

Report of Independent Accountants

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

We have examined the accompanying assertion¹ made by the management Consejo General de la Abogacía Española (CGAE), titled “**Management’s Assertion Regarding the Effectiveness of Its Controls Over the Certification Authority Services. Based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3**” that provides its Certification Authority (CA) services at Spain, throughout the period April 1st 2019 to March 31st 2020 for CAs as enumerated in Appendix A, CGAE has:

- Disclosed its SSL certificate lifecycle management business practices in its:
 - CPS_ACA_017.0 - DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA
 - AUTORIDAD DE CERTIFICACIÓN DE LA ABOGACÍA and
 - CP1_ACA_CA3_002.pdf

including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the ABC-CA website, and provided such services in accordance with its disclosed practices

- Maintained effective controls to provide reasonable assurance that:
 - The integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
 - SSL subscriber information is properly authenticated (for the registration activities performed by CGAE).
- 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.
- Maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

based on the [WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3](#).

CGAE 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.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management’s assertion is fairly stated, in all material respects. An examination involves performing procedures

¹ Hyperlink to management assertion

to obtain evidence about management's assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertion, 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 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, CGAE 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.

YCGAE's use of the WebTrust for Certification Authorities – SSL Baseline with Network Security 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.

This report does not include any representation as to the quality of CGAE's CA services beyond those covered by the [WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3](#) criteria, or the suitability of any of CGAE's services for any customer's intended purpose.



EY TRANSFORMA SERVICIOS DE CONSULTORIA, S.L.

A handwritten signature in black ink, consisting of several overlapping loops and a vertical line, positioned above a horizontal line.

Ramiro Mirones Gómez - Partner

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 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 the Certification Authority Services
Based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with
Network Security v2.3

June 30, 2020

We, as the management of Consejo General de la Abogacía Española (CGAE), are responsible for operating the SSL Certification Authority (CA) services at Spain for the the Root CA and Subordinate CA in scope for SSL Baseline Requirements and Network Security Requirements listed at Appendix A.

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 disclosures of its certificate practices and controls over its SSL CA services. Based on that assessment, in providing its SSL Certification Authority (CA) services at Spain throughout the period from April 1st 2019 through March 31st 2020, CGAE has:

- Disclosed its SSL certificate lifecycle management business practices in its:
 - CPS_ACA_017.0 - DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AUTORIDAD DE CERTIFICACIÓN DE LA ABOGACÍA and
 - CP1_ACA_CA3_002.pdf

including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the CGAE website, and provided such services in accordance with its disclosed practices

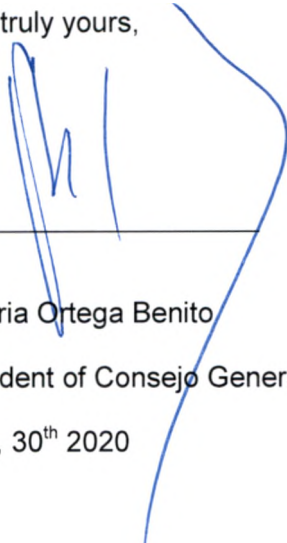
- Maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and SSL certificates it manages was established and protected throughout their lifecycles; and
 - SSL subscriber information was properly authenticated (for the registration activities performed by CGAE)

- 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 are properly authorized and performed to maintain CA systems integrity

- Maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

for the Root CA and Subordinate CA in scope for SSL Baseline Requirements and Network Security Requirements at Appendix A, based on the [WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3.](#)

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 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