AENOR

Appendix to the Certificate of Trust Service Provider

PSC- 2018/0001

The Conformity Assessment Body, AENOR INTERNACIONAL SAU, issues this appendix to certificate number PSC-2018/0001 to the organization:

AC CAMERFIRMA S.A.

to confirm that its trust service:	Certificate for website authentication
provided at:	Jorge Juan, 106. Madrid 28009
complies with the requirements defined in standard:	ETSI EN 319 411-1 v1.2.2
First issuance date:	2019-03-28
Updating date:	2019-03-30
Expiration date:	2020-03-28

This appendix to the certificate is valid only in its entirety (7 pages).

Rafael GARCÍA MEIRO
Director General
30-03-2019

AENOR INTERNACIONAL, S.A.U.
Génova, 6. 28004 Madrid. España
Tel. 91 432 60 00.- www.aenor.com
Accredited CAB

Appendix to the Certificate for Trust Service Provider: PSC-2018/0001

Assessment criteria

The assessment criteria are defined in standard ETSI EN 319 411-1:

- ETSI EN 319 411-1 V1.2.2 (2018-04): "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements", Version 1.2.2, 2018-04, European Telecommunications Standards Institute

The applicable ETSI Certification Policies are:

- OVCP: Organizational Validation Certificates Policy
- EVCP: Extended Validation Certificates Policy

Audit period

The Audit was carried out at the TSP sites in Madrid (Spain) between February 18st, 2019 (2019-02-18) and February 22th, 2019 (2019-02-22) with additional checks performed until March 8th, 2019 (2019-03-08).

The audit was carried out as a period audit and covered the period from the May 8th, 2018 (2018-05-08) until March 28th, 2019 (2019-03-28)

Assessment scope

The scope of the assessment includes the following CA certificates:

Root CAs
1. Chambers of Commerce Root - 2008
4. CHAMBERS OF COMMERCE ROOT 2018
OV SSL Issuing CAs
2. Camerfirma AAPP II - 2014
3. Camerfirma Corporate Server II – 2015
5. AC CAMERFIRMA FOR WEBSITES 2018
EV SSL Issuing CAs
3. Camerfirma Corporate Server II - 2015

*See Appendix A

together with the Certificate Practice Statement (CPS) and Certificate Policies (CP):

- DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN CERTIFICADOS DIGITALES AC CAMERFIRMA SA Versión 3.3.4
- POLÍTICA DE CERTIFICACIÓN CAMERFIRMA CORPORATE SERVER EV Versión 1.0.2
- POLÍTICA DE CERTIFICACIÓN CAMERFIRMA EXPRESS CORPORATE SERVER Versión 1.1.2

for the following *Object Identifier* (OID) of the certificates:

- 1.3.6.1.4.1.17326.1.3.2.2 - OVCP (Camerfirma AAPP II - 2014)
- 1.3.6.1.4.1.17326.10.16.3.2.2 - OVCP (AC CAMERFIRMA FOR WEBSITES 2018)
- 1.3.6.1.4.1.17326.10.16.3.2.2 - OVCP (AC CAMERFIRMA FOR WEBSITES - 2016)
- 1.3.6.1.4.1.17326.10.11.2.1 - OVCP (Camerfirma Corporate Server II - 2015)
- 1.3.6.1.4.1.17326.10.14.2.1.2 - EVCP (Camerfirma Corporate Server II - 2015)

Assessment results

In our opinion, based on the Audit work for the Audit period, the assessment scope complies in all material aspects with the assessment criteria mentioned above with the exceptions noted in the following section. This appendix to the certificate is subject to a comprehensive follow-up Audit prior to January 2020.

This report does not include any representation as to the quality of the Trust Service Provider services beyond the assessment criteria covered, nor the suitability of any of Trust Service Provider services for any customer's intended purpose.

Summary of the Audit requirements

The ETSI specification contains the following:

5.1 General requirements

Compliance

5.2 Certification Practice Statement requirements

Compliance

5.3 Certificate Policy name and identification

Compliance

5.4 PKI participants

Compliance

6.1 Publication and repository responsibilities

Compliance.

6.2 Identification and authentication

Compliance

6.3 Certificate Life-Cycle operational requirements

Compliance.

6.4 Facility, management, and operational controls

Compliance with findings.

#1 We found no evidence that there is a security policy communication procedure for third-parties. The entity has provided no evidence either that the entity's security policies have

been communicated to third-parties in the past. Furthermore, no evidence was found to obtain sufficient assurance that the entity is monitoring the third-partie's adherence to Camerfirma security policy and controls.

#2 The logs of the different systems and applications are stored in a syslog server. Additionally, some of these logs are also stored on tape by the Datacenter provider. However, evidence was found that most of these logs are being stored without hashing, so their integrity cannot be guaranteed, which is a breach of the procedure "IN-2005-04-10 Log Management" from Camerfirma, which indicates that backup files containing logs shall include their fingerprint (SHA-2) in all cases.

Finally, there was evidence that the five-year retention period indicated in Camerfirma's "IN-2005-04-10 Log Management" procedure is not being implemented in all cases.

Furthermore, this retention period is not aligned with the ETSI EN 319 411-1 standard, which indicates that the logs of all the events related to the life cycle of the CA keys must be kept for seven years, including the generation of the pair of Subscriber keys.

6.5 Technical security controls

Compliance.

6.6 Certificate, CRL, and OCSP profiles

Compliance with findings.

