

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", "CHAMBERS OF COMMERCE ROOT - 2016" and "GLOBAL CHAMBERSIGN ROOT - 2016" as detailed in Appendix 1, Camerfirma has:

- disclosed its extended validation SSL ("EV SSL") certificate lifecycle management business practices in its:
 - CERTIFICATION PRACTICES STATEMENT DIGITAL CERTIFICATES AC CAMERFIRMA SA EIDAS - 2016- Version 1.2.4
http://docs.camerfirma.com/publico/DocumentosWeb/politicas/CPS_eidas_1.2.4_EN.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
 - CERTIFICATION POLICY CAMERFIRMA CORPORATE SERVER EV – Version 1.0.1
http://docs.camerfirma.com/publico/DocumentosWeb/politicas/PC_Camerfirma_Corporate_Server_EV_1_0_1.pdf

including its commitment to provide EV SSL certificates in conformity with the CA/Browser Forum Guidelines 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 EV SSL certificates it manages is established and protected throughout their lifecycles; and
 - EV SSL subscriber information is properly authenticated (for the registration activities performed by Camerfirma)

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.6.

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 – Extended Validation SSL v1.6.

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 EV SSL certificate lifecycle management business practices including its relevant controls over the issuance, renewal, and revocation of EV SSL certificates;
- (2) selectively testing transactions executed in accordance with disclosed EV 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 Camerfirma had issued certificates with errors according to the CA/B Forum requirements. Specifically:

- Certificates with commonName that is not in Subject Alternative Name
- Duplicate SAN entry
- Certificates without businessCategory
- Certificates without Country
- Certificates without jurisdictionCountryName

This caused WebTrust Criterion 2.2.1 of Principle 2 which reads:

The CA maintains controls to provide reasonable assurance that EV SSL certificates issued meet the minimum requirements for Certificate Content and Profile, including additional technical requirements as specifically established in section 9 of the EV SSL Guidelines, including the following:

- *Issuer Common Name Field*
- *Issuer Domain Component Field*
- *Issuer Organization Name Field*
- *Issuer Country Name Field*
- *Full legal organization name and if space is available the d/b/a name may also be disclosed*
- *Subject Alternative Name Extension*
- *Subject Common Name Field*
- *Subject Business Category Field*
- *Subject Jurisdiction of Incorporation or Registration Field*
- *Subject Registration Number Field*
- *Subject Physical Address of Place of Business Field*
- *Other Subject Attributes*

to not be met.



During our procedures, we noted that certificate status information was inconsistent between the OCSP and CRL service under certain circumstances. Specifically:

- The revocation time differs between the OCSP service and CRL for a few certificates.
- The OCSP service responds good for some certificates revoked according to the CRL.

This caused WebTrust Criterion 5.5 of Principle 2 which reads:

The CA maintains controls to provide reasonable assurance that the CA:

- *makes revocation information available via the cRLDistributionPoints and/or authorityInformationAccess certificate extensions for Subordinate CA and Subscriber Certificates in accordance with the SSL Baseline Requirements Section 7.1.2; and*
- *for high-traffic FQDNs, distributes its OCSP responses in accordance with SSL Baseline Requirements.*

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 5.1 of Principle 2 which reads:

The CA maintains controls to provide reasonable assurance that a process is available 24x7 that the CA is able to accept and respond to revocation requests and related inquiries, and that the CA provides a process for Subscribers to request revocation of their own 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.

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 – Extended Validation SSL v1.6.

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 – Extended Validation SSL v1.6, nor the suitability of any of Camerfirma's services for any customer's intended purpose.

A handwritten signature in blue ink, appearing to be "F. Mondragon".

