Audit Attestation for

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

Reference: PSC-2019-0003

Madrid, 2024-04-09

To whom it may concern,

This is to confirm that AENOR CONFÍA, S.A. has audited the CAs of the FÁBRICA NACIONAL DE MONEDA Y TIMBRE - REAL CASA DE LA MONEDA without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number “PSC-2019-0003” multiple Root-CAs and consists of 11 pages.

Kindly find here below the details accordingly.

In case of any question, please contact:

AENOR CONFÍA, S.A.
Génova, 6. 28004 Madrid. España
E-Mail: info@aenor.com
Phone: 91 432 60 00

With best regards,

Rafael GARCÍA MEIRO
Director General
2024-04-09

This attestation is based on the template version 3.1 as of 2023-08-24, that was approved for use by ACAB-c.

Identification of the conformity assessment body (CAB) and assessment organization acting as ETSI auditor:	• AENOR CONFÍA, S.A. Génova, 6. 28004 Madrid. España. www.aenor.com • Accredited by ENAC under registration 01/C-PR329 for the certification of trust services according to "UNE-EN ISO/IEC 17065:2012" and "ETSI EN 319 403-1 V2.3.1 (2020-06) respectively. Attestation of accreditation link: https://www.enac.es/documents/7020/5ae31445-73fa-4e16-acc4-78e079375c4f • Insurance Carrier (BRG section 8.2): MAPFRE • Third-party affiliate audit firms involved in the audit: none
Identification and qualification of the audit team:	• Number of team members: 1 Lead auditor and 3 auditors • Academic qualifications of team members: All team members have formal academic qualifications or professional training or extensive experience indicating general capability to carry out audits based on the knowledge given below and at least four years full time practical workplace experience in information technology, of which at least two years have been in a role or function relating to relevant trust services, public key infrastructure, information security including risk assessment/management, network security and physical security. • Additional competences of team members: All team members have knowledge of 1) audit principles, practices and techniques in the field of CA/TSP audits gained in a training course of at least five days; 2) the issues related to various areas of trust services, public key infrastructure, information security including risk assessment/management, network security and physical security; 3) the applicable standards, publicly available specifications and regulatory requirements for CA/TSPs and other relevant publicly available specifications including standards for IT product evaluation; and 4) the Conformity Assessment Body's processes. Furthermore, all team members have language skills appropriate for all organizational levels within the CA/TSP organization; note-taking, report-writing, presentation, and interviewing skills; and relevant personal attributes: objective, mature, discerning, analytical, persistent and realistic. • Professional training of team members: See "Additional competences of team members" above. Apart from that are all team members trained to demonstrate adequate competence in: a) knowledge of the CA/TSP standards and other relevant publicly available specifications; b) understanding functioning of trust services and information security including network security issues; c) understanding of risk assessment and risk management from the business perspective; d) technical knowledge of the activity to be audited;

	e) general knowledge of regulatory requirements relevant to TSPs; and f) knowledge of security policies and controls. • Types of professional experience and practical audit experience: The CAB ensures, that its personnel performing audits maintains competence on the basis of appropriate education, training or experience; that all relevant experience is current and prior to assuming responsibility for performing as an auditor, the candidate has gained experience in the entire process of CA/TSP auditing. This experience shall have been gained by participating under supervision of lead auditors in a minimum of four TSP audits for a total of at least 20 days, including documentation review, on-site audit and audit reporting. • Additional qualification and experience Lead Auditor: On top of what is required for team members (see above), the Lead Auditor a) has acted as auditor in at least three complete TSP audits; b) has adequate knowledge and attributes to manage the audit process; and c) has the competence to communicate effectively, both orally and in writing. • Special skills or qualifications employed throughout audit: none. • Special Credentials, Designations, or Certifications: All members are qualified and registered assessors within the accredited CAB. • Auditors code of conduct incl. independence statement: Code of Conduct as of Annex A, ETSI EN 319 403 or ETSI EN 319 403-1 respectively.
Identification and qualification of the reviewer performing audit quality management:	• Number of Reviewers/Audit Quality Managers involved independent from the audit team: 1 • The reviewer fulfils the requirements as described for the Audit Team Members above and has acted as an auditor in at least three complete CA/TSP audits.

