Audit Attestation for

Consorci Administració Oberta de Catalunya

Reference: 2304_CAO_FR

"Madrid, 2023-06-06"

To whom it may concern,

This is to confirm that DEKRA Testing and Certification S.A.U has audited the CAs of the Consorci Administració Oberta de Catalunya without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number "2304_CAO_FR" covers a single Root-CA and consists of 7 pages.

Kindly find here below the details accordingly.

In case of any question, please contact:

DEKRA Testing and Certification S.A.U
C/ Severo Ochoa 2 y 6. Parque tecnológico de Andalucía
29590, Málaga. España
E-Mail: jose.rico@dekra.com
Phone: +34 95 261 91 00

With best regards,

_____
JOSE EMILIO RICO
Director of eIDAS Certification Body

This attestation is based on the template version 3.0 as of 2023-02-20, that was approved for use by ACAB-c.

General audit information

Identification of the conformity assessment body (CAB) and assessment organization acting as ETSI auditor

- DEKRA Testing and Certification S.A.U, C/ Severo Ochoa 2 y 6. Parque tecnológico de Andalucía, 29590 Malaga, Spain, registered under "Registro Mercantil de Madrid, folio 92, inscripción 1ª."
- Accredited by ENAC under registration 134/C-PR337 for the certification of trust services according to "EN ISO/IEC 17065:2012" and "ETSI EN 319 403-1 V2.3.1 (2020-06)". Attestation of accreditation link: https://www.enac.es/documents/7020/9a29e298-3657-408e-b140-a8e70bf9dc09 Insurance Carrier (BRG section 8.2):Allianz
- Third-party affiliate audit firms involved in the audit:None.

Identification and qualification of the audit team

- Number of team members: 1 Lead auditor, 1 auditor and 1 technical expert.
- Academic qualifications of team members:
  Lead auditor and auditor 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):	Consorci Administració Oberta de Catalunya, C/Tánger 98, bajo, 08018 Barcelona, España.

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:	2022-03-29 to 2023-03-28
Audit dates:	2023-04-03 to 2023-05-30
Audit location:	CA - C/Tánger 98, bajo 08018 Barcelona (España) CPD - Calle Agustín Goytisolo, 10-12 08908 - Hospitalet de Llobregat (Barcelona) CPD - PTV: Carrer dels Artesans, 7 08290 Cerdanyola del Vallès, (Barcelona)

Root 1: EC-ACC

Standards considered:	European Standards: ☒ ETSI EN 319 411-2 V2.4.1 (2021-11) ☒ ETSI EN 319 411-1 V1.3.1 (2021-05) ☒ ETSI EN 319 401 V2.3.1 (2021-05) CA Browser Forum Requirements: ☐ EV SSL Certificate Guidelines, version 1.8.0 ☐ Baseline Requirements, version 2.0.0 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 audit was based on the following policy and practice statement documents of the CA / TSP:

1. (CPS) Declaración de Prácticas de Certificación Autoridad de Certificación del Consorci AOC, version 6.9, as of 2023-05-10

2. (CP) Política de Certificación para Certificados Personales del Sector Público Consorci AOC, version 6.6 as of 2023-03-29

3. (CP) Política de Certificación para Dispositivos e Infraestructuras Consorci AOC, version 6.6 as of 2023-05-10

4. (CP) Política de Certificación para Certificados de Ciudadanía Consorci AOC, version 6.7 as of 2023-03-29

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

Findings with regard to ETSI EN 319 401:

6.2 Terms and Conditions

The audit team did not find any section related to complaints procedure and disputes [REQ-6.2-02]

7.12 TSP termination and termination plans

The audit team did not find any reference to the update or revision of the termination plan in the current year. [REQ-7.12-02]

Findings with regard to ETSI EN 319 411-1:

5.2 Certification Practice Statement requirements

The audit team did not find any evidence related to the use of CA keys in order to sign CRL and OCSP certificates. [OVR-5.2-10]

6.5.5 Computer security controls

The audit team did not find any access control when the operator tries to revoke a certificate. [CSS-6.5.5-06]

Findings with regard to ETSI EN 319 411-2:

6.6.1 Certificate Profile

> The audit team has found that QCStatements have been tagged as critical in the certificate profiles document. [GEN-6.6.1-02]

6.3.5 Key Pair and Certificate Usage

> The audit team did not find any section related to specific requirements for qualified electronic seal certificates. [SDP-6.3.5-09, SDP-6.3.5-11]

All major non-conformities have been closed before the issuance of this attestation. For all minor non-conformities, remediation has been scheduled within three months after the onsite audit at latest and will be covered by a corresponding audit.

To the best of our knowledge, no incidents have occurred within this Root-CA's hierarchy during the audited period.

Distinguished Name	SHA-256 fingerprint	Applied policy and OID
CN = EC-ACC OU = Jerarquia Entitats de Certificacio Catalanes OU = Vegeu https://www.catcert.net/verarrel (c)03 OU = Serveis Publics de Certificacio O = Agencia Catalana de Certificacio (NIF Q-0801176-I) C = ES	88497F01602F3154246AE28C4D5AEF10F1D87EBB76626F4AE0B7F95BA7968799	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

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, O = CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA, OU = Serveis P\C3\BAblics de Certificaci\C3\B3, CN = EC-Ciutadania	0FD99AAE1FFCD5D9F0AD76EDDDCBEF6B884CC85C16BFCFA4B5246155D6597ED6	ETSI EN 319 411-2 V2.4.1, QCP-n	not defined
C = ES, O = CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA, OU = Serveis P\C3\BAblics de Certificaci\C3\B3, CN = EC-SectorPublic	356A5F4D994E9EFA7CAEFC491768911D65EC25977465B610E2F29AA4472631C3	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	not defined

Table 2: 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	2023-06-06	Initial attestation

End of the audit attestation letter.