5D:BA:40:BD:BD:99:C5:F7:53:31:9C:F6:29:35:49:B7:28:47:41:E4:39:16:AD:3B:FB:DD:75

MANAGEMENT ASSERTION REGARDING ITS BUSINESS PRACTICES AND CONTROLS OVER ITS CERTIFICATION AUTHORITY OPERATIONS DURING THE PERIOD FROM APRIL 14TH, 2017 THROUGH APRIL13TH, 2018

July 12th, 2018

The management of the Certification Authority AC Camerfirma, S.A (hereinafter Camerfirma) had evaluated the disclosure of the certification practices and its controls over SSL Certification Authority services through hierarchies:

- "Chambers of Commerce Root" and its 2008 and 2016 update with the corresponding Delegated Certification Authorities linked to the above "Camerfirma Corporate Server" in its different versions as defined in Annex 1 of this assertion.
- "Global ChamberSign Root" and its 2008 and 2016 update with the corresponding Representative Certification Authorities linked to the above "Global Corporate Server" in its different versions as defined in Annex 1 of this assertion.

Based on this assessment, in the opinion of Camerfirma's Management, appropriate controls regarding services SSL certification at its headquarters in Avila, Spain for the period from April 14th, 2017 and April 13th, 2018 have been designed, implemented and managed. During this period, Camerfirma has:

a) Disclosed its Certificate practices and its commitment to provide SSL Certificates in conformity with the application CA/Browser Forum Guidelines.

  - Name: CPS_eidas_EN_v_1_2_3.pdf
  - Link: https://goo.gl/jzM81N
  - Version: 1.2.3

  - Name: CPS_EN_v_3_3.pdf
  - Link: https://goo.gl/qBmG3E
  - Version: 3.3

    - PC_Chambers_of_Commerce_Root_1_0_1.pdf
    - Link: https://goo.gl/7WG3T2
    - Version: 1.0.1

    - Name: PC_Camerfirma_For_Websites.pdf
    - Link: https://goo.gl/GTBe36
    - Version: 2.0

    - Name: PC_Camerfirma_Corporate_Server_1_1_1.pdf
    - Link: https://goo.gl/G42Amh
    - Version 1.1.1

b) Maintained effective controls to provide reasonable assurance that:

- The Certificate Policy and the Certificate Practice Statement are available on a 24x7 basis and updated annually;
- Subscriber information is properly collected, authenticated (for the

registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;

- The integrity of keys and certificates that manages is established and protected throughout their life cycles;
- Logical and physical access to CA systems and data is restricted to authorized individuals;
- The continuity of key and certificate management operations is maintained; and
- CA systems development, maintenance and operations are properly authorized and performed to maintain CA systems integrity.

in accordance with the AICPA/CPA Canada of WebTrust for Certification Authorities – Baseline Requirements for SSL with network security.

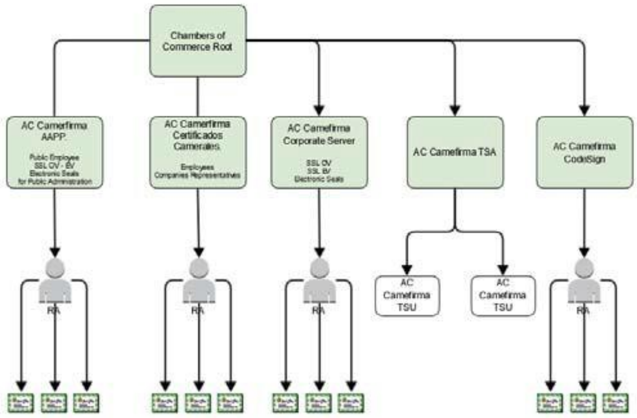
Alfonso Carcasona García
Chief Executive Officer
AC Camerfirma, S.A.

ANNEX I
STRUCTURE OF CERTIFICATION AUTHORITIES PROPERTY OF CA CAMERFIRMA S.A.