Identification of the CA / Trust Service Provider (TSP):	FÁBRICA NACIONAL DE MONEDA Y TIMBRE - REAL CASA DE LA MONEDA Jorge Juan, 106. Madrid 28009 SPAIN

Type of audit:	☐ Point in time audit ☐ Period of time, after x month of CA operation ☒ Period of time, full audit
Audit period covered for all policies:	2023-01-13 to 2024-01-12

Audit dates:	2024-02-12 to 2024-03-01
Audit location:	CA/RA - Jorge Juan, 106. Madrid 28009 SPAIN

Root 1: AC RAIZ FNMT-RCM

Standards considered:	European Standards: • ETSI EN 319 411-2, V2.5.1 (2023-10) • ETSI EN 319 411-1, V1.4.1 (2023-10) • ETSI EN 319 401, V2.3.1 (2021-05) • ETSI TS 119 411-6, V1.1.1 (2023-08) CA Browser Forum Requirements: • EV Guidelines for TLS Server Certificates, version 1.8.0 • Baseline Requirements for TLS Server Certificates, version 2.0.1 • Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.2 For the Trust Service Provider Conformity Assessment: • ETSI EN 319 403-1 V2.3.1 (2020-06) • ETSI TS 119 403-2 V1.3.1 (2023-03)

The full annual audit was based on the following policy and practice statement documents of the CA / TSP:

1. (CPS) DECLARACIÓN GENERAL DE PRÁCTICAS DE SERVICIOS DE CONFIANZA Y DE CERTIFICACIÓN ELECTRÓNICA version 6.0 as of 2023-08-28
2. (CP) POLÍTICA Y PRÁCTICAS DE CERTIFICACIÓN PARTICULARES DE LOS CERTIFICADOS DE PERSONAS FÍSICAS DE LA "AC FNMT USUARIOS" version 1.8 as of 2023-05-31
3. (CP) POLÍTICA Y PRÁCTICAS DE CERTIFICACIÓN PARTICULARES DE LOS CERTIFICADOS DE REPRESENTANTE DE PERSONAS JURÍDICAS Y DE ENTIDADES SIN PERSONALIDAD JURÍDICA DE LA "AC REPRESENTACIÓN" version 2.0 as of 2023-08-28
4. (CP) DECLARACIÓN DE PRÁCTICAS Y POLÍTICAS DE CERTIFICACIÓN DE CERTIFICADOS DE COMPONENTES "AC COMPONENTES INFORMÁTICOS" version 2.7 as of 2024-02-07
5. (CP) POLÍTICAS Y PRÁCTICAS DE CERTIFICACIÓN DE CERTIFICADOS DE FIRMA ELECTRÓNICA Y SELLO ELECTRÓNICO DEL SECTOR PÚBLICO version 1.5 as of 2023-08-28
6. (CP) DECLARACIÓN DE PRÁCTICAS Y POLÍTICAS DE CERTIFICACIÓN DE CERTIFICADOS DE CREACIÓN DE SELLOS DE TIEMPO ELECTRÓNICOS version 1.3 as of 2023-12-22
7. (CP) POLÍTICA Y PRÁCTICAS DEL SERVICIO CUALIFICADO DE SELLADO DE TIEMPO version 1.4 as of 2023-12-22
8. (CP) POLÍTICA Y PRÁCTICAS DEL SERVICIO DE FIRMA EN SERVIDOR version 1.1 as of 2024-02-09

No major or minor non-conformities have been identified during the audit.

This Audit Attestation also covers the following incidents as documented under

- Bug 1828717, FNMT: CRL problems displayed during the monitoring: https://bugzilla.mozilla.org/show_bug.cgi?id=1828717
- Bug 1875942, FNMT: Certificates issued included Policy qualifiers other than id-qt-cps: https://bugzilla.mozilla.org/show_bug.cgi?id=1875942
-

The remediation measures taken by FNMT as described on Bugzilla (see link above) have been checked by the auditors and properly addressed the incident. The long-term effectiveness of the measures will be rechecked at the next regular audit.

