AENOR

Anexo al Certificado de Prestadores de Servicios de Confianza

PSC-2017/0002

La entidad de evaluación de conformidad, AENOR INTERNACIONAL SAU, conforma el presente anexo al certificado número 2017/9901/PSC/01 a la empresa

CONSORCI ADMINISTRACIÓ OBERTA DE CATALUNYA

para confirmar que su servicio de confianza:	Servicio de expedición de certificados electrónicos cualificados de autenticación de sitios web
que se realizan en:	CARRER DE TÀNGER, 98. (PLANTA BAIXA) 08018 BARCELONA - ESPAÑA
cumple los requisitos definidos en la norma:	ETSI EN 319 411-2 v2.1.1
Fecha de primera emisión:	2017-06-26
Fecha de expiración:	2018-06-25

Este anexo del certificado solamente es válido en su totalidad (5 páginas) y en conjunción con Informe de evaluación de conformidad (CAR): "PSC-2017/0002 – CONSORCI ADMINISTRACIÒ OBERTA DE CATALUNYA (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

ENAC
CERTIFICACIÓN
Nº 1/C-PR322

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=EC-SectorPublic** *X509v3 Subject Key Identifier*: 47:3C:DE:14:77:BB:6A:4F:47:91:A9:02:FF:D4:06:E1:73:DC:E2:D9
ISSUER:	**CN = EC-ACC**
Certificado X.509 v3 (PEM 64):	-----BEGIN CERTIFICATE----- MIIF4zCCBMugAwIBAgIQcbBlOXyOB9JUGpZ/dVk3kjANBgkqhkiG9w0BAQsFADCB 8zELMAkGA1UEBhMCRVMxOzA5BgNVBAoTMkFnZW5jaWEgQ2F0YWxhbmEgZGUgQ2Vy dGlmaWNhY2lvIChOSUYgUS0wODAxMTc2LUkpMSgwJgYDVQQLEx9TZXJ2ZWlzIFB1 YmxpY3MgZGUgQ2VydGlmaWNhY2lvMTUwMwYDVQQLEyxWZWdldSBodHRwczovL3d3 dy5jYXRjZXJ0Lm5ldC92ZXJhcnJlbCAoYykwMzE1MDMGA1UECxMsSmVyYXJxdWlh IEVudGl0YXRzIGRlIENlcnRpZmljYWNpbyBDYXRhbGFuZXMxDzANBgNVBAMTBkVD LUFDQzAeFw0xNDA5MTgwODIzMjdaFw0zMDA5MTgwODIzMjdaMIGIMQswCQYDVQQG EwJFUzEzMDEGA1UECgwqQ09OU09SQ0kgQURNSU5JU1RSQUNJTyBPQkVSVEEgREUg Q0FUQUxVTllBMSowKAYDVQQLDCFTZXJ2ZWlzIFDDumJsaWNzIGRlIENlcnRpZmlj YWNpw7MxGDAWBgNVBAMMD0VDLVNlY3RvclB1YmxpYzCCASIwDQYJKoZIhvcNAQEB BQADggEPADCCAQoCggEBAMuuTjExvPHbEfGJ3MU9RznScEIL86TETwZTO1GZsF1v RrGAJBV3QcXSXp9/r5h7cyq19DKLTiqRtKmnwSDfQCHbtv4mIJWc8mbEZCRwQ2fp 1TRV1YGFnUZghLh32PjSrjlcZcTH5rAaS8uGXdITf4Amms9wa+Ax705XFCd52sji B4qUJtp6hMC7ECCHjWbLw0Akp4vPiPfbhLAxg400869eaMyEdkQsQYxgzyrEE9mo NFRV66y3iB8env1QmN/NkMqdKlgy86HP22PrSed4fONGSB2mz/Ti4qfGY1eoroPn m5Q8IiWtvfDaBKi/DW5j+ogUJ7+2w6fMAbVZUsHWo8MCAwEAAaOCAdowggHWMBIG A1UdEwEB/wQIMAYBAf8CAQAwDgYDVR0PAQH/BAQDAgEGMB0GA1UdDgQWBBRHPN4U d7tqT0eRqQL/1Abhc9zi2TAfBgNVHSMEGDAWgBSgw4tEqjelRb+XgFrR8Xiim+ld jTCB1gYDVR0gBIHOMIHLMIHIBgRVHSAAMIG/MDEGCCsGAQUFBwIBFiVodHRwczov L3d3dy5hb2MuY2F0L0NBVENlcnQvUmVndWxhY2lvMIGJBggrBgEFBQcCAjB9DHtB cXVlc3QgY2VydGlmaWNhdCDDqXMgZW3DqHMgw7puaWNhIGkgZXhjbHVzaXZhbWVu dCBhIEVudGl0YXRzIGRlIENlcnRpZmljYWNpw7MuIFZlZ2V1IGh0dHBzOi8vd3d3 LmFvYy5jYXQvQ0FUQ2VydC9SZWd1bGFjaW8wMwYIKwYBBQUHAQEEJzAlMCMGCCsG AQUFBzABhhdodHRwOi8vb2NzcC5jYXRjZXJ0LmNhdDBiBgNVHR8EWzBZMFegVaBT hidodHRwOi8vZXBzY2QuY2F0Y2VydC5uZXQvY3JsL2VjLWFjYy5jcmyGKGh0dHA6 Ly9lcHNjZDIuY2F0Y2VydC5uZXQvY3JsL2VjLWFjYy5jcmwwDQYJKoZIhvcNAQEL BQADggEBADMRO0eqGiqUdIFFbxqwKXh+K6rXGJAnfgYI4bABMbbIAZaDklfwXj23 BO8JxLPMzgIilTXgswBSZTbTVEujYQfP+lrUjP1ZG2XFPM+vKzsyF4K3s3FyfjdR mj0chun0Flao+gd9nl6j7ySzHspZb1u/i0LSz4/48mY+pTxT1HCVw4zvzm9E9X26 uKxn/UikI9B5EECHGChxw5Cx1RSF7THvhEBXfCQ6wsY632uvhi/H4QAkzmOZkh1P VzzehlsK2telJGfAt+xIxLHYvRUOTC5MRpSt2EzqvTjdsC8gKzGvgqYEhZBqrq7V PnbUX9LuF9aeJlZXPsfNRaIkAJW8smo= -----END CERTIFICATE-----

