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:	Qualified certificate for electronic signature Qualified certificate for electronic seal Qualified certificate for website authentication
provided at:	Jorge Juan, 106. Madrid 28009
complies with the requirements defined in standard:	ETSI EN 319 411-2 v2.2.2
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

Assessment criteria

The assessment criteria are defined in standard ETSI EN 319 411-2:

- ETSI EN 319 411-2 V2.2.2 (2018-04): "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates", Version 2.2.2, 2018-04, European Telecommunications Standards Institute

The applicable ETSI Certification Policies are:

- QCP-n: Policy for EU qualified certificate issued to a natural person
- QCP-n-qscd: Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD
- QCP-l: Policy for EU qualified certificate issued to a legal person
- QCP-w: Policy for EU qualified website certificate issued to a natural or a legal person and linking the website to that person

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 - 2016 6. CHAMBERS OF COMMERCE ROOT 2018
QCP-n Issuing CAs
3. AC CAMERFIRMA FOR NATURAL PERSONS - 2016
QCP-n-qscd Issuing CAs
3. AC CAMERFIRMA FOR NATURAL PERSONS - 2016
QCP-l Issuing CAs
2. AC CAMERFIRMA FOR LEGAL PERSONS – 2016
QCP-l-qscd Issuing CAs
2. AC CAMERFIRMA FOR LEGAL PERSONS – 2016
QCP-w Issuing CAs
4. AC CAMERFIRMA FOR WEBSITES – 2016 7. AC CAMERFIRMA FOR WEBSITES 2018
Timestamp CAs
5. AC CAMERFIRMA TSA - 2016

*See Appendix A

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

- DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN CERTIFICADOS DIGITALES AC CAMERFIRMA SA EIDAS Versión 1.2.10

- POLÍTICA DE CERTIFICACIÓN CAMERFIRMA FOR LEGAL PERSONS Versión 1.0.1
- POLÍTICA DE CERTIFICACIÓN AC CAMERFIRMA FOR NATURAL PERSONS Versión 1.1
- POLÍTICA DE CERTIFICACIÓN AC CAMERFIRMA FOR WEBSITES Versión 2.1
- POLÍTICA DE CERTIFICACIÓN AC CAMERFIRMA TSA Versión 2.0.3

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

- 1.3.6.1.4.1.17326.10.16.1.1.2 - QCP-n *(*AC CAMERFIRMA FOR NATURAL PERSONS - 2016*)*
- 1.3.6.1.4.1.17326.10.16.1.2.1 - QCP-n-qscd *(*AC CAMERFIRMA FOR NATURAL PERSONS - 2016*)*
- 1.3.6.1.4.1.17326.10.16.1.2.2 - QCP-n *(*AC CAMERFIRMA FOR NATURAL PERSONS - 2016*)*
- 1.3.6.1.4.1.17326.10.16.1.3.1.1 -QCP-n-qscd *(*AC CAMERFIRMA FOR NATURAL PERSONS - 2016*)*
- 1.3.6.1.4.1.17326.10.16.1.3.1.2 - QCP-n *(*AC CAMERFIRMA FOR NATURAL PERSONS - 2016*)*
- 1.3.6.1.4.1.17326.10.16.1.3.2.1 - QCP-n-qscd *(*AC CAMERFIRMA FOR NATURAL PERSONS - 2016*)*
- 1.3.6.1.4.1.17326.10.16.1.3.2.2 - QCP-n *(*AC CAMERFIRMA FOR NATURAL PERSONS - 2016*)*
- 1.3.6.1.4.1.17326.10.16.1.3.3.1 - QCP-n-qscd *(*AC CAMERFIRMA FOR NATURAL PERSONS - 2016*)*
- 1.3.6.1.4.1.17326.10.16.1.3.3.2 - QCP-n *(*AC CAMERFIRMA FOR NATURAL PERSONS - 2016*)*
- 1.3.6.1.4.1.17326.10.16.1.5.1.3.4.1 - QCP-n-qscd *(*AC CAMERFIRMA FOR NATURAL PERSONS - 2016*)*
- 1.3.6.1.4.1.17326.10.16.1.5.1.3.4.4 - QCP-n-qscd *(*AC CAMERFIRMA FOR NATURAL PERSONS - 2016*)*
- 1.3.6.1.4.1.17326.10.16.5.1.1 - TSU *(*AC CAMERFIRMA TSA - 2016*)*
- 1.3.6.1.4.1.17326.10.16.3.5.1 - QCP-w *(*AC CAMERFIRMA FOR WEBSITES - 2016*)*
- 1.3.6.1.4.1.17326.10.16.3.6.1.3.2.2 - QCP-w *(*AC CAMERFIRMA FOR WEBSITES - 2016*)*
- 1.3.6.1.4.1.17326.10.16.3.5.1 - QCP-w *(*AC CAMERFIRMA FOR WEBSITES 2018*)*
- 1.3.6.1.4.1.17326.10.16.2.1.1 - QCP-l-qscd *(*AC CAMERFIRMA FOR LEGAL PERSONS - 2016*)*
- 1.3.6.1.4.1.17326.10.16.2.1.2 - QCP-l *(*AC CAMERFIRMA FOR LEGAL PERSONS - 2016*)*
- 1.3.6.1.4.1.17326.10.16.2.2.1.3.3.1 - QCP-l-qscd *(*AC CAMERFIRMA FOR LEGAL PERSONS - 2016*)*
- 1.3.6.1.4.1.17326.10.16.2.2.1.4.3.1 - QCP-l *(*AC CAMERFIRMA FOR LEGAL PERSONS - 2016*)*
- 1.3.6.1.4.1.17326.10.16.3.5.1 - QCP-w *(*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 with findings.