Distinguished Name	SHA-256 fingerprint	Applied policy and OID
C = ES, O = FNMT-RCM, OU = AC RAIZ FNMT-RCM	EBC5570C29018C4D67B1AA127BAF12F703B4611EBC17B7DAB5573894179B93FA	ETSI EN 319 411-2 V2.5.1, QCP-n ETSI EN 319 411-2 V2.5.1, QCP-n-qscd ETSI EN 319 411-2 V2.5.1, QCP-l ETSI EN 319 411-2 V2.5.1, QNCP-W ETSI EN 319 411-1 V1.4.1, OVCP ETSI TS 119 411-6 V1.1.1, OVL[1]
C = ES, O = FNMT-RCM, OU = AC RAIZ FNMT-RCM	B82210CDE9DDEA0E14BE29AF647E4B32F96ED2A9EF1AA5BAA9CC64B38B6C01CA	ETSI EN 319 411-2 V2.5.1, QCP-n ETSI EN 319 411-2 V2.5.1, QCP-n-qscd ETSI EN 319 411-2 V2.5.1, QCP-l ETSI EN 319 411-2 V2.5.1, QNCP-W ETSI EN 319 411-1 V1.4.1, OVCP ETSI TS 119 411-6 V1.1.1, OVL[1]
C = ES, O = FNMT-RCM, OU = AC RAIZ FNMT-RCM	4D9EBB28825C9643AB15D54E5F9614F13CB3E95DE3CF4EAC971301F320F9226E	ETSI EN 319 411-2 V2.5.1, QCP-n ETSI EN 319 411-2 V2.5.1, QCP-n-qscd ETSI EN 319 411-2 V2.5.1, QCP-l ETSI EN 319 411-2 V2.5.1, QNCP-W ETSI EN 319 411-1 V1.4.1, OVCP ETSI TS 119 411-6 V1.1.1, OVL[1]

Table 1: Root-CA in scope of the audit

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CAs, that are listed in the following table and that have been covered in this audit.

Distinguished Name	SHA-256 fingerprint	Applied policy and OID	EKU
C = ES, O = FNMT-RCM, OU = Ceres, CN = AC FNMT Usuarios	601293CA20B09A03295D196256C6953FF9EBA811DB8E3CE140413C1BFFE9A869	ETSI EN 319 411-2 V2.5.1, QCP-n	not defined
C = ES, O = FNMT-RCM, OU = CERES, CN = AC Representación	8FD16A179944D5D1D420AF09405EDA7ABF2A9C742883E8C2F89E0D90AFAF754B	ETSI EN 319 411-2 V2.5.1, QCP-n ETSI EN 319 411-2 V2.5.1, QCP-l ETSI TS 119 411-6 V1.1.1, OVL[1]	not defined

[1] Organization-validated - Legacy

Distinguished Name	SHA-256 fingerprint	Applied policy and OID	EKU
C = ES, O = FNMT-RCM, OU = AC Componentes Informáticos	DB0DA16032F1643A2496FDE742E2BBE81DACA58CD7612061420E154CE1BCE2BD	ETSI EN 319 411-2 V2.5.1, QCP-l ETSI EN 319 411-2 V2.5.1, QNCP-w ETSI EN 319 411-1 V1.4.1, OVCP	not defined
C = ES, O = FNMT-RCM, OU = AC Componentes Informáticos	F038421F07F20D63A20D3691E5A178AB8459EBE570C1647B7690554EF23876AB	ETSI EN 319 411-2 V2.5.1, QCP-l ETSI EN 319 411-2 V2.5.1, QNCP-w ETSI EN 319 411-1 V1.4.1, OVCP	not defined
C = ES, O = FNMT-RCM, OU = Ceres, organizationIdentifier = VATES-Q2826004J, CN = AC Sector Público	8265756DD5CD8A37EE61E40351288E4B16A89DD248C1EC4EBA25AAF161ABF498	ETSI EN 319 411-2 V2.5.1, QCP-n ETSI EN 319 411-2 V2.5.1, QCP-n-qscd ETSI EN 319 411-2 V2.5.1, QCP-l	not defined
C = ES, O = FNMT-RCM, OU = Ceres, organizationIdentifier = VATES-Q2826004J, CN = AC Unidades de Sellado de Tiempo	9CE630B35F8AE2C6419E734AD9D2FA30476DD9E7394B1E93B27F83F776A024EA	ETSI EN 319 411-2 V2.5.1, QCP-l	not defined

