AENOR

Anexo al Certificado de Prestadores de Servicios de Confianza

PSC-2017/0003

La entidad de evaluación de conformidad, AENOR INTERNACIONAL SAU, conforma el presente anexo al certificado número PSC-2017/0003 a la empresa

FIRMAPROFESIONAL, S.A.

para confirmar que su servicio de confianza:	Servicio de expedición de certificados electrónicos cualificados de autenticación de sitios web
que se realizan en:	Avda. Torre Blanca, 57. Local M2. 08173 Sant Cugat del Vallès – ESPAÑA
cumple los requisitos definidos en la norma:	ETSI EN 319 411-2 v2.1.1
Fecha de primera emisión:	2017-06-21
Fecha de expiración:	2018-06-20

Este anexo del certificado solamente es válido en su totalidad (5 páginas) y en conjunción con Informe de evaluación de conformidad (CAR): "PSC-20170003 - FIRMAPROFESIONAL, S.A." de fecha 21-06-2017

Rafael GARCÍA MEIRO
Director General

AENOR INTERNACIONAL, S.A.U.
Génova, 6. 28004 Madrid. España
Tel. 91 432 60 00.- www.aenor.com

Criterios de evaluación

Los criterios de evaluación se definen en la norma ETSI EN 319 411-2:

- ETSI EN 319 411-2 v2.1.1 (2016-02): "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". European Telecommunications Standards Institute

Las políticas de certificado ETSI aplicables son:

- QCP-w: Policy for EU qualified website certificate issued to a natural or a legal person and linking the website to that person.

Objetivo de la evaluación

El objetivo de la evaluación se caracteriza por la información del certificado del servicio evaluado:

