AENOR

Appendix to the Certificate of Trust Service Provider

PSC- 2017/0001

The Conformity Assessment Body, AENOR INTERNACIONAL SAU, issues this appendix to certificate number PSC-2017/0001 to the organization:

EDICOM CAPITAL, S.L.

to confirm that its trust service: Qualified certificate for electronic signature

Qualified certificate for electronic seal

provided at: Calle de Charles Robert Darwin, 8,

46980 Paterna, Valencia – ESPAÑA

complies with the requirements defined in standard: ETSI EN 319 411-2 v2.2.2

First issuance date:2017-06-19
Updating date:2019-05-30
Expiration date:2020-05-29

This appendix to the certificate is valid only in its entirety *(5 pages)*.

Rafael GARCÍA MEIRO
Director General
30-05-2019

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: certificate policy for EU qualified certificate issued to natural persons
- QCP-n-qscd: certificate policy for EU qualified certificate issued to natural persons with private key related to the certified public key in a QSCD
- QCP-l: certificate policy for EU qualified certificate issued to legal persons
- QCP-l-qscd: certificate policy for EU qualified certificate issued to legal persons with private key related to the certified public key in a QSCD

Audit period

The Audit was carried out at the TSP sites in Paterna (Spain) between 2019-04-08 and 2019-05-03.

The audit was carried out as a period audit and covered the period from the 2018-04-25 until 2019-04-24

Assessment scope

The scope of the assessment includes the following CA certificates:

Root CAs
1. CAEDICOM Root
QCP-n Issuing CAs
2. CAEDICOM01
QCP-n-qscd Issuing Cas
2. CAEDICOM01
QCP-l Issuing CAs
2. CAEDICOM01
QCP-l-qscd Issuing CAs
2. CAEDICOM01
Timestamp CAs
2. CAEDICOM01

*See Appendix A

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

- CAEDICOM01_DPC_DeclaracionPracticasCertificacion
- CAEDICOM01_PC_PoliticaCertificacionPersFisica
- CAEDICOM01_PC_PoliticaCertificacionRepresentantePersJuridica
- CAEDICOM01_PC_PoliticaCertificacionSelloElectronico

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

- 1.3.6.1.4.1.30051.2.3.2.10 QCP-l / TSU (CAEDICOM01)
- 1.3.6.1.4.1.30051.2.3.2.14 QCP-l (CAEDICOM01)

- 1.3.6.1.4.1.30051.2.3.2.21 QCP-n *(CAEDICOM01)*
- 1.3.6.1.4.1.30051.2.3.2.23 QCP-n-qscd *(CAEDICOM01)*
- 1.3.6.1.4.1.30051.2.3.2.24 QCP-l-qscd *(CAEDICOM01)*
- 1.3.6.1.4.1.30051.2.3.2.26 QCP-l-qscd *(CAEDICOM01)*

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:

- It does not include the period of time during the which the certificate status information will be available.
- It does not indicate how the certificate status information will be provided in case of compromise of the CA private keys or termination of the PSC activities.

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.

#2 The EDICOM policies and procedures indicate that the minimum privilege principles are applied when granting access to the systems. Accesses over and above what is strictly required will need to be requested and authorised.

However, it was noted that not all the members of the "sistemas" group have been assigned trusted roles (administrators and operators) even though this group has permissions to carry out administrative and operational tasks and have access to the CA systems.

6.5 Technical security controls

Compliance.

6.6 Certificate, CRL, and OCSP profiles

Compliance.

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	C=ES, O=EDICOM, CN=CAEDICOM Root	C=ES, O=EDICOM, CN=CAEDICOM Root	FB712658AD99E5	rsaEncryption	4096 bit	sha256WithRSAEncryption	May 21 11:06:35 2014 GMT	May 21 10:20:00 2034 GMT	14:CD:2A:59:78:63:AB:61:19:E8:B8:3D:A1:E0:5A:C0:75:E7:F9:CB	1501F89C5C4DCF36CF588A17C9FD7CFCEB9EE01E8729BE355E25DE80EB6284B4
2	1	C=ES, L=Calle Charles Robert Darwin 8 - 46980 - Paterna, O=EDICOM, serialNumber=B96490867, CN=CAEDICOM01	C=ES, O=EDICOM, CN=CAEDICOM Root	2789BAEB6C594B5A	rsaEncryption	4096 bit	sha256WithRSAEncryption	Jul 22 11:00:43 2014 GMT	May 22 10:20:00 2024 GMT	6D:6A:88:F8:2E:EA:7F:2F:CD:C0:F4:76:77:93:E6:45:32:EF:8B:05	339D15B165CA8161E4D3792618C6FDE84E4904D04669541CEE6BD333BCD5B5F4