

Report of Independent Accountants

To the Management of Consejo General de la Abogacía (CGAE)

We have examined the accompanying assertion made by the management Consejo General de la Abogacía Española (CGAE), titled “**Management’s Assertion Regarding the Effectiveness of Its Controls Over its Certification Authority Services. Based on the Trust Services Principles and Criteria for Certification Authorities Version 2.1**” that provides its Certification Authority (CA) services at Spain for the Root CA and Subordinate CAs referenced in Appendix A during the period from April 1st 2019 through March 31st 2020. Consejo General de la Abogacía Española has:

- Disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
 - CPS_ACA_017.0 - DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AUTORIDAD DE CERTIFICACIÓN DE LA ABOGACÍA and
 - CP1_ACA_009.0.pdf
 - CP2_ACA_009.pdf
 - CP8_ACA_CA1_003.0.pdf
 - CP7_ACA_004.0.pdf
 - CP2_ACATC_006.0.pdf
 - CP4_ACATC_004.0.pdf
 - CP7_ACA_CA2_002.pdf
 - CP6_ACATC_003.0.pdf
 - CP1_ACA_CA3_002.pdf
- Maintained effective controls to provide reasonable assurance that:
 - CGAE - CA’s Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)]
 - CGAE - CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)
- 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 ABC-CA); 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



based on the American Institute of Certified Public Accountants (AICPA)'s [Trust Services Principles and Criteria for Certification Authorities 2.1](#)

CGAE's management is responsible for its assertion and for specifying the aforementioned Criteria. Our responsibility is to express an opinion on management's assertion based on our examination.

CGAE's makes use of external registration authorities for specific subscriber registration activities as disclosed in Consejo General de la Abogacía Española business practice disclosures. Our examination did not extend to the controls of external registration authorities.

CGAE's does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our examination did not extend to controls that would address those criteria. ^(F)

Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of CGAE's key and certificate life cycle management business practices, policies, processes and controls, and its suitability of the design and implementation of the controls intended to achieve the Criteria and examining evidence supporting management's assertion and performing such other procedures over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate life cycle management operations, and over the development, maintenance and operation of systems integrity as we considered necessary in the circumstances; (2) selectively testing transactions executed in accordance with disclosed key and certificate life cycle 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. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

The relative effectiveness and significance of specific controls at CGAE's 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.

Our examination was not conducted for the purpose of evaluating CGAE's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its internal control, Consejo General de la Abogacía Española may achieve reasonable, but not absolute assurance that all security events are prevented and, for those controls may provide reasonable, but not absolute assurance that its commitments and system requirements are



achieved. Controls may not prevent or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements.

Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with

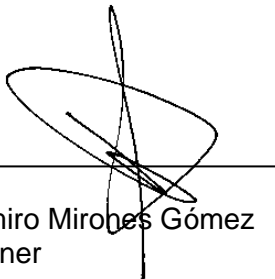
the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity. Furthermore, the projection of any evaluations of effectiveness to future periods is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations.

In our opinion, CGAE's management's assertion referred to above, is fairly stated, in all material respects, based on the aforementioned criteria.

The WebTrust seal of assurance for Certification Authority on CGAE's website 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.

This report does not include any representation as to the quality of CGAE's CA services beyond those covered by the [Trust Services Principles and Criteria for Certification Authorities Version 2.1](#) criteria, or the suitability of any of CGAE's services for any customer's intended purpose.

EY TRANSFORMA SERVICIOS DE CONSULTORIA, S.L.



Ramiro Mirores Gómez
Partner

June 30st 2020

Appendix A:

Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA Fingerprint - 256
CA ACA ROOT	1a 55 e4 15 31 e2 31 9b 11 d4 88 71 7a 00 3d 70 28 05 bf cd	47 43 91 24 3f ce c3 0d 57 48 28 6b ee 80 5d ab	97 f6 54 85 9c bd e5 86 fd 90 31 1e 82 ec 79 02 c2 38 cb a0 d6 e5 29 56 4c 9c 88 f4 48 95 ec 50
ACA ROOT / CA Subordinada ACA CA1	72 a9 e7 d6 8e 02 67 a0 4a 4c 1a 67 31 bc b7 fe cb 84 b4 9b	49 1e f8 c2 bf 47 24 d3 57 6b d1 81 fc 67 05 ad	70 5e b3 a0 b1 f0 9d ed a3 ed 45 76 6b bb c0 21 97 70 0a bb 1e 2d 1d 9e 28 62 ac 58 9d c9 fd 77
ACA ROOT / CA Subordinada ACA CA2	8a 15 1f af 74 ef 1f 01 07 73 2a 90 2a 41 09 7e 1b 48 d0 c0	49 a9 1d a5 cd 0d 70 c3 57 6b d1 1e 00 9d 55 dd	7e 93 16 a5 ce cf b9 0a 53 ad c3 c7 76 94 50 f4 2c dc 3a 9b 85 df 4c 75 77 b0 53 dc bb 25 58 12
ACA ROOT / CA Subordinada ACA CA3	3d d8 dd 01 ba c6 28 c5 4c b5 39 c2 f0 ad e6 d7 35 95 4f 2f	56 0f 1e 56 a6 30 b0 d4 57 6b cf e9 0f ba 2c eb	af 57 fd 80 5a 0e f9 0e 97 57 65 c0 d5 d5 5e 3f d2 4c fc 49 b7 3 ^a a1 a4 9e 19 79 01 8d 54 fc 26

Management's Assertion Regarding the Effectiveness of Its Controls
Over its Certification Authority Services
Based on the Trust Services Principles and Criteria for Certification Authorities Version 2.1

June 30, 2020

We, as management of Consejo General de la Abogacía Española (CGAE), are responsible for operating a Certification Authority (CA) at Spain for the Root CA, and subordinate CAs listed in Appendix A.

