AENOR

Appendix to the Certificate of Trust Service Provider

PSC- 2017/0002

The Conformity Assessment Body, AENOR INTERNACIONAL SAU, issues this appendix to certificate number PSC-2017/0002 to the organization:

CONSORCI ADMINISTRACIÓ OBERTA DE CATALUNYA

to confirm that its trust service:	Qualified certificate for electronic signature
	Qualified certificate for electronic seal
	Qualified certificate for website authentication
provided at:	CARRER DE TÀNGER, 98. (PLANTA BAIXA)
	08018 BARCELONA - ESPAÑA
complies with the requirements defined in standard:	ETSI EN 319 411-2 v2.2.2
First issuance date:	2017-06-26
Updating date:	2019-05-31
Expiration date:	2020-05-30

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

Rafael GARCÍA MEIRO
Director General
31-05-2019

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-2017/0002

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 Barcelona (Spain) between March 28th, 2019 (2019-03-28) and April 5th, 2019 (2019-04-05).

The audit was carried out as a period audit and covered the period from the March 29th, 2018 (2018-03-29) until March 28th, 2019 (2019-03-28)

Assessment scope

The scope of the assessment includes the following CA certificates:

Root CAs
1. EC-ACC
QCP-n Issuing CAs
2. EC-SectorPublic 3. EC-Ciutadania
QCP-n-qscd Issuing Cas
2. EC-SectorPublic
QCP-l Issuing CAs
2. EC-SectorPublic
QCP-w Issuing CAs
2. EC-SectorPublic

*See Appendix A

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

- Declaración de Prácticas de Certificación Autoridad de Certificación del Consorci AOC v6.0
- Política de Certificación para Dispositivos e Infraestructuras Consorci AOC v6.0
- Política de Certificación para Certificados Personales del Sector Público Consorci AOC v6.0
- Política de Certificación para Certificados de Ciudadanía Consorci AOC v6.0

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

- 1.3.6.1.4.1.15096.1.3.2.4.1.1 QCP-n-qscd (EC-SectorPublic)

- 1.3.6.1.4.1.15096.1.3.2.5.2 QCP-w (EC-SectorPublic)
- 1.3.6.1.4.1.15096.1.3.2.51.2 QCP-w (EC-SectorPublic)
- 1.3.6.1.4.1.15096.1.3.2.6.2 QCP-l (EC-SectorPublic)
- 1.3.6.1.4.1.15096.1.3.2.7.1.1 QCP-n-qscd (EC-SectorPublic)
- 1.3.6.1.4.1.15096.1.3.2.7.3.1 QCP-n (EC-SectorPublic)
- 1.3.6.1.4.1.15096.1.3.2.8.1.1 QCP-n-qscd (EC-SectorPublic)
- 1.3.6.1.4.1.15096.1.3.2.82.1 QCP-n-qscd (EC-SectorPublic)
- 1.3.6.1.4.1.15096.1.3.2.86.1 QCP-n (EC-SectorPublic)
- 1.3.6.1.4.1.15096.1.3.2.91.1 QCP-l (EC-SectorPublic)
- 1.3.6.1.4.1.15096.1.3.2.86.2 QCP-n (EC-Ciutadania)

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 April 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 with findings

#1 The following deficiencies were identified in the CPS and CPs:

- Evidence could not be found in the CPS that an annual review is carried out as required by clause 2 of the CA/Browser Forum Baseline Requirements.
- The CPS and CPs are not fully aligned with RFC 3647 or RFC 2527.
- There is reference included in the CPS to indicate conformance to the CA/Browser Forum guidelines for BR and EV. However, it is not clearly indicated that those guidelines have prevalence over the DPC where they are not fully aligned.
- Evidence could not be found in the CPS or CPs of indications about how the DNS CAA records are reviewed.
- In the CPS and CPs for each type of certificate inconsistencies have been identified about how frequent the CRL is published since documents make reference to each other but the frequency as such is not specified in none of them.

5.3 Certificate Policy name and identification

Compliance

5.4 PKI participants

Compliance

6.1 Publication and repository responsibilities

Compliance with findings

#2 Even though the PSC has informed that the certificates are not published, in section 4.4.3 of the CPS it is indicated that the certificates can be published without the previous consent of the subscribers who have control of the private key. However, the previous consent is a requirement to be able to publish the certificates.

6.2 Identification and authentication

Compliance

6.3 Certificate Life-Cycle operational requirements

Compliance with findings.

#3 According to CPS, suspension is prohibited for the web authentication certificates and systems do not allow the suspension of these type of certificates. However evidence was found through the certificate validation services that there are suspended certificates of other types in the EC-SectorPublic repository which is not allowed by the BRG requirements.

6.4 Facility, management, and operational controls

Compliance with findings.

#4 The PSC has carried out a risk analysis following the MAGERIT methodology. However, the risk analysis and the residual risk have not been formally approved by management.

#5 Evidence could not be found that the start/stop of logging activities are being logged and monitored for the infrastructure supporting the trusted services.

#6 The CPS does not indicate the maximum interval between reviews of the configuration of the systems supporting the trusted services.

#7 The password policies of the EACAT Active Directory and Corporate Active Directory are not compliant with the password policy defined in the CAOC security policies.

#8 Section 5.7.3 of the CPS includes the compromise of the private keys. However, evidence could not be found that the business continuity plan (BCP) includes this scenario and the

steps that need to be taken by the PSC. The BCP does not contemplate either the scenario related to the compromise of the algorithms used for certificate generation.

