AENOR

Appendix to the Certificate of Trust Service Provider

PSC- 2017/0003

The Conformity Assessment Body, AENOR INTERNACIONAL SAU, issues this appendix to certificate number PSC-2017/0003 to the organization:

FIRMAPROFESIONAL, S.A.

to confirm that its trust service:	Certificate for website authentication
provided at:	EDIFICIO ESADECREÀPOLIS Avda. Torre blanca, 57 local m2 28173 Sant Cugat del Valles - España
complies with the requirements defined in standard:	ETSI EN 319 411-1 v1.2.2
First issuance date:	2017-06-21
Updating date:	2019-06-17
Expiration date:	2020-06-16

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

Rafael GARCÍA MEIRO
Director General
17-06-2019

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-2017/0003

Assessment criteria

The assessment criteria are defined in standard ETSI EN 319 411-1:

- 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:

- OVCP: Organizational Validation Certificate Policy
- EVCP: Extended Validation Certificate Policy

Audit period

The Audit was carried out at the TSP sites in San Cugat (Spain) between March 25st, 2019 (2019-03-25) and April 5th, 2019 (2019-04-05).

The audit was carried out as a period audit and covered the period from the March 28th, 2018 (2018-03-28) until March 27th, 2019 (2019-03-27)

Assessment scope

The scope of the assessment includes the following CA certificates:

Root CAs
1. Autoridad de Certificacion Firmaprofesional CIF A62634068
OV SSL Issuing CAs
2. AC Firmaprofesional - INFRAESTRUCTURA

*See Appendix A

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

- Certification Practices Statement (CPS) Firmaprofesional, S.A. Version 181221
- Certification Policy Website Authentication Certificates Version 190305

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

- 1.3.6.1.4.1.13177.10.1.3.1 - SSL OV (AC Firmaprofesional - INFRAESTRUCTURA)

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

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 It has been verified that, although the web application enables the revocation of certificates and prompt registration of the requests, in the rest of the cases (e.g. requests for revocation by email, telephone, etc.) no record of revocation request is kept. As a result, we could not find evidence that the status information of certificates is changed in less than 24 hours since a revocation request is received.

In addition, as indicated by the TSP, in some cases (e.g. request revocation by telephone) there is no explicit check to ensure the request revocation is originated by an authorized person. However, the TSP has stated that no cases of non-authorized revocation have happened during the audit period.

6.3 Certificate Life-Cycle operational requirements

Compliance.

6.4 Facility, management, and operational controls

Compliance with findings.

#2 During the review of the log events it was noted that full access (read and write) to the audit logs is restricted to authorized individuals. However, the person who has been assigned the role of auditor does not have permissions on the system to review the logs, whilst a read-only access is expected for such an auditor profile.

6.5 Technical security controls

Compliance.

6.6 Certificate, CRL, and OCSP profiles

Compliance with findings.

#3 Evidence has been found that shows authentication certificates meet the BRG requirements with the following exceptions:

- Entropy for the SSL certificates issued by "AC Firmaprofesional - INFRASTRUCTURE" is only of 63 bits (64 bits is required). The TSP is aware of this situation (https://bugzilla.mozilla.org/show_bug.cgi?id=1538638)

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-2017/0003

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	1	CN=AC Firmaprofesional - INFRAESTRUCTURA, serialNumber=A62634068, OU=Security Services, O=Firmaprofesional S.A., C=ES	CN=Autoridad de Certificacion Firmaprofesional CIF A62634068, C=ES	2B891DB7F6087583	rsaEncryption	2048 bit	sha256WithRSAEncryption	Jul 29 11:25:09 2015 GMT	Dec 31 04:02:55 2030 GMT	62:15:AB:B5:B3:08:79:A5:87:FE:80:D9:22:F0:8E:FC:8F:11:FD:79	CD74198D4C23E4701DEA579892321B9E4F47A08BD8374710B899AAD1495A4B35