AC Camerfirma manages six hierarchical structures **(Chambers of Commerce Root JCC, Global Chambersign Root JCS, Chambers of Commerce Root - 2008 JCC-2008, Global Chambersign Root - 2008 JCS-2008, CHAMBERS OF COMMERCE ROOT – 2016 JCC-2016, GLOBAL CHAMBERSIGN ROOT – 2016 JCS-2016).**

a) Chambers of Commerce Root Hierarchy (JCC)

This hierarchy is designed to build a trusted network, where the RAs are managed by the Cámaras de Comercio, Industria y Navegación of Spain, with the primary objective of issuing digital certificates of corporate identity.



Intermediate Certification Authorities that form the hierarchy are:

a.1) Camerfirma Corporate Server

From the Root Entity (JCC) depends one intermediate Certification Authority called "Camerfirma Corporate Server" that issues two types of certificates:

- **Secure server certificates for HTML pages (OV) 1.3.6.1.4.1.17326.10.11.2 and Corporate Server EV 1.3.6.1.4.1.17326.10.14.2** these digital certificates are issued to HTML pages servers with HTTPS protocol. In this case the issuance of certificates is governed by a policy of certification subject to the requirements of the "CA/Browser Forum".
- **Electronic seal certificate for company (1.3.6.1.4.1.17326.10.11.3)**

a.2) Code Signing 1.3.6.1.4.1.17326.10.12

a.3) Timestamps 1.3.6.1.4.1.17326.10.13

a.4) AC Camerfirma Certificados Camerales.

The final certificates are addressed to:

Company membership	1.3.6.1.4.1.17326.10.9.2
Representation.	1.3.6.1.4.1.17326.10.9.3
Special empowerment	1.3.6.1.4.1.17326.10.9.5
Legal Persons	1.3.6.1.4.1.17326.10.9.4
Electronic Invoice	1.3.6.1.4.1.17326.10.9.7
Encryption	1.3.6.1.4.1.17326.10.9.6

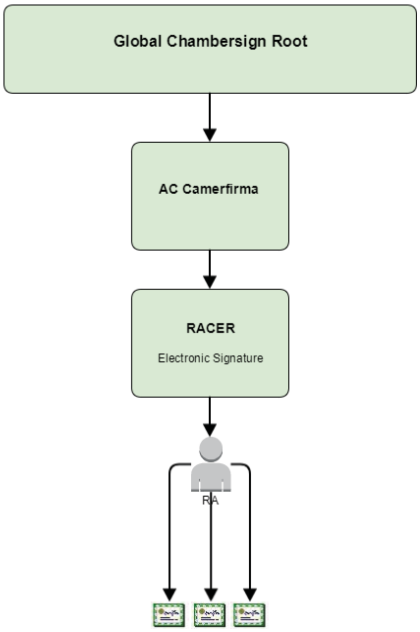
a.5) AC Camerfirma Public Administration.

Certificates issued under the Law 11/2007 of 22 June, of Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP). It establishes in Chapter II, Title Second, the mechanisms to be applied by the Public Administrations for the identification and electronic signature based on electronic certificates.
The final certificates are addressed to:

Administrative electronic site, high level.	1.3.6.1.4.1.17326.1.3.2.1
Administrative electronic site, medium level.	1.3.6.1.4.1.17326.1.3.2.2
Electronic Seal for Automated Performance, high level.	1.3.6.1.4.1.17326.1.3.3.1
Electronic Seal for Automated Performance, medium level.	1.3.6.1.4.1.17326.1.3.3.2
Public Employee, high level, signature	1.3.6.1.4.1.17326.1.3.4.1
Public Employee, high level, authentication	1.3.6.1.4.1.17326.1.3.4.2
Public Employee, high level, encryption	1.3.6.1.4.1.17326.1.3.4.3
Public Employee, medium level	1.3.6.1.4.1.17326.1.3.4.4

b) Chambersign Global ROOT Hierarchy (JCS)

This hierarchy is created for the issuance of certificates where the Registry Authorities do not belong to the scope of the Chambers of Commerce, or where the certification policies require that the certificates issued are business oriented.



b.1) AC Camerfirma (Spain).

