

INDEPENDENT ASSURANCE REPORT

To the management of Consejo General de la Abogacía Española. (“CGAE”)

We have been engaged, in a reasonable assurance engagement, to report on CGAE management’s assertion that for its Certification Authority (CA) operations at Madrid, Spain, throughout the period from April 1st, 2023, to March 31st, 2024, for its CAs as enumerated in Appendix A, CGAE has:

- Disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:

CPS Name	OID	CPS Link
Certification Practices Statement	1.3.6.1.4.1.16533.10.1.1	CPS_ACA_022_EN.pdf
CP Link		
Qualified Membership Certificate	1.3.6.1.4.1.16533.10.2.1	CP1_ACA_014_EN.pdf
Qualified Administrative Staff Certificates	1.3.6.1.4.1.16533.10.3.1	CP2_ACA_014_EN.pdf
Qualified Legal Entity Representative Certificates	1.3.6.1.4.1.16533.10.10.1	CP8_ACA_CA1_007.0_EN.pdf
Qualified European Lawyer Certificates	1.3.6.1.4.1.16533.10.9.1	CP7_ACA_009.0_EN.pdf
Qualified Certificates of Electronic Seal	1.3.6.1.4.1.16533.20.3.1	CP2_ACA_TC_010.0_EN.pdf
Qualified Professional Staff Certificates	1.3.6.1.4.1.16533.20.4.1	CP4_ACATC_009.0_EN.pdf
Qualified Authorized Certificates	1.3.6.1.4.1.16533.20.6.1	CP7_ACACA2_007_EN.pdf
The Law Society of Scotland Qualified Certificates	1.3.6.1.4.1.16533.20.5.1	CP6_ACATC_006.0_EN.pdf

- Maintained effective controls to provide reasonable assurance that:
 - CGAE’s Certification Practice Statements are consistent with its Certificate Policies
 - CGAE provides its services in accordance with its Certificate Policies (if applicable) and Certification Practice Statements
- Maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and certificates it manages is established and protected throughout their lifecycles.
 - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles
 - subscriber information is properly authenticated (for the registration activities performed by CGAE; and
 - subordinate CA certificate requests are accurate, authenticated, and approved.

- Maintained effective controls to provide reasonable assurance that:
 - logical and physical access to CA systems and data is restricted to authorized individuals.
 - the continuity of key and certificate management operations is maintained; and
 - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity.

in accordance with the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#)

CGAE makes use of external registration authorities for specific subscriber registration activities as disclosed in CGAE's business practices. Our procedures did not extend to the controls exercised by these external registration authorities.

CGAE does not escrow its CA keys. Accordingly, our procedures did not extend to controls that would address that criterion.

Certification authority's responsibilities

CGAE's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.2.2

Our independence and quality control

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality, and professional behavior.

The firm applies International Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Historical Financial Information, and Other Assurance and Related Services, Engagements* and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion¹⁶ based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion is fairly stated, and, accordingly, included:

1. Obtaining an understanding of CGAE's key and certificate lifecycle management business practices and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate lifecycle management operations and over development, maintenance, and operation of systems integrity.
2. Selectively testing transactions executed in accordance with disclosed key and certificate lifecycle management business practices.
3. Testing and evaluating the operating effectiveness of the controls; and

4. Performing such other procedures as we considered necessary in the circumstances.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

The relative effectiveness and significance of specific controls at CGAE and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. For example, because of their nature, controls may not prevent, or detect unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection to the future of any conclusions based on our findings is subject to the risk that controls may become ineffective.

Opinion

In our opinion, throughout the period from April 1st, 2023, through March 31st, 2024, CGAE management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

This report does not include any representation as to the quality of CGAE's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities v2.2.2, nor the suitability of any of CGAE's services for any customer's intended purpose.

Use of the WebTrust seal

CGAE's use of the WebTrust for Certification Authorities Seal constitutes a symbolic representation of the contents of this report, and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

EY TRANSFORMA SERVICIOS DE CONSULTORIA, S.L.

Calle de Raimundo Fernández Villaverde 65, 28003
Madrid, Spain.



Joaquín Castellón Colomina
Partner
May 27st, 2024

Appendix A:

Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA Fingerprint - 256	MD5 Fingerprint
CA ACA ROOT	1a55e41531e 2319b11d488 717a003d702 805bfcd	474391243fcec 30d5748286be e805dab	97f654859cbde586fd9 0311e82ec7902c238c ba0d6e529564c9c88f4 4895ec50	d496592b30570738 6cc5f3cdb259ae66d 7661fca
ACA ROOT / CA Subordinada ACA CA1	72a9e7d68e0 267a04a4c1a 6731bcb7fecb 84b49b	491ef8c2bf472 4d3576bd181fc 6705ad	705eb3a0b1f09deda3e d45766bbbc02197700 abb1e2d1d9e2862ac5 89dc9fd77	53d27de605858349f a2bd581d386407ee e732517
ACA ROOT / CA Subordinada ACA CA2	8a151faf74ef1 f0107732a902 a41097e1b48 d0c0	49a91da5cd0d 70c3576bd11e 009d55dd	7e9316a5cecfb90a53a dc3c7769450f42cdc3a 9b85df4c7577b053dcb b255812	5c4df5ddc8e269a35 d26ec18e14402f109 b25030

