Abogacía Española
CONSEJO GENERAL

AUTORIDAD DE CERTIFICACIÓN DE LA ABOGACÍA

Certification Practice Statement

(CPS_ACA_020.0)

Public Document

This document has been translated by an automatic translation system. Although it has been reviewed, the correct translation of all terms cannot be guaranteed.
Please contact us if you need any clarification on terminology Contacto - Abogacía Española (abogacia.es)
Original document can be found at Políticas y prácticas de certificación - Abogacía Española (abogacia.es)

VERSION CONTROL

Version	Date	Description / Relevant Changes
27/03/2003	CPS_ACA_001.0	Initial version
02/03/2004	CPS_ACA_001.1	Error Correction, Modification of certificate profile AKI extensions. Changes in CA certificate profile and CRL profile.
26/10/2004	CPS_ACA_002.0	General review. Modifications for better adaptation to the provisions of Law 59/2003 on Electronic Signature and greater clarity for subscribers and users.
17/08/2005	CPS_ACA_002.1	Updating new root certificate
13/03/2006	CPS_ACA_003.0	Adaptation to new DPC environment
13/07/2006	CPS_ACA_004.0	Inclusion of Legal Entity Certificates
24/10/2006	CPS_ACA_005.0	Inclusion of Secure Server Certificates
25/05/2007	CPS_ACA_006.0	Inclusion of legal entity certificates software
02/03/2009	CPS_ACA_007.0	Fax is included as a contact The renewal procedure is detailed The process for notification of suspension or revocation is detailed The suspension procedure is detailed Inclusion of E-Stamp certificates
02/09/2009	CPS_ACA_008.0	Trusted CA is included which depends on our hierarchy and with the corresponding policies
28/02/2010	CPS_ACA_009.0	Including the software legal entity certificate policy under the Trusted CA
01/10/2010	CPS_ACA_010.0	Including the software e-Stamp certificate policy under the Trusted CA
21/12/2010	CPS_ACA_011.0	Including the policy of recognized certificate of professional association personnel
01/10/2011	CPS_ACA_012.0	European lawyer recognized certificate policy included
11/03/2014	CPS_ACA_013.0	A description of the PKI Hierarchy is included Fingerprints are included for intermediate CAs 2014 Details of the Cryptographic module model are eliminated Increased the length of user keys to 2048 bits

13/04/2016	CPS_ACA_014.0	The denomination of "qualified certificate" is eliminated for Penalnet certificates
27/06/2016	CPS_ACA_015.0	New PKI Hierarchy is included, new CAs certificates information Aligned with eIDAS Adaptation of recognized services to qualified Registration of new qualified service of Representative of Legal Entity Registration of new qualified service of Authorized Person Registration of new qualified Web Site Authentication service Legal Entity, Legal Entity in Software, Penalnet Lawyer, Legal Entity in Software.
14/09/2016	CPS_ACA_016.0	Amendments are incorporated for alignment with the provisions of Article 24.4 of Regulation 910/2014 (eIDAs)
03/05/2017	CPS_ACA_017.0	Including SPC review procedure Including PDS access link Including PDS access link Public key generation parameters are included Certificate validation mode is included after the validity period of the certificate by means of OCSP
02/06/2020	CPS_ACA_018.0	Adequacy of the document to RFC 3647 Updating point 5 physical security controls
31/05/2022	CPS_ACA_019.0	Change of document template Elimination of duplicated sections with the Certification Policies Legislative adaptation Law 6/2020, of November 11, 2010 Updating acronyms
21/03/2023	CPS_ACA_020.0	Annual legislative review Update section 4.9.5 indicating that if a revocation request cannot be confirmed within 24 hours it does not revoke the certificate. Update section 5.8 informing how the termination of service information will be provided. Update of section 7.1 indicating that the size of the fields can be larger than those established in RFC 5280. Update section 9.6.4 and Summary of rights and obligations indicating the user's obligation to check the TSL

INDEX

Contenido

Summary of the fundamental rights and obligations contained in this Certification Practice Statement (CPS)

tHIS TEXT IS A MERE SYNTHESIS OF THE COMPLETE CONTENT OF THE DECLARATION OF PRACTICS OF CERTIFICATION (CPS). WE RECOMMEND THAT YOU READ ITS FULL TEXT AND THE OTHER RELATED DOCUMENTS TO OBTAIN A CLEAR VIEW OF THE OBJECTIVES OF THE PROJECT, SPECIFICATIONS, STANDARDS, PROCESSES, RIGHTS AND OBLIGATIONS GOVERNING THE PROVISION OF THE CERTIFICATION SERVICE.