The first intermediate certification authority corresponds to CA Camerfirma (Spain) whose function is to issue certificates in the Spanish regulatory framework.

b.1.a) RACER (**R**ed de **A**lta **C**apilaridad de **E**ntidades de **R**egistro), whose main feature is that it can use any agent as a Registration Authority, as long as the RA has previously received the proper training and it has been audited to verify that the RA is able to apply properly the "obligations" stipulated in the relevant Certification Policies.

RACER is a general-purpose multi-policy AC not applied to any particular sector that issues end-entity certificates.

The final certificates are addressed to:

Legal Person of Linkage Certificate - belonging	1.3.6.1.4.1.17326.10.8.2

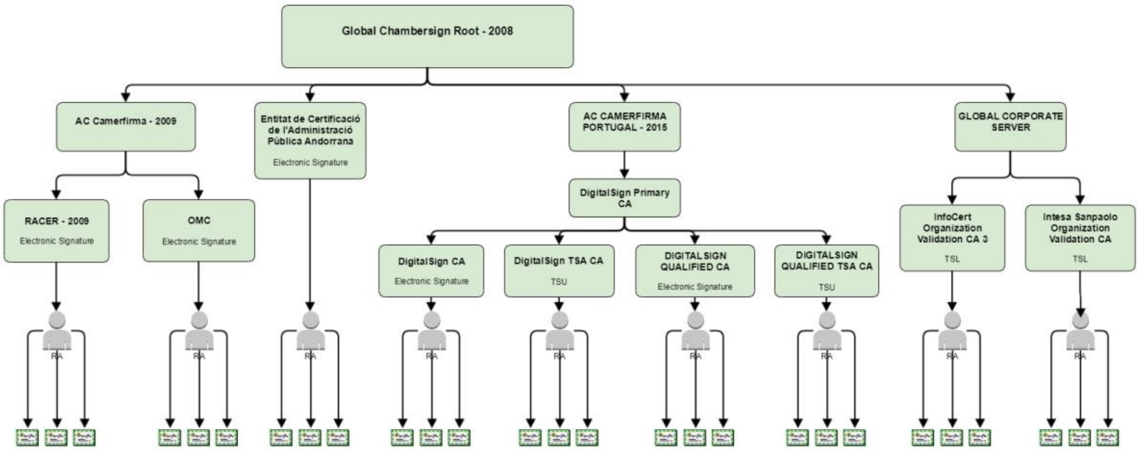
Legal Person of Linkage Certificate - representation	1.3.6.1.4.1.17326.10.8.3
Legal Person Certificate	1.3.6.1.4.1.17326.10.8.4
Electronic Seal Certificate	1.3.6.1.4.1.17326.10.8.5
Legal Person Certificate - Entrepreneur Citizen	1.3.6.1.4.1.17326.10.8.6
Legal Person Certificate - Linking Electronic Invoice.	1.3.6.1.4.1.17326.10.8.7
Legal Person Certificate - Linking Bonding Agent	1.3.6.1.4.1.17326.10.8.8
Legal Person Certificate - Encryption	1.3.6.1.4.1.17326.10.8.9

c) Chambers of Commerce Root – 2008 Hierarchy (JCC-2008)

This Hierarchy is identical to the **Chambers of Commerce Root Hierarchy (JCC)** and is intended to replace the latter.

d) Chambersign Global Root – 2008 Hierarchy (JCS-2008)

This hierarchy is created for the issuance of certificates where the Registry Authorities do not belong to the scope of the Chambers of Commerce, or where the certification policies require that the certificates issued are business oriented.



d.1) AC Camerfirma (Spain).

The first intermediate certification authority corresponds to AC Camerfirma (Spain) whose function is to issue certificates in the Spanish regulatory framework.

d.1.a) RACER (**R**ed de **A**lta **C**apilaridad de **E**ntidades de **R**egistro), whose main feature is that it can use any agent as a Registration Authority, as long as the RA has previously received the proper training and it has been audited to verify that the RA is able to apply properly the "obligations" stipulated in the relevant Certification Policies.

RACER is a general-purpose multi-policy AC not applied to any particular sector that issues end-entity certificates.