#3 Currently, all requests to OCSP services are recorded and stored. However, no analysis is carried out in relation to the requests for non-issued certificates on the responder as part of Camerfirma security response procedures to check if this is an indication of an attack.

6.7 Compliance audit and other assessment

Compliance.

6.8 Other business and legal matters

Compliance.

6.9 Other provisions

Compliance.

7.1 Certificate policy management

Compliance.

7.2 Additional requirements

Compliance.

All the minor non-conformities have been scheduled to be addressed in the corrective action plan of the Trust Service Provider.

No critical non-conformities were identified.

Appendix A: Identifying Information for in Scope CAs

CA #	Cert #	Subject	Issuer	serialNumber	Key Algorithm	Key Size	Sig Algorithm	notBefore	NotAfter	SKI	SHA256 Fingerprint
1	1	CN=Chambers of Commerce Root - 2008, O=AC Camerfirma S.A., serialNumber=A82743287, L=Madrid (see current address at www.camerfirma.com/address), C=EU	CN=Chambers of Commerce Root - 2008, O=AC Camerfirma S.A., serialNumber=A82743287, L=Madrid (see current address at www.camerfirma.com/address), C=EU	A3DA427EA4B1AEDA	rsaEncryption	4096 bit	sha1WithRSAEncryption	Aug 1 12:29:50 2008 GMT	Jul 31 12:29:50 2038 GMT	F9:24:AC:0F:B2:B5:F8:79:C0:FA:60:88:1B:C4:D9:4D:02:9E:17:19	063E4AFAC491DFD332F3089B8542E94617D893D7FE944E10A7937EE29D9693C0
2	2	CN=Camerfirma AAPP II - 2014, L=Madrid (see current address at https://www.camerfirma.com/address), serialNumber=A82743287, O=AC Camerfirma S.A., OU=AC CAMERFIRMA, C=ES	CN=Chambers of Commerce Root - 2008, O=AC Camerfirma S.A., serialNumber=A82743287, L=Madrid (see current address at www.camerfirma.com/address), C=EU	1548D054B8A842BA	rsaEncryption	4096 bit	sha256WithRSAEncryption	Dec 16 11:59:01 2014 GMT	Dec 15 11:59:01 2037 GMT	5D:A1:55:A4:DC:4A:AC:83:11:F9:AA:38:E5:F7:68:4A:FE:15:15:4C	7239D2F770FAFF3B1CF8BE2A05EC03EDEAAC053B554F90D36921155BA8051981
3	3	CN=Camerfirma Corporate Server II - 2015, L=Madrid (see current address at https://www.camerfirma.com/address), serialNumber=A82743287, O=AC Camerfirma S.A., OU=AC CAMERFIRMA, C=ES	CN=Chambers of Commerce Root - 2008, O=AC Camerfirma S.A., serialNumber=A82743287, L=Madrid (see current address at www.camerfirma.com/address), C=EU	621FF31C489BA136	rsaEncryption	4096 bit	sha256WithRSAEncryption	Jan 15 09:21:16 2015 GMT	Dec 15 09:21:16 2037 GMT	63:E9:F0:F0:56:00:68:65:B0:21:6C:0E:5C:D7:19:08:9D:08:34:65	66EAE2709B54CDD1693177B1332FF036CDD0F723DB3039ED311555A6CBF5FF3E
4	4	CN=CHAMBERS OF COMMERCE ROOT 2018, O=AC CAMERFIRMA S.A., 2.5.4.97=VATES-A82743287, serialNumber=A82743287, OU=CHAMBERS OF COMMERCE ROOT 2018, OU=see current address at www.camerfirma.com/address, L=MADRID, ST=MADRID, C=ES	CN=CHAMBERS OF COMMERCE ROOT 2018, O=AC CAMERFIRMA S.A., 2.5.4.97=VATES-A82743287, serialNumber=A82743287, OU=CHAMBERS OF COMMERCE ROOT 2018, OU=see current address at www.camerfirma.com/address, L=MADRID, ST=MADRID, C=ES	19A41376352ACD26	rsaEncryption	4096 bit	sha256WithRSAEncryption	Oct 4 08:15:28 2018 GMT	Sep 28 08:15:28 2042 GMT	B5:2E:59:20:B2:AF:43:BB:95:3D:C2:51:99:E3:75:55:34:48:B0:1C	9ACC89C46D684F5F2F9BB8B01B61EC7FBC7BDBE6697F076C595B842C07CF6820

5	5	CN=AC CAMERFIRMA FOR WEBSITES 2018, O=AC CAMERFIRMA S.A., 2.5.4.97=VATES-A82743287, serialNumber=A82743287, OU=AC CAMERFIRMA FOR WEBSITES 2018, OU=see current address at https://www.camerfirma.com/address, L=MADRID, ST=MADRID, C=ES	CN=CHAMBERS OF COMMERCE ROOT 2018, O=AC CAMERFIRMA S.A., 2.5.4.97=VATES-A82743287, serialNumber=A82743287, OU=CHAMBERS OF COMMERCE ROOT 2018, OU=see current address at www.camerfirma.com/address, L=MADRID, ST=MADRID, C=ES	18CDF491B343480C	rsaEncryption	4096 bit	sha256WithRSAEncryption	Oct 4 09:00:23 2018 GMT	Aug 28 09:00:23 2042 GMT	50:47:5C:2F:BA:12:7B:5F:74:38:1B:07:12:31:FB:68:4C:A8:EF:DE	BF0F4491F371489DF2EB187BDCB4B2EDD9AB2DA016CC64084CAC45195EF3590D