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

- D1111E0650N-PGdCv5r0draftCAT-r01.pdf
- D1111E0650N-DPCEC-SectorPublicv2r0draft2CAT.pdf

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

- 1.3.6.1.4.1.15096.1.3.2.5.2 CDS-1 SENM - Certificat de seu electrònica de nivell mig, emès per l'EC-SECTORPUBLIC
- 1.3.6.1.4.1.15096.1.3.2.51.2 Certificat de dispositiu SSL EV
-

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 La PC correspondiente a EC-SectorPublic establece los requisitos y circunstancias para la suspensión de certificados. Sin embargo, no se incluye la excepción para los certificados de autenticación web, cuando no es posible la suspensión de este tipo de certificados. Cabe indicar que se han detectado certificados suspendidos con más de 120 días en dicha CRL contradiciendo lo establecido en la propia política.

#2 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.

#3 En el aparatado 5.2.1 de la DPC se definen los roles de confianza y las funciones de cada uno de ellos. No obstante, no todos los roles de confianza se encuentran asignados. Igualmente, los roles de confianza no están aceptados por la dirección y por las personas que ocupan dichos roles.

#4 Respecto al control de acceso lógico, se han identificado ciertas desviaciones tales como una cuenta de usuario administrador del dominio que está en desuso, pero sigue habilitada, las principales máquinas Linux que soportan la infraestructura PKI no cumplen estrictamente con la política de contraseñas especificada en la Normativa de creación y uso de contraseñas, respecto a los parámetros de caducidad, complejidad e histórico. Asimismo, se ha verificado que los usuarios no han cambiado la contraseña desde hace más de un año en dichas máquinas Linux.

#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 CAOC está adherido al Plan de Continuidad de Firmaprofesional, que cubre la infraestructura PKI. Entre los escenarios de desastre contemplados se incluye el compromiso de las claves. No obstante, el CAOC no dispone de un Plan de Continuidad particular que cubra aquello que no está dentro del alcance del Plan de Continuidad de Firmaprofesional *(*p.ej. servidor web, controlador de dominio, instalaciones de oficinas, personal, etc.*)*. La entidad indica que actualmente está trabajando en este aspecto.

#7 El CAOC está adherido al Plan de Continuidad de Firmaprofesional que contempla el escenario de pérdida, compromiso o sospecha de compromiso de la clave privada. Asimismo, este escenario se describe en el apartado 5.7.3 de la DPC. No obstante, no se incluye en este escenario de forma explícita la necesidad de revocar cualquier certificado de la CA que haya sido emitido por el PSC comprometido.

#8 No se contempla en el plan de terminación del PSC, que se mantendrá o transferirá a una parte de confianza sus obligaciones de poner a disposición su clave pública a las partes interesadas durante un período razonable. Igualmente, no se contempla que se disponga de un acuerdo para cubrir los costes que permita cumplir los requisitos mínimos de terminación en caso de quiebra del PSC, o por otras razones por las que no pueda cubrir los costes por sí mismo.

6.5 Technical security controls

Cumplimiento con hallazgos.

#9 Se dispone de antivirus instalado en los equipos del CAOC y se gestiona desde consola centralizada. Se ha verificado que en general está instalado el antivirus en los equipos y servidores *(*como el controlador de dominio*)*. Sin embargo, se ha detectado que, en el servidor web, que funciona con sistema operativo Windows, no se dispone de antivirus instalado. Según se ha indicado, esta casuística se debe a que el antivirus interfería con la realización de las copias de seguridad y la entidad está tratando de solucionar esta situación.

#10 Respecto a la infraestructura PKI, se 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.

#11 En el apartado 9.15 de la DPC se establece la normativa aplicable a la entidad. Sin embargo, se han evidenciado incumplimientos al respecto del Esquema Nacional de Seguridad para el que no se han asignado los niveles de cada servicio que ofrece y respecto al cumplimiento de la LOPD y el RLOPD no se ha evidenciado que se hayan realizado auditorías de protección de datos, tal como se requiere por el artículo 96 del RLOPD.

6.9 Other provisions

Cumplimiento con hallazgos.

#12 A pesar de que las webs del CAOC (www.aoc.cat, www.idcat.cat) cumplen con ciertos requisitos mínimos de accesibilidad, se ha evidenciado que existen algunos aspectos a mejorar, que no cumplen con el Nivel de adecuación Prioridad 1 (se encarga de características básicas que una página Web tiene que cumplir para ser accesible), tal como se indica en los informes de accesibilidad web realizado por el Observatorio de Accesibilidad.

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