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	sha256WithRSAEncryption	April 14 093548 2016 GMT	April 08 093548 2040 GMT	9E2E654F3E57F5AB7D96C68BDFB3356D4AE89E8B	04F1BEC36951BC1454A904CE32890C5DA3CDE1356B7900F6E2DFA2041EBAD51
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	sha256WithRSAEncryption	April 14 103307 2016 GMT	March 09 103307 2040 GMT	C3278593D72F96C51BAC7633D986A2A47D681442	3A8066266D28BD28CCD0F564C8FBC1219B4FFAE403E01E5039D30F2400F0EB09
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	sha256WithRSAEncryption	April 14 104809 2016 GMT	March 09 104809 2040 GMT	70B8F824C751CACE22809208C9C0682FC1475851	EEDD457AF1353D76F48E7C6123F39140E5F9A069CA51B43EEA8615C9CEC0D4BB
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	sha256WithRSAEncryption	Apr 18 174354 2016 GMT	March 13 174354 2040 GMT	EC95333B71C0D2B19C58230B3641BC549E2C921D	937D7D5D0B7FB7DB039399BC0B670CC203C7AB4E332FAE453CC38EC188DDEA2B
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	454A8B1B4E135F2	rsaEncryption - 4096 bit	sha256WithRSAEncryption	Apr 14 101754 2016 GMT	March 09 101754 2040 GMT	A7254A064EE5609040E49E72259885EA3CDFFA92	4908F2337567BE505C26CC01A7F07C4B802132A095B2BAEEEE6DE20883088A56
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	sha256WithRSAEncryption	Apr 14 124209 2016 GMT	March 09 121209 2040 GMT	1E6DB5C63FEF9255E537FADBF10AABAD93B4E2C	BAAE2C6338857D50200F6F73DD45E65AA2D895BED4675B6E396B7222E018A9B8

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	sha256WithRSAEncryption	Apr 14 095006 2016 GMT	Apr 08 095006 2040 GMT	E89BCD7E86629B7A4D8C00973985CF1C7890703A	C1D80CE474A51128B77E794A98AA2D62A0225DA3F419E5C7ED73DFBF660E7109
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	sha256WithRSAEncryption	Apr 14 132349 2016 GMT	March 09 132349 2040 GMT	D28497444DD988EE7C25BF5280B329489B8B1884	371C57982CF543FBF9041EDC348A2E0ACDCDE4B6EC25EC242BAC84F01DAB181C
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	sha256WithRSAEncryption	Apr 14 171334 2016 GMT	Feb 08 171334 2040 GMT	4E3656A858CE1B8385604CD41BA1DF723DAF7B5F	EF411C837AC3304185E53913FE369BF8FF6598C2A52BDB1B6E2DEAB5DCC7F06F
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	sha256WithRSAEncryption	Apr 14 165836 2016 GMT	Feb 08 165836 2040 GMT	8021DF71F1EFD46BDA3386D10FBEC5DD654C845E	4D20C951E134893BC5901BFAF8E240A5BE7D00596DD31C40429252F2E04F8B46
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	sha256WithRSAEncryption	Apr 18 175756 2016 GMT	Feb 12 175756 2040 GMT	F435D1DAFDFEA41106C62C3CC2FF9CFA89910F6A	99BDA6792DCAED7145BF9B7F466831051821AEF03216971176241AFC2123AB84



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 142950 2008 GMT	July 31 142950 2038 GMT	F924AC0FB2B5F879C0FA60881BC4D94D029E1719	063E4AFAC491DFD332F3089B8542E94617D893D7FE944E10A7937EE29D9693C0
3.1	CN=Camerfirma Certificados Camerale - 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 194020 2009 GMT	March 14 194020 2019 GMT	1EC45A8A846F119058B3E209D716E6EAC324E68D	2F2B32E78FC69D2FFC645EB6068E074E749774495FDC251093B0EEE04EFAFD17
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	sha256WithRSAEncryption	January 15 112116 2015 GMT	December 15 112116 2037 GMT	63E9F0F056006865B0216C0E5CD719089D083465	66EAE2709B54CDD1693177B1332FF036CDD0F723DB3039ED311555A6CBF5FF3E
3.3	CN=Camerfirma AAPF 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	sha256WithRSAEncryption	Dec 16 135901 2017 GMT	Dec 15 135901 2037 GMT	5DA155A4DC4AAC8311F9AA38E5F7684AFE15154C	7239D2F770FAFF3B1CF8BE2A05EC03EDEAAC053B554F90D36921155BA8051981
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 194526 2009 GMT	March 14 194526 2019 GMT	0E314D5DE9E1C25C5BBCF52B05BAAF470D16ABDC	4C2512B5DBC0D354C7214250B8256D4BFB608941969B8D89C4215021E0B2B905
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	sha256WithRSAEncryption	Dec 16 164533 2014 GMT	Dec 15 164533 2037 GMT	17C540BC2AF845B8AB33BFF86F496CF617CAB7D4	65695D500117FD7270F1027ED121F05942670075461D337EEEC7F6A5B757A47A