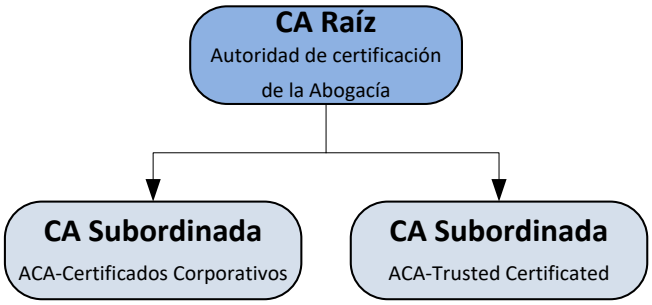
- This Certification Practice Statement (CPS) and related documents regulate everything related to the application, issuance, acceptance, renewal, reissuance, suspension and revocation of certificates among many other vital aspects for the life of the certificate and the legal regime that is established between the Applicant/Subscriber, the Certification and Registration Authority, and the Users who rely on certificates and third parties.
- Both the Certification Practice Statement (CPS) and all other related documents are made available to prospective Applicants, Subscribers and Users at the following Internet address http://www.acabogacia.org/doc so that they know exactly before hiring or relying on AC Abogacía which are the rules and regulations applicable to our certification system.
- AC Abogacía issues several types of certificates, so the Applicant of a certificate must know the conditions established in the Certification Practices Statement (CPS) and in the corresponding Certification Policies of that type of certificate, so that he/she can proceed correctly to the application and use of the certificate.
- The Applicant shall request the corresponding certificate in the manner established in the procedure determined in the Certification Practice Statement (CPS) and related documents.
- It is essential for the Subscriber to keep the private keys of his certificate safe, because if he does not take the appropriate measures, the security system to be implemented will be meaningless. In this sense, it is necessary to immediately inform AC Abogacía when there is any cause for revocation/suspension of the certificate established in the Certification Practices Statement (CPS) and proceed, in this way, to its suspension in order to avoid an illegitimate use of the certificate by an unauthorized third party.
- The subscriber must communicate to AC Abogacía any modification or variation of the data provided to obtain the certificate, whether they appear in the certificate itself or not.
- The Subscriber must make proper use of the certificate, and it will be the Subscriber's sole responsibility to use the certificate in a manner different from the uses provided in the Certification Practices Statement (CPS) and other related documents.
- It is the User's obligation to check in the Certificate Repository published by AC Abogacía that the certificate he/she intends to trust and the rest of the certificates in the chain of trust are valid and have not expired or been suspended or revoked.
- The user must verify by his own mechanisms, that the hierarchy with which the certificate is issued is in the list of qualified certificates of the European Union (TSL).
- The Certification Practices Statement (CPS) and related documents establish the liability of AC Abogacía and the Applicants, Subscribers and Users, as well as the limitation of the same in the event of possible damages.

1. Introduction

The Consejo General de la Abogacía Española (CGAE) is the representative, coordinating and executive body of the Bar Associations of Spain and has, for all purposes, the status of a public law corporation, with its own legal personality and full capacity to fulfill its purposes.

The Consejo General de la Abogacía Española has become a Trust Service Provider through the creation of its own PKI hierarchy. In compliance with Regulation 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.

The general structure of ACA's PKI is composed of two levels

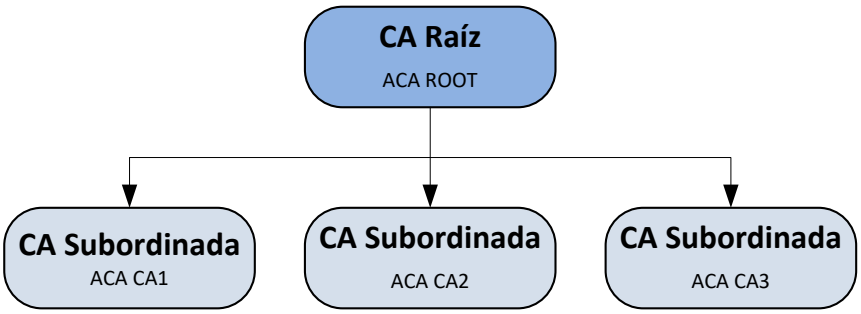


In 2014 new subordinated CAs were generated with the same denomination followed by the year of issuance: *ACA - Corporate Certificates 2014 and ACA-Trusted Certificates 2014.*

The certificates issued by both subordinated CAs have continuity with the same OIDs in the 2014 version CAs.