The final certificates are addressed to:

Legal Person of Linkage Certificate - belonging	1.3.6.1.4.1.17326.10.8.2
Legal Person of Linkage Certificate - representation	1.3.6.1.4.1.17326.10.8.3
Legal Person Certificate	1.3.6.1.4.1.17326.10.8.4
Electronic Seal Certificate	1.3.6.1.4.1.17326.10.8.5
Legal Person Certificate - Entrepreneur Citizen	1.3.6.1.4.1.17326.10.8.6
Legal Person Certificate - Linking Electronic Invoice.	1.3.6.1.4.1.17326.10.8.7

Legal Person Certificate - Linking Bonding Agent	1.3.6.1.4.1.17326.10.8.8
Legal Person Certificate - Encryption	1.3.6.1.4.1.17326.10.8.9

d.2.b) CA of Organización Médica Colegial

Out of scope.

d.3) Entidad de Certificación de la Administración Pública Andorrana.

Out of scope.

d.4) AC CAMERFIRMA PORTUGAL - 2015.

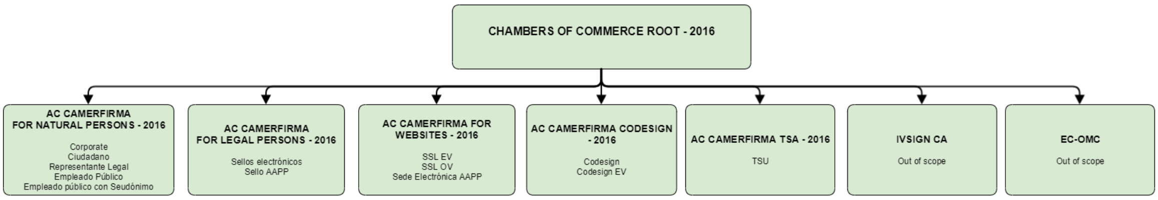
Out of scope.

d.5) GLOBAL CORPORATE SERVER

Out of scope.

e) CHAMBERS OF COMMERCE ROOT – 2016 Hierarchy (JCC-2016)

This hierarchy is designed to build a trusted network, where the RAs are managed by the Cámaras de Comercio, Industria y Navegación of Spain, with the primary objective of issuing digital certificates of corporate identity. This hierarchy is intended to replace the **JCC** and **JCC-2008** hierarchies.


CHAMBERS OF COMMERCE ROOT - 2016
AC CAMERFIRMA FOR NATURAL PERSONS - 2016
Corporate
Ciudadano
Representante Legal
Empleado Público
Empleado público con Seudónimo
AC CAMERFIRMA FOR LEGAL PERSONS - 2016
Sellos electrónicos
Sello AAPP
AC CAMERFIRMA FOR WEBSITES - 2016
SSL EV
SSL OV
Sede Electrónica AAPP
AC CAMERFIRMA CODESIGN - 2016
Codesign
Codesign EV
AC CAMERFIRMA TSA - 2016
TSU
IVSIGN CA
Out of scope
EC-OMC
Out of scope

Intermediate Certification Authorities that form the hierarchy are:

e.1) AC CAMERFIRMA FOR LEGAL PERSONS

From the Root Entity (JCC-2016) depends one intermediate Certification Authority called "**AC CAMERFIRMA FOR LEGAL PERSONS - 2016**".

The final certificates are addressed to:

Qualified Certificate of Electronic Seal in QSCD	1.3.6.1.4.1.17326.10.16.2.1.1
Qualified Certificate of Electronic Seal	1.3.6.1.4.1.17326.10.16.2.1.2
Electronic Seal Certificate	1.3.6.1.4.1.17326.10.16.2.3.2
Electronic Seal Certificate. High Level.	1.3.6.1.4.1.17326.10.16.2.2.1.3.3.1
Electronic Seal Certificate. Medium Level.	1.3.6.1.4.1.17326.10.16.2.2.1.4.3.1

e.2) AC CAMERFIRMA FOR NATURAL PERSONS

From the Root Entity (JCC-2016) depends one intermediate Certification Authority called "**AC CAMERFIRMA FOR NATURAL PERSONS - 2016**".