SUBJECT:	**CN = AC Firmaprofesional - INFRAESTRUCTURA** *X*509*v*3 *Subject Key Identifier:* 62:15:*AB*:*B*5:*B*3:08:79:*A*5:87:*FE*:80:*D*9:22:*F*0:8*E*:*FC*:8*F*:11:*FD*:79
ISSUER:	**CN = Autoridad de Certificación Firmaprofesional CIF A62634068**
Certificado X.509 v3 (PEM 64):	-----BEGIN CERTIFICATE----- MIIHADCCBOigAwIBAgIIK4kdt/YIdYMwDQYJKoZIhvcNAQELBQAwUTELMAkGA1UE BhMCRVMxQjBABgNVBAMMOUF1dG9yaWRhZCBkZSBDZXJ0aWZpY2FjaW9uIEZpcm1h cHJvZmVzaW9uYWwgQ0lGIEE2MjYzNDA2ODAeFw0xNTA3MjkxMTI1MDlaFw0zMDEy MzEwNDAyNTVaMIGNMQswCQYDVQQGEwJFUzEeMBwGA1UECgwVRmlybWFwcm9mZXNp b25hbCBTLkEuMRowGAYDVQQLDBFTZWN1cml0eSBTZXJ2aWNlczESMBAGA1UEBRMJ QTYyNjM0MDY4MS4wLAYDVQQDDCVBQyBGaXJtYXByb2Zlc2lvbmFsIC0gSU5GUkFF U1RSVUNUVVJBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuqX7V9RP HmZ/SpGlhXSfREEtOiiRS8SdJC1QuOB2EYLiFEeL2QFZHIRP4HBm+CbLZ7ts+GLD 5XOGWa84Q9BgRI2HXF4E9PeCQh+ejtnnpDRQlx/cIkX5zt750xXfjArifVS4IUHR fiyfZmNuyn3qqB5O/nz1K/YelKSZtbjc00qlwXU4sfrZRFJgm0PD6oxJqLoU8VVE jBzdbVWsG9KEc91gG0u5UJZyLWGJP2f7I/zrki2WOf9SPfrA01viYw2PSe/81Z7O tADKy076N6Z8ky4HaS1aNsqxx/LTylUh+9O0ccGKSQSpO87LFbrKNilGvIRQYzrj ItUawGsF0KuUEwIDAQABo4ICnTCCApkwdAYIKwYBBQUHAQEEaDBmMDYGCCsGAQUF BzAChipodHRwOi8vY3JsLmZpcm1hcHJvZmVzaW9uYWwuY29tL2Nhcm9vdC5jcnQw LAYIKwYBBQUHMAGGIGh0dHA6Ly9vY3NwLmZpcm1hcHJvZmVzaW9uYWwuY29tMB0G A1UdDgQWBBRiFau1swh5pYf+gNki8I78jxH9eTASBgNVHRMBAf8ECDAGAQH/AgEA MB8GA1UdIwQYMBaAFGXN66s1HgA+ftV0wBy0c0cOGmQvMIIBQQYDVR0gBIIBODCC ATQwggEwBgRVHSAAMIIBJjCB8gYIKwYBBQUHAgIwgeUegeIAQwBlAHIAdABpAGYA aQBjAGEAZABvACAAZABlACAAQQB1AHQAbwByAGkAZABhAGQAIABkAGUAIABDAGUA cgB0AGkAZgBpAGMAYQBjAGkA8wBuAC4AIABDAG8AbgBzAHUAbAB0AGUAIABsAGEA cwAgAGMAbwBuAGQAaQBjAGkAbwBuAGUAcwAgAGQAZQAgAHUAcwBvACAAZQBuACAA aAB0AHQAcAA6AC8ALwB3AHcAdwAuAGYAaQByAG0AYQBwAHIAbwBmAGUAcwBpAG8A bgBhAGwALgBjAG8AbQAvAGMAcABzMC8GCCsGAQUFBwIBFiNodHRwOi8vd3d3LmZp cm1hcHJvZmVzaW9uYWwuY29tL2NwczA7BgNVHR8ENDAyMDCgLqAshipodHRwOi8v Y3JsLmZpcm1hcHJvZmVzaW9uYWwuY29tL2Zwcm9vdC5jcmwwDgYDVR0PAQH/BAQD AgEGMDsGA1UdJQQ0MDIGCCsGAQUFBwMBBggrBgEFBQcDAgYIKwYBBQUHAwMGCCsG AQUFBwMIBggrBgEFBQcDCTANBgkqhkiG9w0BAQsFAAOCAgEAuyL2fYjjyavpt0Fz yNnxL/qGfErI4+Ygf4B1659KUxv7xxZv4YkttzPVZwz/hf++u80OfwPLsVSqn6nI snotWqUwk/nInkOu4sEugHDZRn642hOvRULYK5xeeSFB6yCPZWWym9dQNBZe+JyW vaBa3NNcNe09EXEkM8+xO2x/kksnxzShspGUCNgHAvvjOwuaCGTXikuME5OTPTte NKwJttpgrRk7OEGstDVOM8wQTWSZeZwk3vvc+Oqvb/61jTYCrQi6XhaN+KcztU4W gz1F0y1Ia3qNdZY0VNeLXUsQiCGBb4wpSayBVC6c3ioAc8Xc6kzEcSszLitfUF+o Ou7jfzavDJn9o/oxwtL+nHsHauOY0xMeozrDbKirBiDqra3QhoWch+Z4GRJKlQqy u63OLkXYz0cQCMx9d0OAzSeCN/ZGEoEM13jOE7oHfV1yA4ppu1gOvtOq/U36HQJC

	z2iA34/XHz6+PZybpxokFLvSRQlYyCdNbdRYkWWOj/goV9J65rpx36K0YNDPCNyq 35jggf0fAhMT/CBUj41L9Mdt0WI5y3247LfIrU7q3crNcUEbljH6t1n1ZPC+6w7G GoXQc05gPZo2W5V7Xc0LL82+lf62uSJP4fBM54EEoRIe5+anZGfRz/WDxEbhVTO3 MAyg3DvW8B/5vU+K/ihS2XY2CRQ= -----END CERTIFICATE-----

Junto con la Declaración de Prácticas de Certificación (DPC) y Políticas de Certificados (PC):

- 170110 0.WiP-FP_CPS-r03.docx
- FP_CP_Servidor_Web_SSL-1702dd.docx
- FP_CP_AAPP_Sede_Electronica-1702dd.docx

Para los *Object Identifier* (OID) de certificados siguientes:

- 1.3.6.1.4.1.13177.10.1.3.10 Certificado de SSL EV-256.
- 1.3.6.1.4.1.13177.10.1.20.1 Certificado de sede electrónica nivel alto.
- 1.3.6.1.4.1.13177.10.1.20.2 Certificado de sede electrónica nivel medio.

