AENOR

Appendix to the Certificate of Trust Service Provider

PSC-2019/0003

The Conformity Assessment Body, AENOR INTERNACIONAL SAU, issues this appendix to certificate number PSC-2019/0003 to the organization:

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

to confirm that its trust service:	Qualified certificates for electronic signatures Qualified certificates for electronic seals Qualified certificates for website authentication
provided at:	JORGE JUAN, 106. MADRID 28009
complies with the requirements defined in standard:	ETSI EN 319 411-2 v2.1.1
First issuance date:	2019-04-09
Updating date:	2019-04-09
Expiration date:	2020-04-09

This appendix to the certificate is valid only in its entirety (6 pages) and in conjunction with Conformity Assessment Report (CAR): "PSC-2019-0003 - FNMT." dated 09-04-2019

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-2019/0003

Assessment criteria

The assessment criteria are defined in standard 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

The applicable ETSI Certification Policies are:

- QCP-n Policy for EU qualified certificate issued to a natural person
- QCP-n-qscd Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD
- QCP-l: Policy for EU qualified certificate issued to a legal person
- QCP-w: Policy for EU qualified website certificate issued to a natural or a legal person and linking the website to that person.

Audit period

The Audit was carried out at the TSP sites in Madrid, Spain between January 21st, 2019 (2019-01-21) and February 6th, 2019 (2019-02-06) with additional checks performed up until Marth 26th 2019 (2019-03-26).

The audit was carried out as a period audit and covered the period from the January 13th, 2018 (2018-01-13) until January 12th, 2019 (2019-01-12)

Assessment scope

The scope of the assessment includes the following CA certificates:

Root CAs
1. AC RAIZ FNMT-RCM
7. AC RAIZ FNMT-RCM SERVIDORES SEGUROS
QCP-n Issuing CAs
2. AC Administración Pública
4. AC FNMT Usuarios
5. AC Representación
QCP-l Issuing CAs
2. AC Administración Pública
3. AC Componentes Informáticos
QCP-w Issuing CAs
2. AC Administración Pública
8. AC SERVIDORES SEGUROS TIPO1
Timestamp CAs
6. AUTORIDAD DE SELLADO DE TIEMPO FNMT-RCM - TSU 2016

*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_4.pdf)
- DECLARACIÓN DE PRÁCTICAS Y POLÍTICAS DE CERTIFICACIÓN DE CERTIFICADOS DE AUTENTICACIÓN DE SITIOS WEB (DPC_AutSitiosWEB_1_0.pdf)
- DECLARACIÓN DE PRÁCTICAS Y POLÍTICAS DE CERTIFICACIÓN DE CERTIFICADOS DE FIRMA ELECTRÓNICA CENTRALIZADA PARA EMPLEADOS PÚBLICOS (DPC_EmpPúblico_Firma_centralizada_1.1.pdf)
- DECLARACIÓN DE PRÁCTICAS Y POLÍTICAS DE CERTIFICACIÓN DE CERTIFICADOS CUALIFICADOS DE SEDE ELECTRÓNICA (DPC_Sedes_1_0.pdf)

Appendix to the Certificate for Trust Service Provider: PSC-2019/0003

- POLÍTICA Y PRÁCTICAS DEL SERVICIO CUALIFICADO DE SELLADO DE TIEMPO (DPSCSTv1_1.pdf)
- POLÍTICAS Y PRÁCTICAS DE CERTIFICACIÓN PARTICULARES EN EL ÁMBITO DE LAS ADMINISTRACIONES PÚBLICAS, ORGANISMOS Y ENTIDADES DE DERECHO PÚBLICO (PC-DPC-APv3.3.pdf)
- POLÍTICA Y PRÁCTICAS DE CERTIFICACIÓN PARTICULARES DE LOS CERTIFICADOS DE COMPONENTE "AC COMPONENTES INFORMÁTICOS" (PC-DPC-COMP.v1.8.pdf)
- POLÍTICA Y PRÁCTICAS DE CERTIFICACIÓN PARTICULARES DE LOS CERTIFICADOS DE PERSONAS FÍSICAS DE LA "AC FNMT USUARIOS" (PC-DPC-PersonasFísicas v1.4.pdf)
- POLÍTICA Y PRÁCTICAS DE CERTIFICACIÓN PARTICULARES DE LOS CERTIFICADOS DE REPRESENTANTE DE PERSONAS JURÍDICAS Y DE ENTIDADES SIN PERSONALIDAD JURÍDICA DE LA "AC REPRESENTACIÓN" (PC-DPC-Representación v1.6.pdf)

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

- 1.3.6.1.4.1.5734.3.10.1 - QCP-n (AC FNMT Usuarios)
- 1.3.6.1.4.1.5734.3.11.1 - QCP-n (AC Representación)
- 1.3.6.1.4.1.5734.3.11.2 - QCP-n (AC Representación)
- 1.3.6.1.4.1.5734.3.11.3 - QCP-n (AC Representación)
- 1.3.6.1.4.1.5734.3.16.1.1 - QCP-w (AC SERVIDORES SEGUROS TIPO1)
- 1.3.6.1.4.1.5734.3.16.1.2 - QCP-w (AC SERVIDORES SEGUROS TIPO1)
- 1.3.6.1.4.1.5734.3.16.1.3 - QCP-w (AC SERVIDORES SEGUROS TIPO1)
- 1.3.6.1.4.1.5734.3.3.10.1 - QCP-n-qscd (AC Administración Pública)
- 1.3.6.1.4.1.5734.3.3.11.1 - QCP-n (AC Administración Pública)
- 1.3.6.1.4.1.5734.3.3.4.4.1 - QCP-n (AC Administración Pública)
- 1.3.6.1.4.1.5734.3.3.4.4.2 - QCP-n (AC Administración Pública)
- 1.3.6.1.4.1.5734.3.3.9.1 - QCP-l (AC Administración Pública)
- 1.3.6.1.4.1.5734.3.9.19 - QCP-l (AC Componentes Informáticos)
- 1.3.6.1.4.1.5734.3.3.12.1 - QCP-w (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 2020.

