

# 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

## 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:	<b>CN = ESFIRMA AC AAPP</b> <i>X509v3 Subject Key Identifier:</i> 61:89:6C:BB:3C:1E:BD:2D:44:FO:CB:FO:67:40:29:80:4D:B5:A3:50
ISSUER:	<b>CN = ESFIRMA AC RAIZ</b>
Certificado X.509 v3 (PEM 64):	<pre> -----BEGIN CERTIFICATE----- MI I I K D C C B h C g A w I B A g I I W i B E C l p p S d M w D Q Y J K o Z I h v c N A Q E N B Q A w g d M x G D A W B g N V B G E M D 1 Z B V E V T L U E l M D g 3 O D g 0 M j E Y M B Y G A 1 U E A w w P R V N G S V J N Q S B B Q y B S Q U l a M S s w K Q Y D V Q Q L D C J B V V R P U k l E Q U Q g R E U g Q 0 V S V E l G S U N B Q 0 l P T i B F U 0 Z J U k 1 B M R Y w F A Y D V Q Q K D A 1 B V U x P Q 0 U g U y 5 B L l U u M U s w S Q Y D V Q Q H D E J a Y X J h Z 2 9 6 Y S A o c 2 V l I G N 1 c n J l b n Q g Y W R k c m V z c y B h d C B o d H R w c z o v L 3 d 3 d y 5 l c 2 Z p c m 1 h L m N v b S 9 k b 2 M t c G t p L y k x C z A J B g N V B A Y T a k V T M B 4 X D T E 2 M D Q y O D E 2 M D U x N F o X D T I 5 M D Q y O D E 2 M D U x N F o g d o x G D A W B g N V B G E M D 1 Z B V E V T L U E l M D g 3 O D g 0 M j E Y M B Y G A 1 U E A w w P R V N G S V J N Q S B B Q y B B Q V B Q M T I w M A Y D V Q Q L D C l B V V R P U k l E Q U Q g R E U g Q 0 V S V E l G S U N B Q 0 l P T i B F U 0 Z J U k 1 B I C 0 g Q U F Q U D E W M B Q G A 1 U E C g w N Q V V M T 0 N F I F M u Q S 5 V L j F L M E k G A 1 U E B w x C W m F y Y W d v e m E g K H N l Z S B j d X J y Z W 5 0 I G F k Z H J l c 3 M g Y X Q g a H R 0 c H M 6 L y 9 3 d 3 c u Z X N m a X J t Y S 5 j b 2 0 v Z G 9 j L X B r a S 8 p M Q s w C Q Y D V Q Q G E w J F U z C C A i I w D Q Y J K o Z I h v c N A Q E B B Q A D g g I P A D C C A g o C g g I B A J y b L P M H y Z 6 e 7 S B m K 4 S 8 s C H e e D d 2 G b P t j P G d E n C E S n F G G L w J 2 3 Y O + P H n 9 C r h o 5 x 2 z W k X 8 L v K x t 8 L Z z v 5 / w G X m A G n D 2 F D / h J a u E 4 j b 0 8 j o 6 V X l P k I T M E n 3 G V a v s J C k h x i M 5 8 F B Y / c Z I d B l A d A U 7 y a W F l o u U D H + u j 8 0 3 d 2 c i s N 2 Q q g n I j d c C M H V P b L y O s y T z k O V 7 o z 8 U j o 5 d / X V Y + G c E s m a b 8 y F c M o T q d w S g X l d 6 x r M W q t 5 Q K W A 4 l L Q K 9 y T l U O Y B 4 5 t U v r + Q d H p h 4 8 M 2 l K v e x v Q F C u l 3 v r k / y r R d L L A n m W t t E B Z E c w R a i 9 d M i p t c e R V 3 Y a a f X 4 0 i J v o 8 v 7 6 4 X 5 p y Q E C r P Z D U e H O a c A g u l H i n q T i f N I 3 V 6 d o z d C N i U m X L + I P W C d s z v 3 a h G G B 4 Z P E 4 g k K t 0 h F t j / v d l H b Y m Q z W J k U H w 8 2 h o L I J X d r J m / A x G x 8 8 q i P v W v G E B m x 2 l a Q s D P 0 5 t F u 3 Z Z q A l c v Z v f L p d 1 H E L C f P 0 h W H A r N 3 7 N 8 J j B 4 b n Q G l u i + 9 + s J 2 W I