

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 2.2.2

May 9th, 2023

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

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

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

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, 2022, through March 31st, 2023, CGAE's has:

- ▶ Disclosed its Business, Key Life Cycle Management, and Certificate Life Cycle Management, and CA Environmental Control practices as below:

CA Name	CPS Name	Policy identifier	CPS Link
ACA ROOT	Declaración de Prácticas de Certificación	1.3.6.1.4.1.16533.10.1.1	CPS_ACA_020.0.pdf
CA Name	Certificate Name	Policy identifier	CP Link
ACA CA1	Certificados Cualificados de Colegiado	1.3.6.1.4.1.16533.10.2.1	CP1_ACA_013.0.pdf
	Certificados Cualificados de Personal Administrativo	1.3.6.1.4.1.16533.10.3.1	CP2_ACA_013.0.pdf
	Certificados Cualificados de representante de persona jurídica	1.3.6.1.4.1.16533.10.10.1	CP8_ACA_CA1_006.0.pdf
	Certificados Cualificados de abogado europeo	1.3.6.1.4.1.16533.10.9.1	CP7_ACA_008.0.pdf

ACA CA2	Certificados Cualificados de sello electrónico	1.3.6.1.4.1.16533.20.3.1	CP2 ACATC 009.0.pdf
	Certificados Cualificados de Personal de colegio profesional	1.3.6.1.4.1.16533.20.4.1	CP4 ACATC 008.0.pdf
	Certificados Cualificados de Autorizado	1.3.6.1.4.1.16533.20.6.1	CP7 ACA CA2 006.pdf
	The Law Society of Scotland Qualified Certificates'	1.3.6.1.4.1.16533.20.5.1	CP6 ACATC-005.0.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 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 2.2.2](#), including the following:

CA Business Practices Disclosure

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

CA Business Practices Management

- Certification Practice Statement (CPS) Management
- Certificate Policy (CP) 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, Maintenance, and Change Management
- Disaster Recovery, Backups, and 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
- CA Key Destruction
- CA Key Compromise
- CA Cryptographic Hardware Life Cycle Management
- CA Key Escrow
- CA Key Transportation
- CA Key Migration

Subscriber Key Lifecycle 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

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

Subordinate CA and Cross Certificate Lifecycle Management Controls

- Subordinate CA Certificate and Cross Certificate Lifecycle Management

Very truly yours,

Victoria Ortega Benito
President of Consejo General de la Abogacía

May 9th, 2023

Appendix A

Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA Fingerprint - 256	MD5 Fingerprint
CA ACA ROOT	1a55e41531e2319b11d488717a003d702805bfcd	474391243fcec30d5748286bee805dab	97f654859cbde586fd90311e82ec7902c238cba0d6e529564c9c88f44895ec50	d496592b305707386cc5f3cdb259ae66d7661fca
ACA ROOT / CA Subordinada ACA CA1	72a9e7d68e0267a04a4c1a6731bc b7fecb84b49b	491ef8c2bf4724d3576bd181fc6705ad	705eb3a0b1f09deda3ed45766bbbc02197700abb1e2d1d9e2862ac589dc9fd77	53d27de605858349fa2bd581d386407eee732517
ACA ROOT / CA Subordinada ACA CA2	8a151faf74ef1f0107732a902a41097e1b48d0c0	49a91da5cd0d70c3576bd11e009d55dd	7e9316a5cecfb90a53adc3c7769450f42cdc3a9b85df4c7577b053dccb255812	5c4df5ddc8e269a35d26ec18e14402f109b25030