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:

6.1 Publication and repository responsibilities

Compliance.

6.2 Identification and authentication

Compliance.

6.3 Certificate Life-Cycle operational requirements

Compliance with findings.

#1 In the case of the QCP-w certificates that will be issued by "AC SERVIDORES SEGUROS TIPO1" with the new validation platform, evidence has been found during the tests, that the same operator can perform both the validation and the approval of the certificate request, therefore not complying with the requirements of section 14.1.3 of EVCG.

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.

In addition, we could not find evidence that the personnel that are currently performing the functions of validation specialist have received specific training during the audit period.

#3 The incidents that have an impact on the availability of the services are not classified as security incidents and, as a result, they do not follow the same management and notification processes as the rest of the security incidents.

6.5 Technical security controls

Compliance.

#4 We have not been able to find evidence of the TSP's monitorization procedures of the status of the QSCD certification or the appropriate measures in case of loss of status as QSCD in the CPS.

6.6 Certificate, CRL, and OCSP profiles

Compliance with findings.

#5 We have evidence qualified certificates issued with errors:

- *(*QCP-n*)* 1.3.6.1.4.1.5734.3.3.4.4.2*:* Certificates with *organizationName* or *organizationUnitName* bigger than 64 characters.
- *(*QCP-n*)* 1.3.6.1.4.1.5734.3.3.4.4.1*:* Certificates with zero length in *Subject Alternative Name*.
- *(*QCP-l*)* 1.3.6.1.4.1.5734.3.3.9.1*:* Certificates with *organizationName* or *commonName* bigger than 64 characters. Certificates with additional *keyUsages* tan permitted *(*Data Encipherment*)*
- *(*QCP-l*)* 1.3.6.1.4.1.5734.3.9.19*:* Certificates with additional *keyUsages* tan permitted *(*Data Encipherment*)*. Issuer without *commonName*.

6.7 Compliance audit and other assessment

Compliance.

6.8 Other business and legal matters

Compliance.

6.9 Other provisions

Compliance with findings.

#6 Although follow-up and actions are performed aimed at improving the level of compliance of the public website with regards to accessibility standards, 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.

#7 The entity makes available the CPS and CP, including adherence to the requirements of the CA / B Forum, although the adherence to the EVCGs requirements in the general CPS are not included.

It should be noted that we have not been able to find evidence of the availability of test sites for the new hierarchy "AC RAIZ FNMT-RCM SERVIDORES SEGUROS".

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-2019/0003

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
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	3	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	4	CN=AC FNMT Usuarios, OU=Ceres, O=FNMT-RCM, C=ES	OU=AC RAIZ FNMT-RCM, O=FNMT-RCM, C=ES	455F3AE15C21CDBA544F82AA4751EBDB	rsaEncryption	2048 bit	sha256WithRSAEncryption	Oct 28 11:48:58 2014 GMT	Oct 28 11:48:58 2029 GMT	B1:D4:4F:C4:23:79:FA:44:05:09:C6:EB:39:CF:E8:35:B0:B8:20:64	601293CA20B09A03295D196256C6953FF9EBA811DB8E3CE140413C1BFFE9A869
5	5	CN=AC Representación, OU=CERES, O=FNMT-RCM, C=ES	OU=AC RAIZ FNMT-RCM, O=FNMT-RCM, C=ES	61C2D4D4F6A9AE77559266B98DAFD621	rsaEncryption	2048 bit	sha256WithRSAEncryption	Jun 30 09:51:53 2015 GMT	Dec 31 10:51:53 2029 GMT	DC:50:96:9F:D7:31:89:C9:11:E4:EF:96:5F:F6:5F:82:52:46:62:53	8FD16A179944D5D1D420AF09405EDA7ABF2A9C742883E8C2F89E0D90AFAF754B
6	6	CN=AUTORIDAD DE SELLADO DE TIEMPO FNMT-RCM - TSU 2016, 2.5.4.97=VATES-Q2826004J, OU=CERES, O=FÁBRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA, C=ES	OU=AC Componentes Informáticos, O=FNMT-RCM, C=ES	15499A8BC209E3C8583828D7A9E09768	rsaEncryption	3072 bit	sha256WithRSAEncryption	Nov 25 12:04:39 2016 GMT	Nov 25 12:04:39 2022 GMT	A1:F6:70:6D:CC:7E:8D:3B:CC:3C:93:E2:DE:94:9B:B1:45:9F:1F:9F	08F2934C394D89DDB0CFC386AAF5C52E4F17AFBBBE1C67A03611132F80BEB7A9
7	7	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
8	8	CN=AC SERVIDORES SEGUROS TIPO1, 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	508986CDB4170EFE5C1B6BD5C824EB5B	id-ecPublicKey	384 bit	ecdsa-with-SHA384	Dec 20 10:15:49 2018 GMT	Dec 20 10:15:49 2033 GMT	8C:42:32:40:F9:79:3F:6B:13:C1:75:C6:5D:EE:86:22:44:39:6F:77	1EDB6BD91274882DB795BFC514F8AABE10AD955CBCCFD3FD5A5B5FEBB2CE5B68