AENOR

Anexo al Certificado de Prestadores de Servicios de Confianza

PSC-2017/0009

La entidad de evaluación de conformidad, AENOR INTERNACIONAL SAU, conforma el presente anexo al certificado número PSC-2017/0009 a la empresa

AULOCE, S.A.U.

para confirmar que su servicio de confianza:	Servicio de expedición de certificados electrónicos cualificados de firma electrónica
	Servicio de expedición de certificados electrónicos cualificados de sello electrónico
que se realizan en:	Calle Bari, 39 (Edif. Binary Building), CP 50197 de Zaragoza - ESPAÑA
cumple los requisitos definidos en la norma:	CEN/TS 419241:2014
Fecha de primera emisión:	2017-06-26
Fecha de expiración:	2018-06-25

Este anexo del certificado solamente es válido en su totalidad (4 páginas) y en conjunción con Informe de evaluación de conformidad (CAR): "PSC-2017/0009 - AULOCE, S.A. (CAR)" de fecha 26-06-2017

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 CEN/TS 419241:

- CEN/TS 419241:2014 "Security Requirements for Trustworthy Systems supporting Server Signing". European Committee for Standardization

El nivel de control exclusivo *(Level of Sole Control)* evaluado es:

- Level 2

Objetivo de la evaluación

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

SUBJECT:	**CN = ESFIRMA AC AAPP** *X509v3 Subject Key Identifier:* 61:89:6C:BB:3C:1E:BD:2D:44:E0:CB:F0:67:40:29:80:4D:B5:A3:50
ISSUER:	**CN = ESFIRMA AC RAIZ**
Certificado X.509 v3 (PEM 64):	-----BEGIN CERTIFICATE----- MIIIKDCCBhCgAwIBAgIIWiBEClppSdMwDQYJKoZIhvcNAQENBQAwgdMxGDAWBgNV BGEMD1ZBVEVTLUE1MDg3ODg0MjEYMBYGA1UEAwwPRVNGSVJNQSBBQyBSQUlaMSsw KQYDVQQLDCJBVVRPUklEQUQgREUgQ0VSVElGSUNBQ01PTiBFU0ZJUk1BMRYwFAYD VQQKDA1BVUxPQ0UgUy5BLlUuMUswSQYDVQQHDEJaYXJhZ296YSAoc2VlIGN1cnJl bnQgYWRkcmVzcyBhdCBodHRwczovL3d3dy5lc2Zpcm1hLmNvbS9kb2MtcGtpLykx CzAJBgNVBAYTAkVTMB4XDTE2MDQyODE2MDUxNFoXDTI5MDQyODE2MDUxNFowgdox GDAWBgNVBGEMD1ZBVEVTLUE1MDg3ODg0MjEYMBYGA1UEAwwPRVNGSVJNQSBBQyBB QVBQMTIwMAYDVQQLDClBVVRPUklEQUQgREUgQ0VSVElGSUNBQ01PTiBFU0ZJUk1B IC0gQUFQUDEWMBQGA1UECgwNQVVMT0NFIFMuQS5VLjFLMEkGA1UEBwxCWmFyYWdv emEgKHNlZSBjdXJyZW50IGFkZHJlc3MgYXQgaHR0cHM6Ly93d3cuZXNmaXJtYS5j b20vZG9jLXBraS8pMQswCQYDVQQGEwJFUzCCAiIwDQYJKoZIhvcNAQEBBQADggIP ADCCAgoCggIBAJybLPMHyZ6e7SBmK4S8sCHeeDd2GbPtjPGdEnCESnFGGLwJ23YO +PHn9Crho5x2zWkX8LvKxt8LZzv5/wGXmAGnD2FD/hJauE4jbO8jo6VXlPkITMEn 3GVavsJCkhxiM58FBY/cZIdB1AdAU7yaWFlouUDH+uj8O3d2cisN2QqgnIjdcCMH VPbLyOsyTzkOV7oz8Ujo5d/XVY+GcEsmab8yFcMoTqdwSgXld6xrMWqt5QKWA4lL QK9yTlUOYB45tUvr+QdHph48M2lKvexvQFCul3vrk/yrRdLLAnmWttEBZEcwRai9 dMiptceRV3YaafX4OiJvo8v764X5pyQECrPZDUeHOacAgu1HinqTIfNI3V6dozdC NiUmXL+IPWCdszv3ahGGB4ZPE4gkKt0hFtj/VdlHbYmQzWJkUHw82hoLIJXdrJm/ AxGx88qiPvWvGEBmx21aQsDP05tFu3ZZqAlcvZVfLpd1HELCfP0hWHArN37N8JjB 4bNQG1ui+9+sJ2WID2EjMtRuiM2k2YZCSfIdU54LWOqTKIDOJWOqMMtK4vUvOdwg p6qxU7rCeKauOLk/RR+nbnbAk6O3unvTuYujmZTB+ul0H1n40OBNVFE5GwMT+NZ4 GpkKMERtbLjCiPU/i/1masde+R/wWosEQfKpNvYknTe4BiDHUgbVR8bzAgMBAAGj ggH1MIIB8TBOBggrBgEFBQcBAQRCMEAwPgYIKwYBBQUHMAKGMmh0dHBzOi8vd3d3 LmVzZmlybWEuY29tL2RvYy1wa2kvZXNmaXJtYS1hY3JhaXouY3J0MB0GA1UdDgQW BBRhiWy7PB69LUTgy/BnQCmATbWjUDASBgNVHRMBAf8ECDAGAQH/AgEAMB8GA1Ud IwQYMBaAFPzvsx7IeDX3Kzk/FtT1jMHRcbKZMIGsBgNVHSAEgaQwgaEwgZ4GBFUd IAAwgZUwLAYIKwYBBQUHAgEWIGh0dHBzOi8vd3d3LmVzZmlybWEuY29tL2RvYy1w a2kvMGUGCCsGAQUFBwICMFkMV0F1dG9yaWRhZCBkZSBjZXJ0aWZpY2FjacOzbiBJ bnRlcm1lZGlhIGRlIGVzRmlybWEuIFZlciBodHRwczovL3d3dy5lc2Zpcm1hLmNv bS9kb2MtcGtpLzBvBgNVHR8EaDBmMDGgL6AthitodHRwczovL2NybHMxLmVzZmly bWEuY29tL2FjcmFpei9hY3JhaXouY3JsMDGgL6AthitodHRwczovL2NybHMyLmVz ZmlybWEuY29tL2FjcmFpei9hY3JhaXouY3JsMA4GA1UdDwEB/wQEAwIBBjAbBgNV HREEFDASgRBpbmZvQGVzZmlybWEuY29tMA0GCSqGSIb3DQEBDQUAA4ICAQBPpVC1 13eQwuniwRyTaYIwA5oWtbdANs0blzIrt52/V384DzdYIWQRHIJwrLcy7KRzdVSC l1oCVdoRneINCjv0dVaaJOHy11SDoSoSsQ1UopES1Ck3nQ+xV0UTKlJuRhFzA6ex 53hyeaJCQcUnrJqhpPhOB5HoNmrioFhd00fXIp1eEyETKwOKNArvCnYdAY8oNnKT FX13w/X6dmIjJbV8yZ02kus1znNHpjqBGAvfG3+PfPkqv8QZet6c3VOV7ZYL6Ffr