#1 In section 4.9 of CPS it is established that the status information of an expired certificate is maintained on its databases and is accessible through the OCSP service.

However, this information is not included in the event of CA's key compromise or in case of TSP termination. Aditionnaly, no retention time is diclosed.

6.4 Facility, management, and operational controls

Compliance with findings.

#2 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.

#3 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 319 411-2 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 with findings

#4 When purchase orders for cryptographic cards are placed, Camerfirma checks with the provider if the device continues being recognized as QSCD. However, QSCD devices' certification status monitoring is not carried out on an on-going basis, neither are the measures to be taken in case of loss of the QSCD status in the CPS.

6.6 Certificate, CRL, and OCSP profiles

Compliance with findings.

#5 The sample of certificates evaluated conforms to the ETSI EN 319 412-5 standard with the following exception: In one (1) test certificate, the ASN.1 structure for the QcType extension is wrongly formatted (OID 1.3.6.1.4.1.17326.10.16.2.1.1 - QCP-l-qscd)

#6 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 - 2016, O=AC CAMERFIRMA S.A., 2.5.4.97=VATES-A82743287, serialNumber=A82743287, OU=CHAMBERS OF COMMERCE ROOT - 2016, OU=see current address at www.camerfirma.com/address, L=MADRID, ST=MADRID, C=ES	CN=CHAMBERS OF COMMERCE ROOT - 2016, O=AC CAMERFIRMA S.A., 2.5.4.97=VATES-A82743287, serialNumber=A82743287, OU=CHAMBERS OF COMMERCE ROOT - 2016, OU=see current address at www.camerfirma.com/address, L=MADRID, ST=MADRID, C=ES	349A2DA18206B2B3	rsaEncryption	4096 bit	sha256WithRSAEncryption	Apr 14 07:35:48 2016 GMT	Apr 8 07:35:48 2040 GMT	9E:2E:65:4F:3E:57:F5:AB:7D:96:C6:8B:DF:B3:35:6D:4A:E8:9E:8B	04F1BEC36951BC1454A904CE32890C5DA3CDE1356B7900F6E62DFA2041EBAD51
2	2	CN=AC CAMERFIRMA FOR LEGAL PERSONS - 2016, O=AC CAMERFIRMA S.A., 2.5.4.97=VATES-A82743287, serialNumber=A82743287, OU=AC CAMERFIRMA FOR LEGAL PERSONS - 2016, OU=see current address at https://www.camerfirma.com/address, ST=MADRID, L=MADRID, C=ES	CN=CHAMBERS OF COMMERCE ROOT - 2016, O=AC CAMERFIRMA S.A., 2.5.4.97=VATES-A82743287, serialNumber=A82743287, OU=CHAMBERS OF COMMERCE ROOT - 2016, OU=see current address at www.camerfirma.com/address, L=MADRID, ST=MADRID, C=ES	54B16EE111245A42	rsaEncryption	4096 bit	sha256WithRSAEncryption	Apr 14 08:33:07 2016 GMT	Mar 9 08:33:07 2040 GMT	C3:27:85:93:D7:2F:96:C5:1B:AC:76:33:D9:86:A2:4A:7D:68:14:42	3A8066266D28BD28CCD0F564C8FBC1219B4FFAE403E01E5039D30F2400F0EB09
