

AENOR

Appendix to the Certificate of Trust Service Provider

PSC- 2017/0005

The Conformity Assessment Body, AENOR INTERNACIONAL SAU, issues this appendix to certificate number PSC-2017/0005 to the organization:

SIGNE, S.A.

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

provided at: AVENIDA DE LA INDUSTRIA, 18
28760 TRES CANTOS - ESPAÑA

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

First issuance date: 2017-06-26
Updating date: 2019-06-26
Expiration date: 2020-06-25

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



Rafael GARCÍA MEIRO
Director General
16-07-2019

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-l-qscd: Policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD

Audit period

The Audit was carried out at the TSP sites in Tres Cantos (Madrid, Spain) between 2019-04-03 and 2019-04-12.

The audit was carried out as a period audit and covered the period from the 2018-03-29 until 2019-03-28.

Assessment scope

The scope of the assessment includes the following CA certificates:

Root CAs
1. Autoridad de Certificacion Firmaprofesional CIF A62634068
QCP-n Issuing CAs
2. SIGNE Autoridad de Certificacion
QCP-n-qscd Issuing CAs
2. SIGNE Autoridad de Certificacion
QCP-l Issuing CAs
2. SIGNE Autoridad de Certificacion
QCP-l-qscd Issuing CAs
2. SIGNE Autoridad de Certificacion
QCP-w Issuing CAs
N/A

*See Appendix A

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

- SIGNE-DPC-AC-01_Declaracion_de_Practicas_de_Certificacion_v2.3
- SIGNE-ES-DPC-AC-01-F10_Condiciones_Generales_de_Contratacion_v1.0
- SIGNE-PDS-AC-01_PKI_Disclosure_Statement_PDS_for_electronic_certificates_v1.2
- SIGNE-POL-ADM-AC-01_PC_Certificados_de_Sello_de_Organo_v2.3
- SIGNE-POL-COR-AC-03_PC_Certificados_Corporativos_de_Persona_Fisica_v2.3
- SIGNE-POL-COR-AC-04_PC_Certificados_Corporativos_de_Sello_Electronico_v1.3
- SIGNE-POL-PER-AC-05_PC_Certificados_de_Titulado_v2.3

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

- 1.3.6.1.4.1.36035.1.10.1 - QCP-l-qscd

- 1.3.6.1.4.1.36035.1.10.2 - QCP-l
- 1.3.6.1.4.1.36035.1.10.3 - QCP-l-qscd
- 1.3.6.1.4.1.36035.1.1.2 - QCP-n
- 1.3.6.1.4.1.36035.1.2.1 - QCP-n-qscd
- 1.3.6.1.4.1.36035.1.2.2 - QCP-n
- 1.3.6.1.4.1.36035.1.2.3 - QCP-n-qscd
- 1.3.6.1.4.1.36035.1.5.1 - QCP-l-qscd
- 1.3.6.1.4.1.36035.1.5.2 - QCP-l
- 1.3.6.1.4.1.36035.1.5.3 - QCP-l-qscd

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 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

6.5 Technical security controls

Compliance

6.6 Certificate, CRL, and OCSP profiles

Compliance with findings.

#1 The sample of certificates evaluated conforms to the ETSI standard with the following exception:

- OID 1.3.6.1.4.1.36035.1.1.2: Although *Surname* is present, *GivenName* is not present, as required by ETSI 411-2. Additionally, in some cases *Surname* only contains the subject first surname and not both (e.g. a person with first and second surname). *Note: This finding applies only until May 2018, certificates issued on June 2018 and thereafter were fixed.*

- OID 1.3.6.1.4.1.36035.1.1.2: There are objects with zero length (e.g. OID.1.3.6.1.4.1.13177.0.3="").

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=Autoridad de Certificacion Firmaprofesional CIF A62634068, C=ES	CN=Autoridad de Certificacion Firmaprofesional CIF A62634068, C=ES	53EC3BEEFBB2485F	rsaEncryption	4096 bit	sha1WithRSAEncryption	May 20 08:38:15 2009 GMT	Dec 31 08:38:15 2030 GMT	65:CD:EB:AB:35:1E:00:3E:7E:D5:74:C0:1C:B4:73:47:0E:1A:64:2F	04048028BF1F2864D48F9AD4D83294366A828856553F3B14303F90147F5D40EF
1	2	CN=Autoridad de Certificacion Firmaprofesional CIF A62634068, C=ES	CN=Autoridad de Certificacion Firmaprofesional CIF A62634068, C=ES	1B70E9D2FFAE6C71	rsaEncryption	4096 bit	sha256WithRSAEncryption	Sep 23 15:22:07 2014 GMT	May 5 15:22:07 2036 GMT	65:CD:EB:AB:35:1E:00:3E:7E:D5:74:C0:1C:B4:73:47:0E:1A:64:2F	57DE0583EFD2B26E0361DA99DA9DF4648DEF7EE8441C3B728AFA9BCDE0F9B26A
2	3	CN=SIGNE Autoridad de Certificacion, serialNumber=A11029279, O=SIGNE S.A., L=Avenida de la Industria 18. Tres Cantos 28760-Madrid, C=ES	CN=Autoridad de Certificacion Firmaprofesional CIF A62634068, C=ES	4084C35C3E665CB5	rsaEncryption	2048 bit	sha1WithRSAEncryption	Jul 21 09:48:57 2010 GMT	Jul 21 09:48:57 2022 GMT	90:AD:1A:31:FD:47:45:6D:32:44:43:18:85:97:64:C7:38:AE:6D:A8	0431D736C77697A0310103C6F890BC41C3A3BB81128ADE8D3C3461B4028D4413
2	4	CN=SIGNE Autoridad de Certificacion, serialNumber=A11029279, O=SIGNE S.A., L=Avenida de la Industria 18. Tres Cantos 28760-Madrid, C=ES	CN=Autoridad de Certificacion Firmaprofesional CIF A62634068, C=ES	21F0F18D95A95B75	rsaEncryption	2048 bit	sha256WithRSAEncryption	Jul 29 11:22:23 2015 GMT	Dec 31 04:02:55 2030 GMT	90:AD:1A:31:FD:47:45:6D:32:44:43:18:85:97:64:C7:38:AE:6D:A8	1CB470728CF56F302003BB0E4EB062414FA11D4F97E3F061170C96C88071D711