Audit Attestation for

AGENCIA DE TECNOLOGÍA Y CERTIFICACIÓN ELECTRÓNICA, ACCV

Reference: PSC-2017-0010

Madrid, 2023-12-20

To whom it may concern,

This is to confirm that AENOR INTERNACIONAL, S.A.U. has audited the CAs of the AGENCIA DE TECNOLOGÍA Y CERTIFICACIÓN ELECTRÓNICA, ACCV. without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number “PSC-2017-0010” multiple Root-CAs and consists of 11 pages.

Kindly find here below the details accordingly.

In case of any question, please contact:

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

With best regards,

Rafael GARCÍA MEIRO
CEO
2023-12-20

Identification of the conformity assessment body (CAB) and assessment organization acting as ETSI auditor:	• AENOR INTERNACIONAL, S.A.U. 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 1 auditor • 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):	AGENCIA DE TECNOLOGÍA Y CERTIFICACIÓN ELECTRÓNICA, ACCV POLÍGONO DE ACCESO A ADEMUZ, S/N 46100 - BURJASSOT 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:	2023-07-25 to 2023-10-20

Audit dates:	2023-10-16 to 2023-10-20
Audit location:	POLÍGONO DE ACCESO A ADEMUZ, S/N 46100 – BURJASSOT - SPAIN

Root 1: ACCV ROOT RSA EIDAS 2023

Standards considered:	European Standards: • ETSI EN 319 411-2 V2.4.1 (2021-11) • ETSI EN 319 401 V2.3.1 (2021-05) CA Browser Forum Requirements: • Baseline Requirements for TLS Server Certificates, version 2.0.1 For the Trust Service Provider Conformity Assessment: • ETSI EN 319 403 V2.2.2 (2015-08) • 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 de Prácticas de Certificación version 5.0.1 as of 2023-09-16
2. (CP) Política de Certificación de Certificados de Aplicación versión 5.0.1 as of 2023-10-12
3. (CP) Política de Certificación de Certificados Cualificados en dispositivo seguro para ciudadanos, version 9.0.1 as of 2023-09-28
4. (CP) Política de Certificación de Certificados Cualificados en soporte software para ciudadanos, version 8.0.1 as of 2023-10-05
5. (CP) Política de Certificación de Certificados Cualificados en dispositivo seguro para empleados públicos, version 6.0.1 as of 2023-10-06
6. (CP) Política de Certificación de Certificados Cualificados de sello electrónico de órgano en dispositivo seguro, version 5.0.1 as of 2023-10-12
7. (CP) Política de Certificación de Certificados Cualificados de sello electrónico de órgano en soporte software, version 5.0.1 as of 2023-10-12
8. (CP) Política de Certificación de Certificados Cualificados en soporte software para empleados públicos, version 4.0.1 as of 2023-10-06
9. (CP) Política de Certificación de Certificados Cualificados en dispositivo seguro de pertenencia a empresa, version 5.0.1 as of 2023-10-06
10. (CP) Política de Certificación de Certificados Cualificados de empleado público con seudónimo en dispositivo seguro, version 4.0.1 as of 2023-10-06
11. (CP) Política de Certificación de Certificados Cualificados en soporte software de pertenencia a empresa, version 3.0.1 as of 2023-10-06
12. (CP) Política de Certificación de Certificados Cualificados de empleado público con seudónimo en soporte software, version 3.0.1 as of 2023-10-06

13. (CP) Política de Certificación de Certificados Cualificados de Representante de Entidad Jurídica en dispositivo seguro, version 3.0.1 as of 2023-10-06
14. (CP) Política de Certificación de Certificados Cualificados de Representante de Entidad Jurídica en soporte software, version 3.0.1 as of 2023-10-06
15. (CP) Política de Certificación de Certificados Cualificados de Representante de Entidad sin Personalidad Jurídica en dispositivo seguro, version 3.0.1 as of 2023-10-06
16. (CP) Política de Certificación de Certificados Cualificados de Representante de Entidad sin Personalidad Jurídica en soporte software, version 3.0.1 as of 2023-10-06
17. (CP) Política de Certificación de Certificados Cualificados en dispositivo seguro para empleados públicos nivel alto (Firma), version 2.0.1 as of 2023-10-06
18. (CP) Política de Certificación de Certificados Cualificados en dispositivo seguro para empleados públicos nivel alto (Autenticación), version 2.0.1 as of 2023-10-06

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

In the following areas, minor non-conformities have been identified throughout the audit:

Findings with regard to ETSI EN 319 401:
5 Risk Assessment
The risk assessment had not been fully reviewed and updated at the audit time.

