AENOR

Appendix to the Certificate of Trust Service Provider

PSC-2019/003

The Conformity Assessment Body, AENOR INTERNACIONAL SAU, issues this appendix to certificate number PSC-2019/003 to the organization:

FÁBRICA NACIONAL DE MONEDA Y TIMBRE - REAL CASA DE LA MONEDA

to confirm that its trust service:	Certificates for website authentication
provided at:	Jorge Juan, 106. Madrid 28009
complies with the requirements defined in standard:	ETSI EN 319 411-1 v1.2.2
First issuance date:	2019-04-09
Updating date:	2020-03-23
Expiration date:	2021-03-22

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

Rafael GARCÍA MEIRO
Director General

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-2019/003

Assessment criteria

The assessment criteria are defined in standard ETSI EN 319 411-2:

- 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", European Telecommunications Standards Institute

The applicable ETSI Certification Policies are:

- ETSI EN 319 411-1, OVCP: Organizational Validation Certificate Policy

Audit period

The Audit was carried out at the TSP sites in Madrid, Spain between January 27, 2020 and February 07, 2020.

The audit was carried out as a period audit and covered the period from the January 13, 2019 until January 12, 2020

Assessment scope

The scope of the assessment includes the following CA certificates:

Root CAs
1. OU= AC RAIZ FNMT-RCM
4. AC RAIZ FNMT-RCM SERVIDORES SEGUROS
OV SSL Issuing CAs
2. AC Administración Pública
3. AC Componentes Informáticos
5. AC SERVIDORES SEGUROS TIPO2

*See Appendix A

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

- DECLARACIÓN GENERAL DE PRÁCTICAS DE SERVICIOS DE CONFIANZA Y DE CERTIFICACIÓN ELECTRÓNICA (DGPCv5_5.pdf)
- DECLARACIÓN DE PRÁCTICAS Y POLÍTICAS DE CERTIFICACIÓN DE CERTIFICADOS DE AUTENTICACIÓN DE SITIOS WEB (DPC_AutSitiosWEB_1_2.pdf)
- POLÍTICAS Y PRÁCTICAS DE CERTIFICACIÓN PARTICULARES EN EL ÁMBITO DE LAS ADMINISTRACIONES PÚBLICAS, ORGANISMOS Y ENTIDADES DE DERECHO PÚBLICO (PC-DPC-APv3.5.pdf)
- POLÍTICA Y PRÁCTICAS DE CERTIFICACIÓN PARTICULARES DE LOS CERTIFICADOS DE COMPONENTE "AC COMPONENTES INFORMÁTICOS" (PC-DPC-COMP.v1.10.pdf)

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

- 1.3.6.1.4.1.5734.3.9.16 - OVCP (AC Componentes Informáticos)
- 1.3.6.1.4.1.5734.3.9.17 - OVCP (AC Componentes Informáticos)
- 1.3.6.1.4.1.5734.3.9.18 - OVCP (AC Componentes Informáticos)
- 1.3.6.1.4.1.5734.3.16.2.1 - OVCP (AC SERVIDORES SEGUROS TIPO2)
- 1.3.6.1.4.1.5734.3.16.2.2 - OVCP (AC SERVIDORES SEGUROS TIPO2)
- 1.3.6.1.4.1.5734.3.16.2.3 - OVCP (AC SERVIDORES SEGUROS TIPO2)
- 1.3.6.1.4.1.5734.3.3.8.1 - OVCP (AC Administración Pública)

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 February 2021.

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 with findings

#1 Although the entity has provided updated versions of CPS, not all of them had been published in the repositories at the audit date.

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

6.3 Certificate Life-Cycle operational requirements

Compliance

6.4 Facility, management, and operational controls

Compliance with findings

#2 We could not find evidence of the formal definition and assignment of the validation specialist profile, as specified in BRG and EVCG, even though there are individuals performing the validation functions as a matter of course.

#3 It was noted that a number of events are not being logged and monitored. However, it was confirmed that most relevant events are being logged and centrally stored and monitored using the SIEM tool Qradar.

#4 Dual control is required in order to obtain the trusted roles credentials to access the PKI systems. However, it was noted that while the credentials are being used, they are temporarily stored in a safe in the PKI Data Center, which does not require dual control access.

6.5 Technical security controls

Compliance.

6.6 Certificate, CRL, and OCSP profiles

Compliance

6.7 Compliance audit and other assessment

Compliance.

6.8 Other business and legal matters

Compliance.

6.9 Other provisions

Compliance with findings.

#5 Although follow-up actions have been performed aimed at improving the level of compliance of the public website with regards to accessibility standards, a number of aspects of improvement have been identified for the compliance with WCAG 2.0 level AA of accessibility for people with disabilities in the websites requesting certificates.