3	3	CN=AC CAMERFIRMA FOR NATURAL PERSONS - 2016, O=AC CAMERFIRMA S.A., 2.5.4.97=VATES-A82743287, serialNumber=A82743287, OU=AC CAMERFIRMA FOR NATURAL PERSONS - 2016, OU=see current address at https://www.camerfirma.com/address, ST=MADRID, L=MADRID, C=ES	CN=CHAMBERS OF COMMERCE ROOT - 2016, O=AC CAMERFIRMA S.A., 2.5.4.97=VATES-A82743287, serialNumber=A82743287, OU=CHAMBERS OF COMMERCE ROOT - 2016, OU=see current address at www.camerfirma.com/address, L=MADRID, ST=MADRID, C=ES	51514CB44FA454F5	rsaEncryption	4096 bit	sha256WithRSAEncryption	Apr 14 08:48:09 2016 GMT	Mar 9 08:48:09 2040 GMT	70:B8:F8:24:C7:51:CA:CE:22:80:92:08:C9:C0:68:2F:C1:47:58:51	EEDD457AF1353D76F48E7C6123F39140E5F9A069CA51B43EEA8615C9CEC0D4BB
4	4	CN=AC CAMERFIRMA FOR WEBSITES - 2016, O=AC CAMERFIRMA S.A., 2.5.4.97=VATES-A82743287, serialNumber=A82743287, OU=AC CAMERFIRMA FOR WEBSITES - 2016, OU=see current address at https://www.camerfirma.com/address, L=MADRID, ST=MADRID,	CN=CHAMBERS OF COMMERCE ROOT - 2016, O=AC CAMERFIRMA S.A., 2.5.4.97=VATES-A82743287, serialNumber=A82743287, OU=CHAMBERS OF COMMERCE ROOT - 2016, OU=see current address at www.camerfirma.com/address, L=MADRID,	23CDF491B343480B	rsaEncryption	4096 bit	sha256WithRSAEncryption	Apr 18 15:43:54 2016 GMT	Mar 13 15:43:54 2040 GMT	EC:95:33:3B:71:C0:D2:B1:9C:58:23:0B:36:41:BC:54:9E:2C:92:1D	937D7D5D0B7FB7DB039399BC0B670CC203C7AB4E332FAE453CC38EC188DDEA2B

		C=ES	ST=MADRID, C=ES								
5	5	CN=AC CAMERFIRMA TSA - 2016, O=AC CAMERFIRMA S.A., 2.5.4.97=VATES-A82743287, serialNumber=A82743287, OU=AC CAMERFIRMA TSA - 2016, OU=see current address at https://www.camerfirma.com/address, L=MADRID, ST=MADRID, C=ES	CN=CHAMBERS OF COMMERCE ROOT - 2016, O=AC CAMERFIRMA S.A., 2.5.4.97=VATES-A82743287, serialNumber=A82743287, OU=CHAMBERS OF COMMERCE ROOT - 2016, OU=see current address at www.camerfirma.com/address, L=MADRID, ST=MADRID, C=ES	15B7A58A54FF0282	rsaEncryption	4096 bit	sha256WithRSAEncryption	Apr 14 10:42:09 2016 GMT	Mar 9 10:42:09 2040 GMT	1E:6D:B5:C6:3F:EF:92:55:5E:37:FA:DB:FD:10:AA:BA:D9:3B:4E:2C	BAAE2C6338857D50200F6F73DD45E65AA2D895BED4675B6E396B7222E018A9B8
6	6	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
7	7	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