Table 2: Sub-CA's issued by the Root-CA or its Sub-CA's in scope of the audit

Root 2: AC RAIZ FNMT-RCM SERVIDORES SEGUROS

Standards considered:	European Standards: • ETSI EN 319 411-2, V2.5.1 (2023-10) • ETSI EN 319 411-1, V1.4.1 (2023-10) • ETSI EN 319 401, V2.3.1 (2021-05) CA Browser Forum Requirements: • EV Guidelines for TLS Server Certificates, version 1.8.0 • Baseline Requirements for TLS Server Certificates, version 2.0.1 For the Trust Service Provider Conformity Assessment: • ETSI EN 319 403-1 V2.3.1 (2020-06) • ETSI TS 119 403-2 V1.2.4 (2020-11)

The full annual audit was based on the following policy and practice statement documents of the CA / TSP:

1. (CPS) DECLARACIÓN GENERAL DE PRÁCTICAS DE SERVICIOS DE CONFIANZA Y DE CERTIFICACIÓN ELECTRÓNICA version 6.0 as of 2023-08-28
2. (CP) DECLARACIÓN DE PRÁCTICAS Y POLÍTICAS DE CERTIFICACIÓN DE CERTIFICADOS DE AUTENTICACIÓN DE SITIOS WEB version 1.12 as of 2024-02-07

No major or minor non-conformities have been identified during the audit.

This Audit Attestation also covers the following incidents as documented under

- Bug 1828717, FNMT: CRL problems displayed during the monitoring: https://bugzilla.mozilla.org/show_bug.cgi?id=1828717
- Bug 1875942, FNMT: Certificates issued included Policy qualifiers other than id-qt-cps: https://bugzilla.mozilla.org/show_bug.cgi?id=1875942
-

The remediation measures taken by FNMT as described on Bugzilla (see link above) have been checked by the auditors and properly addressed the incident. The long-term effectiveness of the measures will be rechecked at the next regular audit.

Distinguished Name	SHA-256 fingerprint	Applied policy and OID
C = ES, O = FNMT-RCM, OU = CERES, ORGANIZATIONIDENTIFIER = VATES-Q2826004J, CN = AC RAIZ FNMT-RCM SERVIDORES SEGUROS	554153B13D2CF9DDB753BFBE1A4E0AE08D0AA4187058FE60A2B862B2E4B87BCB	ETSI EN 319 411-2 V2.5.1, QEVCP-W ETSI EN 319 411-1 V1.4.1, OVCP

Table 3: Root-CA in scope of the audit

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CAs, that are listed in the following table and that have been covered in this audit.

Distinguished Name	SHA-256 fingerprint	Applied policy and OID	EKU
C = ES, O = FNMT-RCM, OU = Ceres, organizationIdentifier = VATES-Q2826004J, CN = AC SERVIDORES SEGUROS TIPO1	1EDB6BD91274882DB795BFC514F8AABE10AD955CBCCFD3FD5A5B5FEBB2CE5B68	ETSI EN 319 411-2 V2.5.1, QEVCP-w	not defined
C = ES, O = FNMT-RCM, OU = Ceres, organizationIdentifier = VATES-Q2826004J, CN = AC SERVIDORES SEGUROS TIPO2	9FF23CB9387B9E0083BD5AA1954EEDDF792890AA8E67CD4D38DD28AF4A439AD8	ETSI EN 319 411-1 V1.4.1, OVCP	not defined

Table 4: Sub-CA’s issued by the Root-CA or its Sub-CA’s in scope of the audit

Modifications record

Version	Issuing Date	Changes
Version 1	2024-04-09	Initial attestation

End of the audit attestation letter.