The final certificates are addressed to:

Qualified Citizen Certificate in QSCD	1.3.6.1.4.1.17326.10.16.1.1.1
Qualified Citizen Certificate	1.3.6.1.4.1.17326.10.16.1.1.2
Qualified Corporate Certificate in QSCD	1.3.6.1.4.1.17326.10.16.1.2.1
Qualified Corporate Certificate	1.3.6.1.4.1.17326.10.16.1.2.2
Qualified Certificate of Representative of Legal Person with General Representation Powers in QSCD	1.3.6.1.4.1.17326.10.16.1.3.1.1
Qualified Certificate of Representative of Legal Person with General Representation Powers	1.3.6.1.4.1.17326.10.16.1.3.1.2
Qualified Certificate of Representative of Entity Without Legal Personality with General Representation Powers in QSCD	1.3.6.1.4.1.17326.10.16.1.3.1.1
Qualified Certificate of Representative of Entity Without Legal Personality with General Representation Powers	1.3.6.1.4.1.17326.10.16.1.3.1.2
Qualified Certificate of Representative of Legal Person for Procedures with Public Authorities in QSCD	1.3.6.1.4.1.17326.10.16.1.3.2.1
Qualified Certificate of Representative of Legal Person for Procedures with Public Authorities	1.3.6.1.4.1.17326.10.16.1.3.2.2
Qualified Certificate of Representative of Entity Without Legal Personality for Procedures with Public Authorities in QSCD	1.3.6.1.4.1.17326.10.16.1.3.2.1
Qualified Certificate of Representative of Entity Without Legal Personality for Procedures with Public Authorities	1.3.6.1.4.1.17326.10.16.1.3.2.2
Qualified Certificate of Representative of Legal Person for Proxies in QSCD	1.3.6.1.4.1.17326.10.16.1.3.3.1
Qualified Certificate of Representative of Legal Person for Proxies	1.3.6.1.4.1.17326.10.16.1.3.3.2
Qualified Certificate of Representative of Entity Without Legal Personality for Proxies in QSCD	1.3.6.1.4.1.17326.10.16.1.3.3.1
Qualified Certificate of Representative of Entity Without Legal Personality for Proxies	1.3.6.1.4.1.17326.10.16.1.3.3.2
Qualified Certificate of Public Employee for Signature. High Level.	1.3.6.1.4.1.17326.10.16.1.5.1.3.4.1
Qualified Certificate of Public Employee for Authentication. High Level.	1.3.6.1.4.1.17326.10.16.1.5.1.3.4.2
Qualified Certificate of Public Employee for Encryption. High Level.	1.3.6.1.4.1.17326.10.16.1.5.1.3.4.3
Qualified Certificate of Public Employee. Medium Level.	1.3.6.1.4.1.17326.10.16.1.5.1.3.4.4
Qualified Certificate of Public Employee with Pseudonym for Signature. High Level.	1.3.6.1.4.1.17326.10.16.1.5.1.3.4.1
Qualified Certificate of Public Employee with Pseudonym for Authentication. High Level.	1.3.6.1.4.1.17326.10.16.1.5.1.3.4.2
Qualified Certificate of Public Employee with Pseudonym for Encryption. High Level.	1.3.6.1.4.1.17326.10.16.1.5.1.3.4.3
Qualified Certificate of Public Employee with Pseudonym. Medium Level.	1.3.6.1.4.1.17326.10.16.1.5.1.3.4.4

e.3) AC CAMERFIRMA FOR WEBSITES

From the Root Entity (JCC-2016) depends one intermediate Certification Authority called "**AC CAMERFIRMA FOR WEBSITES - 2016**".

The final certificates are addressed to:

OV Website Certificate	1.3.6.1.4.1.17326.10.16.3.2.2
Qualified Certificate of EV Website	1.3.6.1.4.1.17326.10.16.3.4.2
Administrative Electronic Site. High Level. EV	1.3.6.1.4.1.17326.10.16.3.6.1.3.2.1
Administrative Electronic Site. Medium Level. EV	1.3.6.1.4.1.17326.10.16.3.6.1.3.2.2

e.4) AC CAMERFIRMA CODESIGN

From the Root Entity (JCC-2016) depends one intermediate Certification Authority called "**AC CAMERFIRMA CODESIGN - 2016**".