On the other hand, in 2016 a new Root CA and subordinate CAs have been generated in accordance with the legislation in force and the described ones are maintained since the certificates issued by these hierarchies are in force. New certificates will be issued through the new subordinated CAs.

New Hierarchy 2016, composed of two levels:



1.1. Overview

This document specifies the Certification Practices Statement of the Certification Authority constituted by the General Council of the Spanish Bar, called the Certification Authority of the Spanish Bar (AC Abogacía), for the issuance of certificates, and is based on the specification of the RCF 3647 standard - Internet X. 509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, of the IETF.

The Certification Practice Statement (CPS) of the Certification Authority of the Bar that establishes the specific terms of the service provided can be found at http://www.acabogacia.org/doc.

As AC Abogacia is a private Trust Service Provider established in Spain, the applicable legal regulations are as follows:

- REGULATION (EU) 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, hereinafter ReIDAS.
- Law 6/2020, of November 11, 1920, regulating certain aspects of electronic trust services.
- Order ETD/465/2021, of May 6, regulating remote video identification methods for the issuance of qualified electronic certificates.

The Consejo General de la Abogacía Española, as the regulatory body for the legal profession, establishes a certification system with the aim of issuing certificates for different uses and different end users. For this reason, types of certificates are established. Certificates are issued to end entities, including members, administrative and service staff, organizations and individuals representing such organizations, by CGAE Certification Authorities.

This Certification Practices Statement (CPS) is in accordance with the certification policies related to the different certificates issued by AC Abogacía and identified in the section "Scope of Application and Uses" of this Certification Practices Statement (CPS). In case of contradiction between the two documents, the provisions of the specific certification policies of each type of certificate issued shall prevail.

The CA Abogacía, governed by this Certification Practices Statement (CPS) and the aforementioned policies, establishes the issuance of the following types of certificates:

1. Service for issuance of qualified electronic signature certificates (QCP-n-qscd)
2. Service for issuance of qualified electronic certificates of electronic seal (QCP-l)

Qualified certificates are qualified in accordance with the provisions of Art. 28 of ReIDAS, being mandatory the use of a qualified electronic signature creation device that meets the definitions of Art. 51 of ReIDAS for the generation and custody of the signature creation data of the subscriber, and the creation of signatures

Additionally, and exclusively for internal use to support the operations of the CA and RA management system, a series of specific certificates associated with the different administration and operation roles will be issued, as well as certificates that allow secure communication between the different technical components of the system. These certificates are simply a form of technical element necessary for the correct and secure management of the life cycle of the aforementioned types of certificates.

This Certification Practices Statement (CPS) defines the way in which the CA Abogacía responds to all the requirements and security levels imposed by the certification policies.

Regarding the content of this Certification Practice Statement (CPS), it is considered that the reader is familiar with the basic concepts of PKI, certification and digital signature, recommending that, in case of ignorance of these concepts, the reader is informed in this regard.

1.2. Document identification

Name:	CPS_ACA_20.0
OID	1.3.6.1.4.1.16533.10.1.1
Description:	Certification Practices Statement of the Certification Authority of the Lawyers' Bar
Version:	020.0
Date of Issue:	21/03/2023
Location:	www.acabogacia.org/doc

1.3. Community and Scope of Application

1.3.1. Certification Authority (CA)

The entity responsible for the issuance and management of digital certificates is the General Council of Spanish Lawyers (CGAE), which constitutes a certification system under the name AC Abogacía and with its own PKI hierarchy.