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-2019/003

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	OU=AC RAIZ FNMT-RCM, O=FNMT-RCM, C=ES	OU=AC RAIZ FNMT-RCM, O=FNMT-RCM, C=ES	5D938D306736C8061D1AC754846907	rsaEncryption	4096 bit	sha256WithRSAEncryption	Oct 29 15:59:56 2008 GMT	Jan 1 00:00:00 2030 GMT	F7:7D:C5:FD:C4:E8:9A:1B:77:64:A7:F5:1D:A0:CC:BF:87:60:9A:6D	EBC5570C29018C4D67B1AA127BAF12F703B4611EBC17B7DAB5573894179B93FA
1	2	OU=AC RAIZ FNMT-RCM, O=FNMT-RCM, C=ES	OU=AC RAIZ FNMT-RCM, O=FNMT-RCM, C=ES	0E1CD8CD45325A4700510CAAC2DB1E	rsaEncryption	4096 bit	sha512WithRSAEncryption	Oct 29 15:59:56 2008 GMT	Jan 1 00:00:00 2030 GMT	F7:7D:C5:FD:C4:E8:9A:1B:77:64:A7:F5:1D:A0:CC:BF:87:60:9A:6D	B82210CDE9DDEA0E14BE29AF647E4B32F96ED2A9EF1AA5BAA9CC64B38B6C01CA
1	3	OU=AC RAIZ FNMT-RCM, O=FNMT-RCM, C=ES	OU=AC RAIZ FNMT-RCM, O=FNMT-RCM, C=ES	81BBDD6B241FDAB4BE8F1BDA0855C4	rsaEncryption	4096 bit	sha1WithRSAEncryption	Oct 29 15:59:55 2008 GMT	Jan 1 00:00:00 2030 GMT	F7:7D:C5:FD:C4:E8:9A:1B:77:64:A7:F5:1D:A0:CC:BF:87:60:9A:6D	4D9EBB28825C9643AB15D54E5F9614F13CB3E95DE3CF4EAC971301F320F9226E
2	1	CN=AC Administración Pública, serialNumber=Q2826004J, OU=CERES, O=FNMT-RCM, C=ES	OU=AC RAIZ FNMT-RCM, O=FNMT-RCM, C=ES	1	rsaEncryption	2048 bit	sha1WithRSAEncryption	May 21 09:26:24 2010 GMT	May 21 09:52:26 2022 GMT	14:11:E2:B5:2B:B9:8C:98:AD:68:D3:31:54:40:E4:58:5F:03:1B:7D	18A43C51D08174C3A6D85F1C1318BD2909753E75D91CF6599F73347B00702890
2	2	CN=AC Administración Pública, serialNumber=Q2826004J, OU=CERES, O=FNMT-RCM, C=ES	OU=AC RAIZ FNMT-RCM, O=FNMT-RCM, C=ES	2	rsaEncryption	2048 bit	sha256WithRSAEncryption	May 21 09:26:24 2010 GMT	May 21 09:57:08 2022 GMT	14:11:E2:B5:2B:B9:8C:98:AD:68:D3:31:54:40:E4:58:5F:03:1B:7D	830FF205AE69485059C3FB2376A7F2F9EE1C2A61DE259DD09D0BB6AD69F88832
3	1	OU=AC Componentes Informáticos, O=FNMT-RCM, C=ES	OU=AC RAIZ FNMT-RCM, O=FNMT-RCM, C=ES	3E7CFD54CDE5E16D51CC498E1B1ECD48	rsaEncryption	2048 bit	sha1WithRSAEncryption	Jun 27 14:17:50 2013 GMT	Jun 27 14:17:50 2028 GMT	19:F8:58:2F:14:D6:A6:CC:9B:04:98:08:0D:4C:D7:AB:00:A7:83:65	DB0DA16032F1643A2496FDE742E2BBE81DACA58CD7612061420E154CE1BCE2BD
3	2	OU=AC Componentes Informáticos, O=FNMT-RCM, C=ES	OU=AC RAIZ FNMT-RCM, O=FNMT-RCM, C=ES	34C6AB044E36991251C8250B6C94D6C0	rsaEncryption	2048 bit	sha256WithRSAEncryption	Jun 24 10:52:59 2013 GMT	Jun 24 10:52:59 2028 GMT	19:F8:58:2F:14:D6:A6:CC:9B:04:98:08:0D:4C:D7:AB:00:A7:83:65	F038421F07F20D63A20D3691E5A178AB8459EBE570C1647B7690554EF23876AB
4	1	CN=AC RAIZ FNMT-RCM SERVIDORES SEGUROS, 2.5.4.97=VATES-Q2826004J, OU=Ceres, O=FNMT-RCM, C=ES	CN=AC RAIZ FNMT-RCM SERVIDORES SEGUROS, 2.5.4.97=VATES-Q2826004J, OU=Ceres, O=FNMT-RCM, C=ES	62F6326CE5C4E3685C1B62DD9C2E9D95	id-ecPublicKey	384 bit	ecdsa-with-SHA384	Dec 20 09:37:33 2018 GMT	Dec 20 09:37:33 2043 GMT	01:B9:2F:EF:BF:11:86:60:F2:4F:D0:41:6E:AB:73:1F:E7:D2:6E:49	554153B13D2CF9DDB753BFBE1A4E0AE08D0AA4187058FE60A2B862B2E4B87BCB
5	1	CN=AC SERVIDORES SEGUROS TIPO2, 2.5.4.97=VATES-Q2826004J, OU=Ceres, O=FNMT-RCM, C=ES	CN=AC RAIZ FNMT-RCM SERVIDORES SEGUROS, 2.5.4.97=VATES-Q2826004J, OU=Ceres, O=FNMT-RCM, C=ES	138E6BBEDF20F5945C1B6CF629B42F4A	id-ecPublicKey	384 bit	ecdsa-with-SHA384	Dec 20 10:20:38 2018 GMT	Dec 20 10:20:38 2033 GMT	C5:F2:05:4E:F4:37:72:E4:EA:4F:02:57:03:FD:86:96:05:AE:50:8F	9FF23CB9387B9E0083BD5AA1954EEDDF792890AA8E67CD4D38DD28AF4A439AD8