D 2 E j M t R u i M 2 k 2 Y Z C s f I d U 5 4 L W o q T K I D O J W o q M M t K 4 v U v O d w g p 6 q x U 7 r C e K a u O L k / R R + n b n b A k 6 0 3 u n v T u Y u j m Z T B + u l 0 H 1 n 4 0 0 B N V F E 5 g W M t + N Z 4 G p k K M E R t b L j C i P U / i / l m a s d e + R / w W o s E Q f K p N v Y k n T e 4 B i D H U g b V R 8 b z A g M B A A G j g g H 1 M I B 8 T B O B g g r B g E F B Q c B A Q R C M E A w P g Y I K w Y B B Q U H M A K G M m h 0 d H B z O i 8 v d 3 d 3 L m V z Z m l y b W E u Y 2 9 t L 2 R v Y y l w a 2 k v Z X N m a X J t Y S 1 h Y 3 J h a X o u Y 3 J 0 M B 0 G A 1 U d D g Q W B B R h i W y 7 P B 6 9 L U T g y / B n Q C m A t b W j U D A S B g N V H R M B A f 8 E C D A G A Q H / A g E A M B 8 G A 1 U d I w Q Y M B a A F P z v s x 7 I e D X 3 K z k / F t T l j M H R c b K Z M I G s B g N V H S A E g a Q w g a E w g Z 4 G B F U d I A A w g Z U w L A Y I K w Y B B Q U H A g E W I G h 0 d H B z O i 8 v d 3 d 3 L m V z Z m l y b W E u Y 2 9 t L 2 R v Y y l w a 2 k v M G U G C C s G A Q U F B w I C M F k M V 0 F l d G 9 y a W R h Z C B k Z S B j Z X J 0 a W z P Y 2 F j a c O z b i B J b n R l c m 1 l Z G l h I G R l I G V z R m l y b W E u I F Z l c i B o d H R w c z o v L 3 d 3 d y 5 l c 2 Z p c m 1 h L m N v b S 9 k b 2 M t c G t p L z B v B g N V H R 8 E a D B m M D G g L 6 A t h i t o d H R w c z o v L 2 N y b H M x L m V z Z m l y b W E u Y 2 9 t L 2 F j c m F p e i 9 h Y 3 J h a X o u Y 3 J s M D G g L 6 A t h i t o d H R w c z o v L 2 N y b H M y L m V z Z m l y b W E u Y 2 9 t L 2 F j c m F p e i 9 h Y 3 J h a X o u Y 3 J s M A 4 G A 1 U d D w E B / w Q E A w I B B j A b B g N V H R E E F D A S g R B p b m Z v Q G V z Z m l y b W E u Y 2 9 t M A 0 G C S q G S I b 3 D Q E B D Q U A A 4 I C A Q B P p V C 1 1 3 e Q w u n i w R y T a Y I w A 5 o W t b d A n s 0 b l z I r t 5 2 / V 3 8 4 D z d Y I W Q R H I J w r L c y 7 K R z d V S C 1 l o C V d o R n e I N C j v 0 d V a a J O H y 1 1 S D o S o S s Q 1 U o p E S 1 C k 3 n Q + x V 0 U T K l J u R h F z A 6 e x 5 3 h y e a J C Q c U n r J q h p P h o B 5 H o N m r i o F h d 0 0 f X I p l e E y E T K w O K N A r v C n Y d a Y 8 o N n K T F X 1 3 w / X 6 d m I j J b V 8 y Z 0 2 k u s 1 z n N H p j q B G A v f G 3 + P f P k q v 8 Q Z e t 6 c 3 V O V 7 Z Y L 6 F f r </pre>

<pre>gUoOj / 9ac71IPbEPSUGhb30Yz8fM26vSiMNUQ1fOXLXBDq52maXA84a+jquN0fu4 xOYvBMmxh+GcK+2jkzW7uujdzGf6Tr4a11k04rhA2bOI/Y4ZAFQ8I11TXtftoKSb FZWeHVoz1naNEExwTKZH7Rqw7jrc1jB86eRd57q5cFtKTrGtdg0tT96NvsPQsGdft Xv+f7Dux6xnm+V8xaQ6XONdmiof6b5yoBfp8bUe11AYfdGQmPYdVQTt5rbRU3dQt UJX2eZQRG0m+LdkMGhmB0d1VHIjmdY+yBPxcLn2wfL6L4nz112vaEyLaMyTg3q7y 51bo7dnctEEw4cA5mYtmG3jArAP+MnIQTtKhpG+jY4Avp/7TCQJsRS8HMY8kOXaR k5AVnStfm3q9zxNfyGjmd776bzuewSI6VbOctg== -----END CERTIFICATE-----</pre>
--

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.