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 Certificate for website authentication
provided at:	Calle de Charles Robert Darwin, 8, 46980 Paterna, Valencia – ESPAÑA
complies with the requirements defined in standards:	ETSI EN 319 411-2 v2.2.2 ETSI EN 319 411-1 v1.2.2
First issuance date:	2017-06-19
Updating date:	2020-05-29
Expiration date:	2021-05-28

This appendix to the certificate is valid only in its entirety (6 pages).

Rafael GARCÍA MEIRO
Director General
29-05-2020

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-2017/0001

Assessment criteria

The assessment criteria are defined in standards ETSI EN 319 411-2 and ETSI EN 319 411-1:

- 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
- 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:

- ETSI EN 319 411-2 V2.2.2, QCP-n: Policy for EU qualified certificate issued to a natural person
- ETSI EN 319 411-2 V2.2.2, 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
- ETSI EN 319 411-2 V2.2.2, QCP-l: Policy for EU qualified certificate issued to a legal person
- ETSI EN 319 411-2 V2.2.2, 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
- ETSI EN 319 411-1 V1.2.2, OVCP: Organizational Validation Certificate Policy
- ETSI EN 319 411-1 V1.2.2, DVCP: Domain Validation Certificate Policy

Audit period

The Audit was carried out at the relevant available TSP sites between March 30, 2020 and April 25, 2020.

The audit was carried out as a period audit and covered the period from the April 25, 2019 until April 24, 2020.

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
OVCP / DVCP Issuing CAs
2. CAEDICOM01

*See Appendix A

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

- CAEDICOM01_DPC_DeclaracionPracticasCertificacion – v1.12
- CAEDICOM01_PC_PoliticaCertificacionPersFisica – v1.4

- CAEDICOM01_PC_PoliticaCertificacionRepresentantePersJuridica – v1.4
- CAEDICOM01_PC_PoliticaCertificacionSelloElectronico – v1.3
- CAEDICOM01_PC_PoliticaCertificadosTLS – v1.8

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

- 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 *(*CAEDICOM01*)*
- 1.3.6.1.4.1.30051.2.3.2.26 - QCP-l-qscd *(*CAEDICOM01*)*
- 1.3.6.1.4.1.30051.2.3.2.7 - OVCP/DVCP *(*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 May 2021.

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 with findings

#1 The domain validation used for certificate with serial number: 249b9bc8a3a80747 were not in line with the requirements of Section 3.2.2 of the BRG.

6.3 Certificate Life-Cycle operational requirements

Compliance with findings

#2 The information stated in the CPS is inconsistent regarding how the certificate status information is provided after the expiration of the certificate, including but not limited to the period during which the certificate status information is made available after the expiration of the certificate or how such information will be provided in the event of CA key compromise or TSP termination of service. (e.g. Sections 7.3.1 and 5.8.1)

Additionally, as indicated in section 5.8.1 of the CPS, the publication of the last CRL "shall remain available until the expiry date of the last certificate issued" would defeat the purpose of a last CRL to provide status information on certificates after expiration.

#3 During the tests evidence has been identified of the existence of a revoked and expired certificate that was not included in the CRL (despite including the extension *ExpiredCertsOnCRL*="20140722110043Z"), although it was confirmed that the OCSP service identified it as revoked.

6.4 Facility, management, and operational controls

Compliance.

6.5 Technical security controls

Compliance with findings.

#4 Although the entity has defined a periodic check in order to monitor the QSCD certification status every 6 months, it has been identified that the last check completed did not detect the imminent loss of qualification of the Aladdin eToken Pro device and, therefore, appropriate action as per section 6.1.8 of the CPS has not been taken.

6.6 Certificate, CRL, and OCSP profiles

Compliance with findings.

#5 The revised certificates meet the requirements of the profiles corresponding to each type with the following exceptions:

- 1.3.6.1.4.1.30051.2.3.2.21 (QCP-n): During the tests a software certificate was issued which included the *QcStatement QcSSCD*.
- 1.3.6.1.4.1.30051.2.3.2.7 (DVCP) One certificate was issued with unallowed key usage for RSA public key (Key Agreement)

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-2017/0001

Appendix A: Identifying Information for in Scope CAs

CA#	Cert #	Subject	Issuer	serialNumber	notBefore	NotAfter	SHA256 Fingerprint
1	1	C=ES, O=EDICOM, CN=CAEDICOM Root	C=ES, O=EDICOM, CN=CAEDICOM Root	FB712658AD99E5	May 21 11:06:35 2014 GMT	May 21 10:20:00 2034 GMT	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	Jul 22 11:00:43 2014 GMT	May 22 10:20:00 2024 GMT	339D15B165CA8161E4D3792618C6FDE84E4904D04669541CEE6BD333BCD5B5F4