	gUoOj/9ac7lIPbEPSUGhb30Yz8fM26vSiMNUQ1fOXLXBDq52maXA84a+jquN0fu4 xOYvBMmxh+GcK+2jkzW7ujjdzGf6Tr4al1k04rhA2bOI/Y4ZAfQ8I1lTXtftoKSb FZWeHVoz1naNExwTKZH7Rqw7jrC1jB86eRd57q5cFtKTrGtdg0tT96NvsPQsGdft Xv+f7Dux6xnm+V8xaQ6X0Ndmiof6b5yoBfp8bUellAYfdGQmPYdVQTt5rbRU3dQt UJX2eZQRG0m+LdkMGhmB0dlVHIjmDY+yBPxcLn2wfL6L4nz112vaEyLaMyTg3q7y 51bo7dnctEEw4cA5mYTmG3jArAP+MnIQTtKhpG+jY4Avp/7TCQJsRS8HMY8kOXaR k5AVnStfm3q9zxNfyGjmd776bzuEwSI6VbOctg== -----END CERTIFICATE-----

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

- esFIRMA DPC v1r4.pdf

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

- 1.3.6.1.4.1.47281.1.1.4 Certificado de Empleado Público nivel medio en HSM
- 1.3.6.1.4.1.47281.1.3.4 Certificado de Empleado Público con seudónimo nivel medio en HSM
- 1.3.6.1.4.1.47281.1.2.4 Certificado de Sello de Órgano nivel medio en HSM

Resultado de evaluación

En nuestra opinión, basada en los trabajos de auditoría realizados entre el 29 de mayo y el 15 de junio 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 mayo 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:

Cláusula 6.2.1 Management (SRG_M)

Cumplimiento.

Cláusula 6.2.2 Systems and Operations (SRG_SO)

Cumplimiento.

Cláusula 6.2.3 Identification and Authentication (SRG_IA)

Cumplimiento.

Cláusula 6.2.4 System Access Control (SRG_SA)

Cumplimiento.

Cláusula 6.2.5 Key Management (SRG_KM)

Cumplimiento con hallazgos.

#1 La entidad dispone de una planificación donde se contemplan las caducidades y renovaciones de los certificados de la Autoridad de Certificación Raíz (ESFIRMA AC RAIZ) y de la Autoridad de Certificación Subordinada (ESFIRMA AC AAPP). Sin embargo, no se ha evidenciado que se disponga de procedimientos formalizados en este sentido, que describan las todas las acciones necesarias para evitar interrupciones en las operaciones.

Cláusula 6.2.6 Accounting and Auditing (SRG_AA)

Cumplimiento con hallazgos.

#2 Aunque se dispone de una aplicación (splunk) de tratamiento de logs o eventos y establecimiento de alertas, esta es de reciente implantación y aún quedan aspectos por configurar, incluido establecer alertas sobre eventos relevantes como por ej. actividades anormales que indiquen potenciales violaciones de seguridad o intrusión en la red del TSP. Los logs de los distintos sistemas y aplicativos se almacenan en un servidor sin firmar ni cifrar, por lo que están accesibles a los administradores de sistemas de manera que no se asegura su confidencialidad ni integridad.

Cláusula 6.2.7 Archiving (SRG_AR)

Cumplimiento.

Cláusula 6.2.8 Backup and Recovery (SRG_BK)

Cumplimiento con hallazgos.

#3 Ver 6.2.6

Cláusula 6.3.1 SCD Setup (SRC_DS) - Cryptographic key (SRC_DS.1)

Cumplimiento.

Cláusula 6.3.2 Signer Authentication (SRC_SA)

Cumplimiento.

Cláusula 6.3.3 Signature Creation (SRC_SC)

Cumplimiento.

Cláusula 6.4.2 SCD Activation (SRA_DA)

Cumplimiento.

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