CGAE's CA services provide the following certification authority services:

- ▶ Certificados cualificados de firma electrónica (QCert for ESig)
- ▶ Certificados cualificados de sello (QCert for ESig)
- ▶ Certificados cualificados de autenticación web (QWAC)

Nombre de la Política de Certificación	OID
ACA CA1	Certificados Cualificados de Colegiado
	Certificados Cualificados de Personal Administrativo
	Certificados Cualificados de representante de persona jurídica
	Certificados Cualificados de abogado europeo
ACA CA2	Certificados Cualificados de sello electrónico
	Certificados Cualificados de Personal de colegio profesional
	Certificados Cualificados de Autorizado
	The Law Society of Scotland Qualified Certificates'
ACA CA3	Certificados Cualificados de autenticación de sitio web

Subordinate CA certification

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.

Controls have inherent limitations, including the possibility of human error and the circumvention or overriding of controls. Accordingly, even effective controls can provide only reasonable assurance with respect to CGAE's CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Management of CGAE has assessed the disclosure of its certificate practices and its controls over its CA operations. Based on that assessment, in CGAE Management's opinion, in providing its CA services for the Root CA and Subordinate CAs listed in Appendix A at Spain locations during the period from April 1st 2019 through March 31st 2020, CGAE's has:

- ▶ Disclosed its Business, Key Life Cycle Management, and Certificate Life Cycle Management, and CA Environmental Control practices as below:
 - CPS_ACA_017.0 - DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AUTORIDAD DE CERTIFICACIÓN DE LA ABOGACÍA and
 - CP1_ACA_009.0.pdf
 - CP2_ACA_009.pdf
 - CP8_ACA_CA1_003.0.pdf
 - CP7_ACA_004.0.pdf
 - CP2_ACATC_006.0.pdf
 - CP4_ACATC_004.0.pdf
 - CP7_ACA_CA2_002.pdf
 - CP6_ACATC_003.0.pdf
 - CP1_ACA_CA3_002.pdf

<https://www.abogacia.es/site/aca/politicas-y-practicas-de-certificacion/>

- ▶ Maintained effective controls to provide reasonable assurance that:
 - **CGAE** - CA's Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)]
 - **CGAE'** - CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)
- ▶ Maintained effective controls to provide reasonable assurance that:
 - The integrity of keys and certificates it manages was established and protected throughout their life cycles;
 - The integrity of subscriber keys and certificates it manages was established and protected throughout their life cycles;
 - The Subscriber information was properly authenticated (for the registration activities performed by CGAE's); and

- Subordinate CA certificate requests were accurate, authenticated and approved
- ▶ Maintained effective controls to provide reasonable assurance that:
 - Logical and physical access to CA systems and data was restricted to authorized individuals;
 - The continuity of key and certificate management operations was maintained; and
 - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity

for the Root CA, and subordinate CAs listed in Appendix A, based on the *Trust Services Principles and Criteria for Certification Authorities Version 2.1*¹, 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

¹ <http://www.webtrust.org/principles-and-criteria/item83172.aspx>



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



Very truly yours,

Victoria Ortega Benito
President of Consejo General de la Abogacía

June, 30th 2020

Appendix A

Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA Fingerprint - 256
CA ACA ROOT	1a 55 e4 15 31 e2 31 9b 11 d4 88 71 7a 00 3d 70 28 05 bf cd	47 43 91 24 3f ce c3 0d 57 48 28 6b ee 80 5d ab	97 f6 54 85 9c bd e5 86 fd 90 31 1e 82 ec 79 02 c2 38 cb a0 d6 e5 29 56 4c 9c 88 f4 48 95 ec 50
ACA ROOT / CA Subordinada ACA CA1	72 a9 e7 d6 8e 02 67 a0 4a 4c 1a 67 31 bc b7 fe cb 84 b4 9b	49 1e f8 c2 bf 47 24 d3 57 6b d1 81 fc 67 05 ad	70 5e b3 a0 b1 f0 9d ed a3 ed 45 76 6b bb c0 21 97 70 0a bb 1e 2d 1d 9e 28 62 ac 58 9d c9 fd 77
ACA ROOT / CA Subordinada ACA CA2	8a 15 1f af 74 ef 1f 01 07 73 2a 90 2a 41 09 7e 1b 48 d0 c0	49 a9 1d a5 cd 0d 70 c3 57 6b d1 1e 00 9d 55 dd	7e 93 16 a5 ce cf b9 0a 53 ad c3 c7 76 94 50 f4 2c dc 3a 9b 85 df 4c 75 77 b0 53 dc bb 25 58 12
ACA ROOT / CA Subordinada ACA CA3	3d d8 dd 01 ba c6 28 c5 4c b5 39 c2 f0 ad e6 d7 35 95 4f 2f	56 0f 1e 56 a6 30 b0 d4 57 6b cf e9 0f ba 2c eb	af 57 fd 80 5a 0e f9 0e 97 57 65 c0 d5 d5 5e 3f d2 4c fc 49 b7 3 ^a a1 a4 9e 19 79 01 8d 54 fc 26