The final certificates are addressed to:

Code Signing Certitficate in QSCD	1.3.6.1.4.1.17326.10.16.4.1.1
Code Signing Certificate	1.3.6.1.4.1.17326.10.16.4.1.2
EV Code Signing Certitficate in QSCD	1.3.6.1.4.1.17326.10.16.4.2.1

e.5) AC CAMERFIRMA TSA

From the Root Entity (JCC-2016) depends one intermediate Certification Authority called "**AC CAMERFIRMA TSA - 2016**".

The final certificates are addressed to:

Qualified TSU Certificate in QSCD	1.3.6.1.4.1.17326.10.16.5.1.1
TSU Certificate	1.3.6.1.4.1.17326.10.16.5.1.2

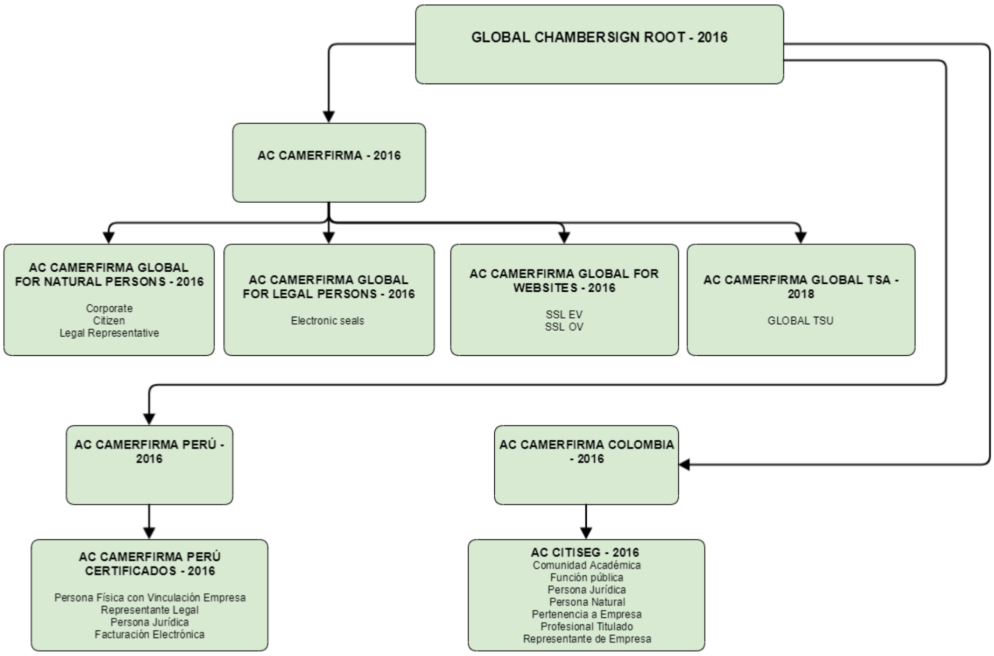
e.6) IVSIGN CA

Out of scope.

e.7) EC-OMC

Out of scope.

f) GLOBAL CHAMBERSIGN ROOT – 2016 Hierarchy (JCS-2016)


GLOBAL CHAMBERSIGN ROOT - 2016
AC CAMERFIRMA - 2016
AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016
Corporate
Citizen
Legal Representative
AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016
Electronic seals
AC CAMERFIRMA GLOBAL FOR WEBSITES - 2016
SSL EV
SSL OV
AC CAMERFIRMA GLOBAL TSA - 2018
GLOBAL TSU
AC CAMERFIRMA PERÚ - 2016
AC CAMERFIRMA COLOMBIA - 2016
AC CAMERFIRMA PERÚ CERTIFICADOS - 2016
Persona Física con Vinculación Empresa
Representante Legal
Persona Jurídica
Facturación Electrónica
AC CITISEG - 2016
Comunidad Académica
Función pública
Persona Jurídica
Persona Natural
Pertenencia a Empresa
Profesional Titulado
Representante de Empresa

This hierarchy is designed to build a trusted network, where the RAs are managed by entities outside the scope of the Cámaras de Comercio, Industria y Navegación of Spain, with the primary objective of issuing digital certificates of corporate identity. This hierarchy is intended to replace the **JCS** and **JCS-2008** hierarchies.