CONSEJO GENERAL DE LA ABOGACÍA ESPAÑOLA MANAGEMENT'S ASSERTION

Consejo General de la Abogacía Española (“CGAE”) operates the Certification Authority (CA) services known as for its CAs listed in Appendix A, and provides the following CA services:

- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation

The management of CGAE is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its website, CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, certificate lifecycle management controls, and subordinate CA certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to CGAE’s Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

CGAE management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in CGAE management’s opinion, in providing its Certification Authority (CA) services at Madrid, Spain, throughout the period from April 1st, 2023, to March 31st, 2024, CGAE has:

- Disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:

CPS Name	OID	CPS Link
Certification Practices Statement	1.3.6.1.4.1.16533.10.1.1	CPS_ACA_022_EN.pdf
CP Link		
Qualified Membership Certificate	1.3.6.1.4.1.16533.10.2.1	CP1_ACA_014_EN.pdf
Qualified Administrative Staff Certificates	1.3.6.1.4.1.16533.10.3.1	CP2_ACA_014_EN.pdf
Qualified Legal Entity Representative Certificates	1.3.6.1.4.1.16533.10.10.1	CP8_ACA_CA1_007.0_EN.pdf
Qualified European Lawyer Certificates	1.3.6.1.4.1.16533.10.9.1	CP7_ACA_009.0_EN.pdf
Qualified Certificates of Electronic Seal	1.3.6.1.4.1.16533.20.3.1	CP2_ACA_TC_010.0_EN.pdf
Qualified Professional Staff Certificates	1.3.6.1.4.1.16533.20.4.1	CP4_ACATC_009.0_EN.pdf
Qualified Authorized Certificates	1.3.6.1.4.1.16533.20.6.1	CP7_ACACA2_007_EN.pdf
The Law Society of Scotland Qualified Certificates	1.3.6.1.4.1.16533.20.5.1	CP6_ACATC_006.0_EN.pdf

- Maintained effective controls to provide reasonable assurance that:
 - CGAE's Certification Practice Statements are consistent with its Certificate Policies
 - CGAE provides its services in accordance with its Certificate Policies (if applicable) and Certification Practice Statements.
- Maintained effective controls to provide reasonable assurance that:
 - The integrity of keys and certificates it manages is established and protected throughout their lifecycles.
 - The integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles.
 - Subscriber information is properly authenticated (for the registration activities performed by CGAE); and
 - Subordinate CA certificate requests are accurate, authenticated, and approved.
- Maintained effective controls to provide reasonable assurance that:
 - logical and physical access to CA systems and data is restricted to authorized individuals.
 - the continuity of key and certificate management operations is maintained; and
 - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity.

In accordance with the WebTrust Principles and Criteria for Certification Authorities v2.2.2 including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)
- Certificate Policy (CP)

CA Business Practices Management

- Certificate Policy Management
- Certification Practice Statement Management
- CP and CPS Consistency

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical & Environmental Security
- Operations Management
- System Access Management
- System Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Lifecycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management
- CA Key Escrow

Subscriber Key Lifecycle Management Controls

- CA-Provided Subscriber Key Generation Services
- CA-Provided Subscriber Key Storage and Recovery Services

- Integrated Circuit Card (ICC) Lifecycle Management
- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls

- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Suspension
- Certificate Validation

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

Consejo General de la Abogacía Española does not escrow its CA keys. Accordingly, our assertion does not extend to controls that would address that criterion.

13082656A

VICTORIA ORTEGA

(R:Q2863006I)

Firmado digitalmente por
13082656A VICTORIA ORTEGA
(R:Q2863006I)
Fecha: 2024.05.28 11:39:58
+02'00'

Victoria Ortega Benito
President of Consejo General de la Abogacía Española
May 27, 2024

Appendix A:

Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA Fingerprint - 256	MD5 Fingerprint
CA ACA ROOT	1a55e41531e 2319b11d488 717a003d702 805bfcd	474391243fcec 30d5748286be e805dab	97f654859cbde586fd9 0311e82ec7902c238c ba0d6e529564c9c88f4 4895ec50	d496592b30570738 6cc5f3cdb259ae66d 7661fca
ACA ROOT / CA Subordinada ACA CA1	72a9e7d68e0 267a04a4c1a 6731bcb7fecb 84b49b	491ef8c2bf472 4d3576bd181fc 6705ad	705eb3a0b1f09deda3e d45766bbbc02197700 abb1e2d1d9e2862ac5 89dc9fd77	53d27de605858349f a2bd581d386407ee e732517
ACA ROOT / CA Subordinada ACA CA2	8a151faf74ef1 f0107732a902 a41097e1b48 d0c0	49a91da5cd0d 70c3576bd11e 009d55dd	7e9316a5cecfb90a53a dc3c7769450f42cdc3a 9b85df4c7577b053dcb b255812	5c4df5ddc8e269a35 d26ec18e14402f109 b25030