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 143140 2008 GMT	July 31 143140 2038 GMT	B909CA9C1EDBD36C3A6BAEED54F15B9306352E5E	136335439334A7698016A0D324DE72284E079D7B5220BB8FBD747816EEBEBACA
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 191625 2009 GMT	March 11 191625 2029 GMT	C8000FFCC652FC9FDB3B642E32B96E2E71F36579	B68D5D9B4EA635957C0C3215C20D35B2217B69E349C7A304C4F97F20C4081F88
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 124709 2009 GMT	March 23 124709 2019 GMT	AC16D710D16F75F6848868E644251172CAB31B80	47CFDEE37609725CFF037B56A071C43AA05869A84428A5D861FF92B9450292AA

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 181343 2003 GMT	Sep 30 181344 2037 GMT	E394F5B14DE9DBA1295B578B4D760676E1D1A28A	0C258A12A5674AEF25F28BA7DCFAECEEA348E541E6F5CC4EE63B71B361606AC3
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 174247 2004 GMT	Feb 09 174247 2034 GMT	B61F4E9D1C68912E377260E1468F5AA52A3131B9	C7D84381E11F7C5746771AF5B050DC51FC6FDAD6F6F35BB53A3DE913822EA09E
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 121812 2009 GMT	Jan 18 121812 2019 GMT	0A4AC0CA9812EF9759DDF7A4AFB014A439AEAE4A	F3A9741B867238875E0A3B5598A3BC911D87563AC6EA47CEF85032FF948BEA31
5.3	CN=AC CAMERFIRMA AAPF, 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 104637 2010 GMT	Feb 20 104637 2022 GMT	E54650E843A0B2F71CE4B6FFD8000420F71FA40B	8390E70357E9B573CA3DD29DBDDC237ECAF936782CA3389C7943FBC2B7FAA0B6
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 092050 2005 GMT	May 20 092050 2035 GMT	BFFA7EAE99DAA656972C632168DE0102EA59B22	BEA3BCAC537113187D05BD3924408F60005D8508DFF48328BC06E79A14B8E49A
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 122019 2009 GMT	Jan 18 122019 2019 GMT	691A9472A0D196FF3D562AD8FE2B4718159DB0EE	9BC4F171FF9AA224F00C799E80490E31010E3475A08FE64DC9A9C4192EB0C0B1

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 181418 2003 GMT	Sep 30 181418 2037 GMT	439C369FB09E304DC6CE5FAD10ABE503A5FAA914	EF3CB417FC8EBF6F97876C9E4ECE39DE1EA5FE649141D1028B7D11C0B2298CED
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 154908 2003 GMT	Nov 14 154908 2033 GMT	70C195FA5DA516BE62E8A47DE3D4645FC4E13E9D	EF3D7112DD3C3C46A3DC4D2E012921EAD83EFC915CA6DE3ACE72F391375BF06A
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 192641 2003 GMT	Dec 04 192641 2023 GMT	BEBC08D42EBA004C80DC2667B4A5D8DDC34A1AF9	F1712177935DBA40BDBD99C5F753319CF6293549B7284741E43916AD3BFBD75

**MANAGEMENT ASSERTION REGARDING ITS BUSINESS PRACTICES AND CONTROLS
OVER ITS CERTIFICATION AUTHORITY OPERATIONS DURING THE PERIOD FROM
APRIL 14TH, 2017 THROUGH APRIL 13TH, 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

- PC_Camerfirma_Corporate_Server_EV_1_0_1.pdf
- Link: <https://goo.gl/tycnG3>
- Version 1.0.1

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 – Extended Validation Requirements for SSL with network security.