Findings with regard to ETSI EN 319 411-2:
None

All non-conformities have been closed before the issuance of this attestation.

This Audit Attestation also covers the following incidents as documented under

- There are no reported or active incidents during the audit period.

Distinguished Name	SHA-256 fingerprint	Applied policy and OID
C = ES, ST = VALENCIA, L = BURJASSOT, O = ISTEC, organizationIdentifier = VATES-A40573396, CN = ACCV ROOT RSA EIDAS 2023	5A769EB3D9D6A9770BDC1BF412632BD35DAD69BDF24EE9CD75D2B659B4A0DDC9	ETSI EN 319 411-2 V2.4.1, QCP-n ETSI EN 319 411-2 V2.4.1, QCP-n-qscd ETSI EN 319 411-2 V2.4.1, QCP-l ETSI EN 319 411-2 V2.4.1, QCP-l-qscd

Table 1: Root-CA in scope of the audit

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, 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, ST = VALENCIA, L = BURJASSOT, O = ISTEC, organizationIdentifier = VATES-A40573396, CN = ACCV RSA1 CLIENTE	A66B485645A5D66A5714A360E02DDF3AB71875E77DB198BA321A8F62FF01D7E1	ETSI EN 319 411-2 V2.4.1, QCP-n ETSI EN 319 411-2 V2.4.1, QCP-n-qscd	clientAuth 1.3.6.1.5.5.7.3.2 pdfAuthenticDocumentsTrust 1.2.840.113583.1.1.5
C = ES, ST = VALENCIA, L = BURJASSOT, O = ISTEC, organizationIdentifier = VATES-A40573396, CN = ACCV RSA1 PROFESIONALES	60ADC74248A45F7DF968587F38119F50E99B4E06D1A6241DC6B8F6D19CD2A38A	ETSI EN 319 411-2 V2.4.1, QCP-n ETSI EN 319 411-2 V2.4.1, QCP-n-qscd	clientAuth 1.3.6.1.5.5.7.3.2 pdfAuthenticDocumentsTrust 1.2.840.113583.1.1.5
C = ES, ST = VALENCIA, L = BURJASSOT, O = ISTEC, organizationIdentifier = VATES-A40573396, CN = ACCV RSA1 COMPONENTES	50D5748D831C2864459B23D8B99DF53DBA43BBBB2BC4BFCDDB5731B52B56B69E	ETSI EN 319 411-2 V2.4.1, QCP-l ETSI EN 319 411-2 V2.4.1, QCP-l-qscd	clientAuth 1.3.6.1.5.5.7.3.2 pdfAuthenticDocumentsTrust 1.2.840.113583.1.1.5

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

Root 2: ACCV ROOT ECC EIDAS 2023

Standards considered:	European Standards: • ETSI EN 319 411-2 V2.4.1 (2021-11) • 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 V2.2.2 (2015-08) • 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 de Prácticas de Certificación version 5.0.1 as of 2023-09-16
2. (CP) Política de Certificación de Certificados de Aplicación versión 5.0.1 as of 2023-10-12
3. (CP) Política de Certificación de Certificados Cualificados en dispositivo seguro para ciudadanos, version 9.0.1 as of 2023-09-28
4. (CP) Política de Certificación de Certificados Cualificados en soporte software para ciudadanos, version 8.0.1 as of 2023-10-05
5. (CP) Política de Certificación de Certificados Cualificados en dispositivo seguro para empleados públicos, version 6.0.1 as of 2023-10-06
6. (CP) Política de Certificación de Certificados Cualificados de sello electrónico de órgano en dispositivo seguro, version 5.0.1 as of 2023-10-12
7. (CP) Política de Certificación de Certificados Cualificados de sello electrónico de órgano en soporte software, version 5.0.1 as of 2023-10-12
8. (CP) Política de Certificación de Certificados Cualificados en soporte software para empleados públicos, version 4.0.1 as of 2023-10-06
9. (CP) Política de Certificación de Certificados Cualificados en dispositivo seguro de pertenencia a empresa, version 5.0.1 as of 2023-10-06
10. (CP) Política de Certificación de Certificados Cualificados de empleado público con seudónimo en dispositivo seguro, version 4.0.1 as of 2023-10-06
11. (CP) Política de Certificación de Certificados Cualificados en soporte software de pertenencia a empresa, version 3.0.1 as of 2023-10-06
12. (CP) Política de Certificación de Certificados Cualificados de empleado público con seudónimo en soporte software, version 3.0.1 as of 2023-10-06
13. (CP) Política de Certificación de Certificados Cualificados de Representante de Entidad Jurídica en dispositivo seguro, version 3.0.1 as of 2023-10-06

