

Report of Independent Accountants

To the Management of Consejo General de la Abogacia (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 2018 to March 30th 2019 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
 - **ACA CA1, ACA CA2 and ACA CA3**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 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.

¹ Hyperlink to management assertion

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.

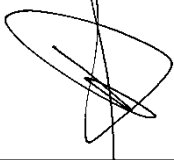
Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the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

CGAE'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.

ERNST & YOUNG, S.L.



Ramiro Mirones Gómez - Partner

December 26th 2019

Appendix A

Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
CA ACA Corporativos 2014 - SHA 1	20 4d 1a 60 2d 8a 3a 5f 53 17 57 7a ea 56 0b 1a	33 6d d0 e9 cd 18 d7 b4 eb 4e fc f3 e3 cd fb 3d 5b c0 a3 9e	c0 b0 e5 a1 28 d1 4d 73 c1 61 28 b2 c5 47 92 95 f7 e4 a1 20
CA ACA Trusted 2014- SHA 1	81 8f d1 63 00 4a ca 4d 20 97 a6 52 00 60 2e d2 cc 36 8b 6d	4d a0 9e b2 fb 90 ca c2 53 17 59 38 18 0f 74 e8	e6 a4 b6 e4 d7 4a 0f 70 c3 57 8a c6 53 12 b5 03 84 fc bf 3d
CA ACA Corporativos 2014 -SHA256	33 6d d0 e9 cd 18 d7 b4 eb 4e fc f3 e3 cd fb 3d 5b c0 a3 9e	25 d3 1c 4b 67 ea b2 00 56 15 1d c6 71 f4 98 cf	b1 22 95 ea 9d d8 75 56 e3 81 69 49 c4 6d d7 63 b1 f4 bd 4c
CA ACA Trusted 2014 -SHA 256	81 8f d1 63 00 4a ca 4d 20 97 a6 52 00 60 2e d2 cc 36 8b 6d	5d 5c dd 22 5d 86 96 a4 56 15 1f 8b 01 09 b4 10	5b 2a ea db a3 f0 cc ef d0 7f 32 86 19 3b 2b 88 19 6a f2 cb
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	53 d2 7d e6 05 85 83 49 fa 2b d5 81 d3 86 40 7e ee 73 25 17
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	5c 4d f5 dd c8 e2 69 a3 5d 26 ec 18 e1 44 02 f1 09 b2 50 30
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	58 49 0a 3f 3e cc 96 d0 87 59 ed 2b 09 1f 28 f1 3b 2a fa ac

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

December 26, 2019

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 CGAE Root CA, ACA – Certificados Corporativos 2014 sub CA and ACA-Trusted Certificates 2014 sub CA, and ACA Root, ACA – CA1 sub CA, ACA – CA2 sub CA and ACA – CA3 sub CA in scope for SSL Baseline Requirements and Network Security Requirements listed at Appendix A.

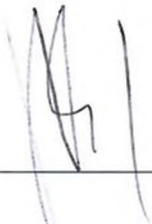
Controls have inherent limitations, including the possibility of human error and the circumvention or overriding of controls. Accordingly, even effective controls can provide only reasonable assurance with respect to CGAE's CA operations. Furthermore, because of changes in conditions, the effectiveness 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 2018 through March 31st 2019, 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
 - **ACA CA1, ACA CA2 and ACA CA3**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(s) and Subordinate CA(s) 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

Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
CA ACA Corporativos 2014 - SHA 1	20 4d 1a 60 2d 8a 3a 5f 53 17 57 7a ea 56 0b 1a	33 6d d0 e9 cd 18 d7 b4 eb 4e fc f3 e3 cd fb 3d 5b c0 a3 9e	c0 b0 e5 a1 28 d1 4d 73 c1 61 28 b2 c5 47 92 95 f7 e4 a1 20
CA ACA Trusted 2014- SHA 1	81 8f d1 63 00 4a ca 4d 20 97 a6 52 00 60 2e d2 cc 36 8b 6d	4d a0 9e b2 fb 90 ca c2 53 17 59 38 18 0f 74 e8	e6 a4 b6 e4 d7 4a 0f 70 c3 57 8a c6 53 12 b5 03 84 fc bf 3d
CA ACA Corporativos 2014 -SHA256	33 6d d0 e9 cd 18 d7 b4 eb 4e fc f3 e3 cd fb 3d 5b c0 a3 9e	25 d3 1c 4b 67 ea b2 00 56 15 1d c6 71 f4 98 cf	b1 22 95 ea 9d d8 75 56 e3 81 69 49 c4 6d d7 63 b1 f4 bd 4c
CA ACA Trusted 2014 -SHA 256	81 8f d1 63 00 4a ca 4d 20 97 a6 52 00 60 2e d2 cc 36 8b 6d	5d 5c dd 22 5d 86 96 a4 56 15 1f 8b 01 09 b4 10	5b 2a ea db a3 f0 cc ef d0 7f 32 86 19 3b 2b 88 19 6a f2 cb
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	53 d2 7d e6 05 85 83 49 fa 2b d5 81 d3 86 40 7e ee 73 25 17
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	5c 4d f5 dd c8 e2 69 a3 5d 26 ec 18 e1 44 02 f1 09 b2 50 30
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	58 49 0a 3f 3e cc 96 d0 87 59 ed 2b 09 1f 28 f1 3b 2a fa ac