The CGAE hierarchy is composed of:

AC Root is the first level Certification Authority. This CA only issues certificates for itself and its SubCAs. It shall only be in operation during the performance of the operations for which it is established. The most relevant information of the certificate:

Distinctive Name	CN = ACA ROOT, SERIAL NUMBER = Q2863006I, O = CONSEJO GENERAL DE LA ABOGACIA, C = ES
Serial number	47 43 91 24 3f ce c3 0d 57 48 28 6b ee 80 5d ab
Validity period	Since Friday, May 27, 2016 Until Monday, May 27, 2041
Fingerprint (SHA1)	d496592b305707386cc5f3cdb259ae66d7661fca
Fingerprint (SHA256)	97f654859cbde586fd90311e82ec7902c238cba0d6e529564

	c9c88f44895ec50
Fingerprint (SHA512)	eabb682b4764d41b4eebcdf35eccb65ed8f8a4b48d674aa35 a16f08c90422d717de175073d36aeaefa1b1d762108c41b94 c116c5100e4efae6e0a644c865bc66

Subordinate CAs, are the subordinate Certification Authorities of "ACA CA ROOT", for the issuance of final certificates. This is the most relevant information:

Distinctive Name	CN = ACA CA1, OI = VATES-Q2863006I, OU = AUTORIDAD DE CERTIFICACION DE LA ABOGACIA, O = CONSEJO GENERAL DE LA ABOGACIA, C = ES
Serial number	49 1e f8 c2 bf 47 24 d3 57 6b d1 81 fc 67 05 ad
Validity period	As of Thursday, June 23, 2016 Until Sunday, June 23, 2030
Fingerprint (SHA1)	53d27de605858349fa2bd581d386407eee732517
Fingerprint (SHA256)	705eb3a0b1f09deda3ed45766bbbc02197700abb1e2d1d9e28 62ac589dc9fd77
Fingerprint (SHA512)	476b08aa3c2c1095eb1a131a08f67a4aba11950fec224fba7f 3a665c13dc858087d0f1b981ecac5aa457d73d2de4af5b4f65 9b51f524b98dc02c3b2719612b42

Distinctive Name	CN = ACA CA2, OI = VATES-Q2863006I, OU = AUTORIDAD DE CERTIFICACION DE LA ABOGACIA, O = CONSEJO GENERAL DE LA ABOGACIA, C = ES
Serial number	49 a9 1d a5 cd 0d 70 c3 57 6b d1 1e 00 9d 55 dd
Validity period	As of Thursday, June 23, 2016 Until Sunday, June 23, 2030
Fingerprint (SHA1)	5c4df5ddc8e269a35d26ec18e14402f109b25030
Fingerprint (SHA256)	7e9316a5cecfb90a53adc3c7769450f42cdc3a9b85df4c7577b 053dcbb255812
Fingerprint (SHA512)	87266affec18817227c786842b1d591650ed7f6d84226dff651 fefbe48efacbedc12c6a69427a1b3c4eb23863197e72edb00aa a0d26edffc1f760aa636c91d89

Distinctive Name	CN = ACA CA3, OI = VATES-Q2863006I, OU = AUTORIDAD DE CERTIFICACION DE LA ABOGACIA, O = CONSEJO GENERAL DE LA ABOGACIA, C = ES
Serial number	56 0f 1e 56 a6 30 b0 d4 57 6b cf e9 0f ba 2c eb
Validity period	As of Thursday, June 23, 2016 Until Sunday, June 23, 2030
Fingerprint (SHA1)	58490a3f3ecc96d08759ed2b091f28f13b2afaac
Fingerprint (SHA256)	af57fd805a0ef90e975765c0d5d55e3fd24cfc49 b73aa1a49e1979018d54fc26
Fingerprint (SHA512)	764c7061fb3d76dbc61c3431c08353e7ffda79db aedaab1b7142bfe8490efa97ad24f94bcb495fa9 b1b70b9c728ad7a7de37a3a9646bde38cc4d9717 ce4ef443

Information regarding the CA can be found at www.acabogacia.org.

1.3.2. Registration Authority (RA)

For the purposes of this Certification Practice Statement (CPS), the following entities may act as Certificate Registration Authorities:

a) General Council of Spanish Lawyers (CGAE)

b) The Autonomous Councils of the Legal Profession

c) Bar Associations (exclusive registrars for the Certificate of Membership)

d) Any other entity delegated by the CA upon signature of a contract

In the Spanish territory, only the Bar Associations can be Registrars for their members, due to the fact that the Bar Associations have the exclusive certifying capacity regarding the status of lawyer.

1.3.3. Subscriber

It is the natural or legal person in favor of whom the certificate is issued, and identified in the distinguished name (DN) x501 of the certificate. In the case of qualified certificates issued to a natural person, the subscriber may also be called "Signatory". In the case of qualified certificates issued to a legal entity, the subscriber is also called the "seal creator".