Intermediate Certification Authorities that form the hierarchy are:

f.1) AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS

From the Root Entity (JCS-2016) depends one intermediate Certification Authority called "**AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016**".

The final certificates are addressed to:

Electronic Seal Certificate in QSCD	1.3.6.1.4.1.17326.20.16.1.2.1.1.1
Electronic Seal Certificate	1.3.6.1.4.1.17326.20.16.1.2.1.1.2

f.2) AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS

From the Root Entity (JCS-2016) depends one intermediate Certification Authority called "**AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016**".

The final certificates are addressed to:

Citizen Certificate in QSCD	1.3.6.1.4.1.17326.20.16.1.1.1.1
Citizen Certificate	1.3.6.1.4.1.17326.20.16.1.1.1.2
Corporate Certificate in QSCD	1.3.6.1.4.1.17326.20.16.1.1.2.1
Corporate Certificate	1.3.6.1.4.1.17326.20.16.1.1.2.2
Certificate of Representative of Legal Person in QSCD	1.3.6.1.4.1.17326.20.16.1.1.3.1.1
Certificate of Representative of Legal Person	1.3.6.1.4.1.17326.20.16.1.1.3.1.2
Certificate of Representative of Entity Without Legal Personality in QSCD	1.3.6.1.4.1.17326.20.16.1.1.3.2.1
Certificate of Representative of Entity Without Legal Personality	1.3.6.1.4.1.17326.20.16.1.1.3.1.2

f.3) AC CAMERFIRMA GLOBAL FOR WEBSITES

From the Root Entity (JCS-2016) depends one intermediate Certification Authority called "**AC CAMERFIRMA GLOBAL FOR WEBSITES - 2016**".

The final certificates are addressed to:

EV Website Certificate	1.3.6.1.4.1.17326.10.8.12.1.2

f.4) AC CAMERFIRMA GLOBAL TSA

From the Root Entity (JCS-2016) depends one intermediate Certification Authority called "**AC CAMERFIRMA GLOBAL TSA - 2018**".

The final certificates are addressed to:

GLOBAL TSU certificate	1.3.6.1.4.1.17326.20.16.1.3.1

f.5) AC CAMERFIRMA COLOMBIA

From the Root Entity (JCS-2016) depends one intermediate Certification Authority called "**AC CAMERFIRMA COLOMBIA - 2016**" and then **"AC CITISEG – 2016"**.

The final certificates are addressed to:

Certificate for Academic Community	1.3.6.1.4.1.17326.20.1.1.2
Certificate for Public Function	1.3.6.1.4.1.17326.20.1.2.2
Certificate for Legal Person	1.3.6.1.4.1.17326.20.1.3.2
Certificate for Natural Person	1.3.6.1.4.1.17326.20.1.4.2
Corporate Certificate	1.3.6.1.4.1.17326.20.1.5.2
Certificate for Professional Title	1.3.6.1.4.1.17326.20.1.6.2
Certificate of Representative of Legal Person	1.3.6.1.4.1.17326.20.1.7.2

f.6) AC CAMERFIRMA PERÚ

From the Root Entity (JCS-2016) depends one intermediate Certification Authority called "**AC CAMERFIRMA PERÚ - 2016**" and then **"AC CAMERFIRMA PERÚ CERTIFICADOS – 2016"**.

The final certificates are addressed to:

Corporate Certificate	1.3.6.1.4.1.17326.30.16.0.1
Certificate of Representative of Legal Person	1.3.6.1.4.1.17326.30.16.10.1
Certificate for Legal Person	1.3.6.1.4.1.17326.30.16.20.1
Certificate for Electronic Invoice	1.3.6.1.4.1.17326.30.16.30.1
Certificate for Natural Person	1.3.6.1.4.1.17326.30.16.40.1
Electronic Seal Certificate	1.3.6.1.4.1.17326.30.16.50.1