Resultado de evaluación

En nuestra opinión, basada en los trabajos de auditoría realizados entre el 30 de enero y el 1 de marzo de 2017, el objetivo de evaluación cumple en todos sus aspectos significativos los criterios de evaluación indicados anteriormente. Este anexo del certificado se encuentra supeditado a una auditoría completa de seguimiento antes de abril de 2018.

Este anexo no incluye ninguna opinión profesional acerca de la calidad de los servicios prestados por el Prestador de Servicios de Confianza, ni de su idoneidad para los objetivos concretos de cualquier suscriptor, más allá de los criterios de evaluación cubiertos.

Detalle del resultado de evaluación frente a los requisitos de evaluación

A continuación, se incluye el detalle de los aspectos revisados:

6.1 Publication and repository responsibilities

Cumplimiento.

6.2 Identification and authentication

Cumplimiento.

6.3 Certificate Life-Cycle operational requirements

Cumplimiento con hallazgos.

#1 No ha podido evidenciarse la existencia de instrucciones para que los suscriptores o terceras partes notifiquen posibles problemas con los certificados de autenticación web

6.4 Facility, management, and operational controls

Cumplimiento con hallazgos.

#2 Se dispone de acuerdos firmados con los proveedores en los que se incluyen cláusulas de confidencialidad y protección de datos personales. No obstante, con un proveedor, que realiza las auditorías de las Autoridades de Registro, se dispone de una oferta comercial que no incluye cláusulas relativas a la seguridad de la información y protección de datos.

#3 La entidad dispone del documento "RG10101 - ROLES Y PERFILES" donde se incluye una descripción de cada uno de los roles, así como una relación del personal que ocupa dichos roles. No obstante, el documento no está totalmente actualizado, puesto que no se reflejan en el mismo, alguna de las recientes incorporaciones. Del mismo modo, no se dispone de evidencia de la aceptación de dichos roles de confianza por las personas que los ocupan.

#4 Según la Normativa de Seguridad de Firmaprofesional, los sistemas de gestión de contraseñas deberán garantizar que las contraseñas de acceso a los sistemas operativos cumplen los requisitos de dicha política. Se ha verificado la política de contraseñas establecida en las principales máquinas de la entidad, y se han identificado incumplimientos de dicha política en alguna de estas máquinas.

#5 No se ha evidenciado que se realice una monitorización de las actividades de inicio y parada de los logs o registros en los sistemas.

#6 El plan de terminación del PSC, no contempla alguno de los aspectos requeridos de la cláusula 7.12 de la ETSI 319 401.

#7 En el apartado "5.4.4 Protección de los registros de auditoría" de la CPS, se indica que los logs de los sistemas son protegidos de su manipulación mediante la firma de los ficheros que los contienen. Sin embargo, esta acción no se está realizando en la práctica para todos los logs.

#8 La entidad dispone de un Plan de Continuidad que no incluye alguno de los aspectos indicados en el apartado 6.4.8.

6.5 Technical security controls

Cumplimiento con hallazgos.

#9 La entidad realiza un análisis de vulnerabilidades enmarcado dentro del test de intrusión externo, que se lleva a cabo con una periodicidad anual. No obstante, los test de intrusión llevados a cabo, y por tanto los análisis de vulnerabilidades, son externos por lo que no se ha realizado los requeridos análisis de vulnerabilidades sobre direcciones IP internas. Asimismo, la "CA Browser Forum network security guide" indica que se deben realizar los análisis de vulnerabilidades con una periodicidad de al menos cada 3 meses *(*o ante cambios significativos*)*.

6.6 Certificate, CRL, and OCSP profiles

Cumplimiento

6.7 Compliance audit and other assessment

Cumplimiento

6.8 Other business and legal matters

Cumplimiento con hallazgos.

#10 Al respecto del cumplimiento legal, se ha identificado alguna desviación en el cumplimiento de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

6.9 Other provisions

Cumplimiento con hallazgos.

#11 Se ha evidenciado que existen algunos aspectos a mejorar en la web de Firmaprofesional para su adecuación con el Nivel de Conformidad "A" de las Pautas de Accesibilidad al Contenido en la Web *(WCAG)*.

Todas las no conformidades menores han sido planificadas en el plan de acciones correctivas del PSC.