A handwritten signature in black ink, appearing to be 'Alfonso Carcasona García', written in a cursive style.

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

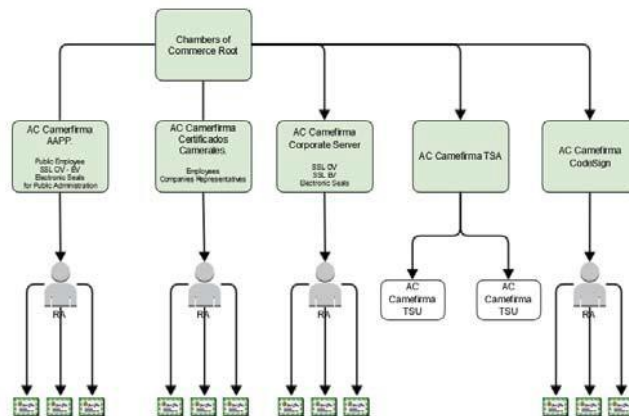
ANNEX I

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.

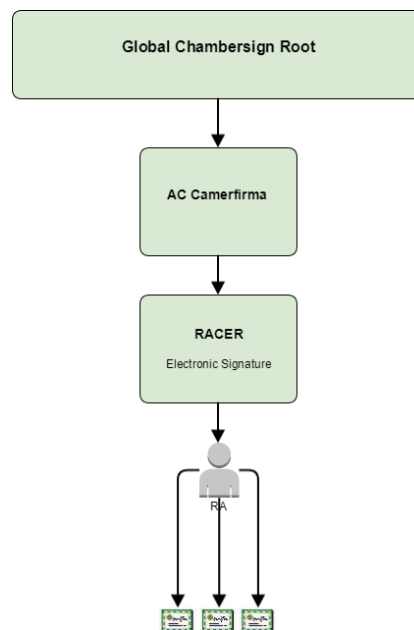
Certificates issued under the Law 11/2007 of 22 June, of Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP). It establishes in Chapter II, Title Second, the mechanisms to be applied by the Public Administrations for the identification and electronic signature based on electronic certificates.

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 (Red de Alta Capilaridad de Entidades de Registro), 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
---	--------------------------

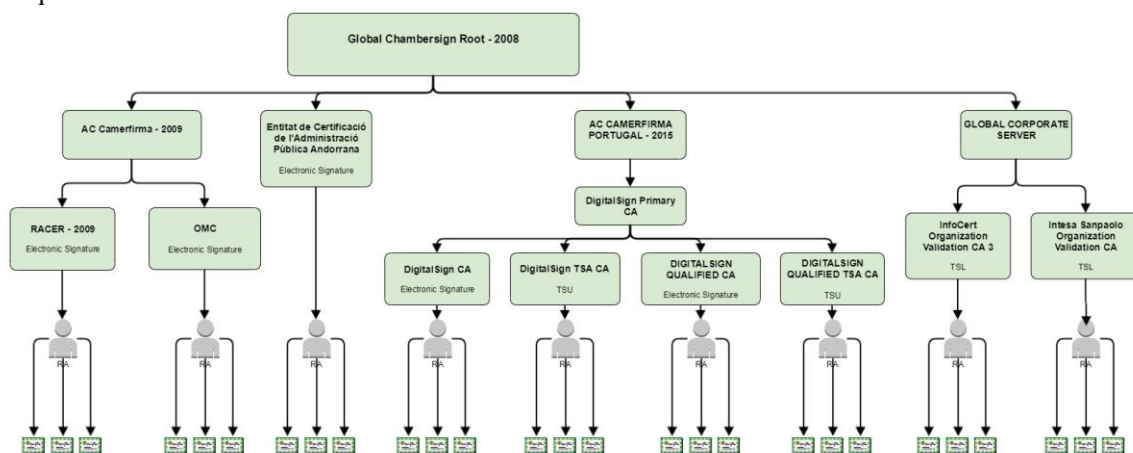
Legal Person of Linkage Certificate - representation	1.3.6.1.4.1.17326.10.8.3
Legal Person Certificate	1.3.6.1.4.1.17326.10.8.4
Electronic Seal Certificate	1.3.6.1.4.1.17326.10.8.5
Legal Person Certificate - Entrepreneur Citizen	1.3.6.1.4.1.17326.10.8.6
Legal Person Certificate - Linking Electronic Invoice.	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 (ICC-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 (Red de Alta Capilaridad de Entidades de Registro), 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.

