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: | Certificate for website authentication |
| provided at: | JORGE JUAN, 106. MADRID 28009 |
| complies with the requirements defined in standard: | ETSI EN 319 411-1 v1.1.1 |
| 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 (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

## Assessment criteria

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

- ETSI EN 319 411-1 V1.1.1 (2016-02): "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements", Version 1.1.1, 2016-02, European Telecommunications Standards Institute

The applicable ETSI Certification Policies are:

- OVCP: Organizational Validation Certificate Policy

## 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 until March 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. 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_4.pdf)
- DECLARACIÓN DE PRÁCTICAS Y POLÍTICAS DE CERTIFICACIÓN DE CERTIFICADOS DE AUTENTICACIÓN DE SITIOS WEB (DPC_AutSitiosWEB_1_0.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)

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

| | | |
|---|---|---|
| ▪ 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) |
| ▪ 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) |

## 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 with findings

#1 We have identified evidence in the sample of the web authentication certificates issued by "AC Administración Pública" and "AC Componentes Informáticos", cases in which the ownership of the domain is not adequately checked according to the methods established in section 3.2.2 of BRG. It should be noted that methods not allowed in the applicable CPS are included.

Likewise, for the certificates of public organizations, the verified information is relied upon when registering the organization but there are not enough controls in place to ensure that the data or documents used to verify certificate information are not older than 825 days.

Finally, it should be noted that it has not been possible to find evidence that CAA records are being checked for all issued web authentication certificates.

#2 In the case of OVCP certificates issued by "AC Administración Pública" and "AC Componentes Informáticos", although the suspension of web authentication certificates according to CPs is not allowed, the suspension of other types of certificates issued by these subordinates is allowed according to CPs. It has been verified that suspended certificates are included in the CRLs of these subordinates and, therefore, is not compliant with section 4.9.13 of the BRGs.

6.3 Certificate Life-Cycle operational requirements

Compliance.

6.4 Facility, management, and operational controls

Compliance with findings.

#3 We could not find evidence of the formal definition and assignment of the validation specialist profile, as specified in BRG, 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.

#4 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.

6.6 Certificate, CRL, and OCSP profiles

Compliance with findings.

#5 We have evidence certificates issued with errors:

- (OVCP) 1.3.6.1.4.1.5734.3.9.16; 1.3.6.1.4.1.5734.3.9.17; 1.3.6.1.4.1.5734.3.3.8.1: Certificates with *organizationName* or *organizationUnitName* bigger than 64 characters.

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 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 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 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 | 5 | 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 |