14. (CP) Política de Certificación de Certificados Cualificados de Representante de Entidad Jurídica en soporte software, version 3.0.1 as of 2023-10-06
15. (CP) Política de Certificación de Certificados Cualificados de Representante de Entidad sin Personalidad Jurídica en dispositivo seguro, version 3.0.1 as of 2023-10-06
16. (CP) Política de Certificación de Certificados Cualificados de Representante de Entidad sin Personalidad Jurídica en soporte software, version 3.0.1 as of 2023-10-06
17. (CP) Política de Certificación de Certificados Cualificados en dispositivo seguro para empleados públicos nivel alto (Firma), version 2.0.1 as of 2023-10-06
18. (CP) Política de Certificación de Certificados Cualificados en dispositivo seguro para empleados públicos nivel alto (Autenticación), version 2.0.1 as of 2023-10-06

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

In the following areas, minor non-conformities have been identified throughout the audit:

Findings with regard to ETSI EN 319 401:
5 Risk Assessment
The risk assessment had not been fully reviewed and updated at the audit time.

Findings with regard to ETSI EN 319 411-2:
6.6.1 Certificate Profile
The sample certificates included an unallowed key usage (keyEncipherment) for EC public key at the audit time.

All non-conformities have been closed before the issuance of this attestation.

This Audit Attestation also covers the following incidents as documented under
- There are no reported or active incidents during the audit period.

Distinguished Name	SHA-256 fingerprint	Applied policy and OID
C = ES, ST = VALENCIA, L = BURJASSOT, O = ISTEC, organizationIdentifier = VATES-A40573396, CN = ACCV ROOT ECC EIDAS 2023	F1AA0EC662705BB297B437F67EA9E4650EC5BC5E956757AA7F04D7D9945471E3	ETSI EN 319 411-2 V2.4.1, QCP-n ETSI EN 319 411-2 V2.4.1, QCP-n-qscd ETSI EN 319 411-2 V2.4.1, QCP-l ETSI EN 319 411-2 V2.4.1, QCP-l-qscd

Table 3: Root-CA in scope of the audit

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, 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, ST = VALENCIA, L = BURJASSOT, O = ISTEC, organizationIdentifier = VATES-A40573396, CN = ACCV ECC1 CLIENTE	5CAF44B2923B146CB575AB2AB9A0A293A134602335D97E579C44493532F48496	ETSI EN 319 411-2 V2.4.1, QCP-n ETSI EN 319 411-2 V2.4.1, QCP-n-qscd	clientAuth 1.3.6.1.5.5.7.3.2 pdfAuthenticDocumentsTrust 1.2.840.113583.1.1.5
C = ES, ST = VALENCIA, L = BURJASSOT, O = ISTEC, organizationIdentifier = VATES-A40573396, CN = ACCV ECC1 PROFESIONALES	34FDB6F3D2D1070DD8428BCE11D62294E1FF2C49E8B128B61160D748C7A537AA	ETSI EN 319 411-2 V2.4.1, QCP-n ETSI EN 319 411-2 V2.4.1, QCP-n-qscd	clientAuth 1.3.6.1.5.5.7.3.2 pdfAuthenticDocumentsTrust 1.2.840.113583.1.1.5
C = ES, ST = VALENCIA, L = BURJASSOT, O = ISTEC, organizationIdentifier = VATES-A40573396, CN = ACCV ECC1 COMPONENTES	D26E702D039A5713DDABF710E47193734E5550711763785051788D0FD2D7F4EA	ETSI EN 319 411-2 V2.4.1, QCP-l ETSI EN 319 411-2 V2.4.1, QCP-l-qscd	clientAuth 1.3.6.1.5.5.7.3.2 pdfAuthenticDocumentsTrust 1.2.840.113583.1.1.5

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	2023-12-20	Initial attestation

End of the audit attestation letter.