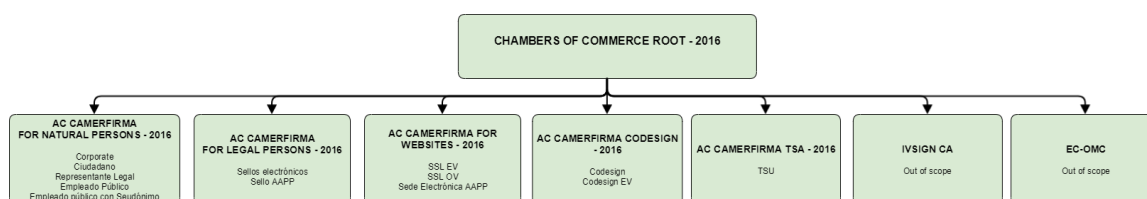
Out of scope.

d.5) GLOBAL CORPORATE SERVER

Out of scope.

e) CHAMBERS OF COMMERCE ROOT - 2016 Hierarchy (ICC-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.



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 Certificate 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 Certificate 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

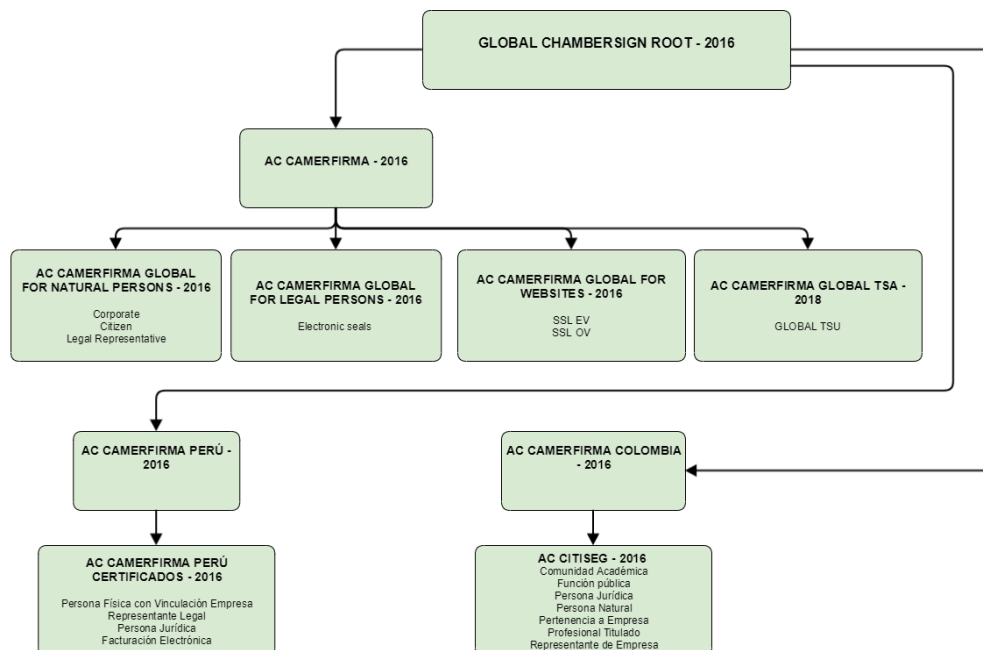
e.6) IVSIGN CA

Out of scope.

e.7) EC-OMC

Out of scope.

f) GLOBAL CHAMBERSIGN ROOT - 2016 Hierarchy (ICS-2016)



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