6.5 Technical security controls

Compliance with findings.

#9 An external pentesting exercise was performed in January 2019. However, the certificate request platform part of the RA services was not in the scope of the pentesting. Nevertheless, the infrastructure hosted in Firmaprofesional are subject to internal and external vulnerability analysis as well as an external pentesting.

6.6 Certificate, CRL, and OCSP profiles

Compliance with findings.

#10 It has been evidenced that authentication certificates met the BRG and EVG requirements with the following exceptions:

- Entropy for the QCP-w certificates issued by "EC-SectorPublic" is only of 63 bits (when 64 bits is required). The TSP is aware of this situation (https://bugzilla.mozilla.org/show_bug.cgi?id=1538673)

#11 The following issues have been evidenced in the profiles of the certificates:

- 1.3.6.1.4.1.15096.1.3.2.5.2 (QCP-w) y 1.3.6.1.4.1.15096.1.3.2.51.2 (QCP-w): In the obtained sample, some certificates corresponding to the QCP-w profile that did not contain corresponding QCType have been identified. This has only been evidenced for those certificates that were issued in 2018, the certificates issued later do not present this issue.

#12 It has been evidenced that qualified certificates met the RFC 5280 and ETSI EN 319 412 requirements with the following exceptions:

- 1.3.6.1.4.1.15096.1.3.2.6.2 (QCP-l): ASN.1 errors of zero-length objects have been found in sample certificates (14 certificates). This error occurs when including in the SubjectAlternativeName fields corresponding to the administrative identity defined by "Secretaría General de Administración Digital" profiles without an associated value. Additionally, certificates with givenName exceeding 17 characters have been found (9 certificates).

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 to the Certificate for Trust Service Provider: PSC-2017/0002

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=EC-ACC, OU=Jerarquia Entitats de Certificacio Catalanes, OU=Vegeu https://www.catcert.net/verarrel (c)03, OU=Serveis Publics de Certificacio, O=Agencia Catalana de Certificacio (NIF Q-0801176-I), C=ES	CN=EC-ACC, OU=Jerarquia Entitats de Certificacio Catalanes, OU=Vegeu https://www.catcert.net/verarrel (c)03, OU=Serveis Publics de Certificacio, O=Agencia Catalana de Certificacio (NIF Q-0801176-I), C=ES	EE2B3DEBD421DE14A862AC04F3DDC401	rsaEncryption	2048 bit	sha1WithRSAEncryption	Jan 7 23:00:00 2003 GMT	Jan 7 22:59:59 2031 GMT	A0:C3:8B:44:AA:37:A5:45:BF:97:80:5A:D1:F1:78:A2:9B:E9:5D:8D	88497F01602F3154246AE28C4D5AEF10F1D87EBB76626F4AE0B7F95BA7968799
1	2	CN=EC-ACC, OU=Jerarquia Entitats de Certificacio Catalanes, OU=Vegeu https://www.catcert.net/verarrel (c)03, OU=Serveis Publics de Certificacio, O=Agencia Catalana de Certificacio (NIF Q-0801176-I), C=ES	CN=EC-ACC, OU=Jerarquia Entitats de Certificacio Catalanes, OU=Vegeu https://www.catcert.net/verarrel (c)03, OU=Serveis Publics de Certificacio, O=Agencia Catalana de Certificacio (NIF Q-0801176-I), C=ES	524B25BD12ED8CFE4F8D37BBC29BA87F	rsaEncryption	2048 bit	sha256WithRSAEncryption	Apr 17 09:28:27 2012 GMT	Jan 7 22:59:59 2031 GMT	A0:C3:8B:44:AA:37:A5:45:BF:97:80:5A:D1:F1:78:A2:9B:E9:5D:8D	A5898E5BFB84295C043EC4034288AFB37E0D5A3866F17CB657B97F72DCB53BEC
2	1	CN=EC-SectorPublic, OU=Serveis Públics de Certificació, O=CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA, C=ES	CN=EC-ACC, OU=Jerarquia Entitats de Certificacio Catalanes, OU=Vegeu https://www.catcert.net/verarrel (c)03, OU=Serveis Publics de Certificacio, O=Agencia Catalana de Certificacio (NIF Q-0801176-I), C=ES	71B065397C8E07D2541A967F75593792	rsaEncryption	2048 bit	sha256WithRSAEncryption	Sep 18 08:23:27 2014 GMT	Sep 18 08:23:27 2030 GMT	47:3C:DE:14:77:BB:6A:4F:47:91:A9:02:FF:D4:06:E1:73:DC:E2:D9	356A5F4D994E9EFA7CAEFC491768911D65EC25977465B610E2F29AA4472631C3
3	1	CN=EC-Ciutadania, OU=Serveis Públics de Certificació, O=CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA, C=ES	CN=EC-ACC, OU=Jerarquia Entitats de Certificacio Catalanes, OU=Vegeu https://www.catcert.net/verarrel (c)03, OU=Serveis Publics de Certificacio, O=Agencia Catalana de Certificacio (NIF Q-0801176-I), C=ES	73EEAE15E3DFADA8541A95ECF258624F	rsaEncryption	2048 bit	sha256WithRSAEncryption	Sep 18 08:21:00 2014 GMT	Sep 18 08:21:00 2030 GMT	0B:68:59:3E:87:C8:A3:15:1A:E0:40:82:22:5F:9F:1D:B2:C5:37:15	0FD99AAE1FFCD5D9F0AD76EDDDCBEF6B884CC85C16BFCFA4B5246155D6597ED6