The details of the subscribers for each type of certificate are defined in each Certification Policy.

1.3.4. User

In this Certification Practice Statement (CPS), the term User, trusted third party, means the person who voluntarily trusts the AC Abogacía Certificate. The details of the users for each type of certificate are defined in each Certification Policy.

1.3.5. Other participants

Not stipulated

1.4. Scope of Application and Uses

This Certification Practice Statement (CPS) responds to the following certification policies, which can be found at www.acabogacia.org/doc

Qualified Member Certificate Policy (OID 1.3.6.1.4.1.16533.10.2.1)	QCP-n-qscd
Administrative Personnel Qualified Certificate Policy (OID 1.3.6.1.4.1.16533.10.3.1)	QCP-n-qscd
Qualified Legal Entity Representative Certificate Policy (OID 1.3.6.1.4.1.16533.10.10.1)	QCP-n-qscd
Qualified E-Stamp Certificate Policy (OID 1.3.6.1.4.1.16533.20.3.1)	QCP-l
Qualified Professional College Personnel Certificates (OID 1.3.6.1.1.4.1.16533.20.4.1)	QCP-n-qscd
European Lawyer Qualified Certificates (OID 1.3.6.1.4.1.16533.10.9.1)	QCP-n-qscd
The Law Society of Scotland Qualified Certificates (OID 1.3.6.1.4.1.16533.20.5.1)	QCP-n-qscd

Qualified "Authorized" Certificates (OID 1.3.6.1.4.1.16533.20.6.1)	

1.4.1. Permitted uses of certificates

AC Abogacía certificates may be used under the terms established by the corresponding certification policies.

1.4.2. Prohibited and Unauthorized Uses

The use of certificates as provided in the Certification Practice Statement (CPS) and the corresponding specific certification policies is prohibited.

Any use contrary to Spanish and Community regulations, international conventions ratified by the Spanish State, customs, morality and public order is not permitted. The use other than what is established in the Policies and in the Certification Practices Statement is not allowed.

The certificates are not designed, intended, and are not authorized for use or resale as hazardous situation monitoring equipment or for uses requiring fail-safe performance, such as the operation of nuclear facilities, airborne navigation or communications systems, or weapons control systems, where failure could directly lead to death, personal injury or severe environmental damage.

End-entity certificates cannot be used to sign certificate issuance, renewal, suspension or revocation requests in the system, or to sign public key certificates of any kind, or to sign certificate revocation lists (CRLs or CRLs).

Alterations to the Certificates are not authorized and they must be used as supplied by the CA.

The CA does not create, store or possess at any time the private key of the subscriber of Qualified certificates, not being possible to recover the encrypted data with the corresponding public key in case of loss or disablement of the private key or the device that keeps it by the Subscriber.

The Subscriber or User who decides to encrypt information will do so in any case under his own and sole responsibility, without, consequently, the CA having any responsibility in the case of encryption of information using the keys associated with the certificate.

1.5. Policy Administration

1.5.1. Responsible organization

Certification Authority of the Bar. General

Council of Spanish Lawyers.

1.5.2. Contact person

Legal Department of the General Council of Spanish Lawyers (Consejo General de la Abogacía Española)

E-mail:	info@acabogacia.org
Phone:	915 23 25 93
Fax	915327836
Address:	Consejo General de la Abogacía Española Paseo de Recoletos, 13 28004 Madrid

1.5.3. Responsible for the adequacy of certification practices and policies

The General Council of the Spanish Bar shall be responsible for the correct adequacy of the Certification Policies and Practices

1.5.4. Policy approval procedures

The publication of revisions to this Certification Practice Statement (CPS) must be approved by AC Abogacía, after verifying compliance with the requirements established by the General Council of Spanish Lawyers.

1.6. Definitions and Acronyms

AC	Certification Authority, can also be identified by the acronym CA*(Certification Authority*)
ACA	Attorney Certification Authority
AR	Registration Authority can also be identified by the acronym RA*(Registration Authority*)
ARL	*Authority Revocation List*list of revoked certificates of the Root Certification Authority
CGAE	General Council of Spanish Lawyers
CPS	*Certification Practice Statement*the Certification Practice Statement may also be identified by the acronym CPD
CRL	*Certificate revocation list*list of revoked certificates
CSR	*Certificate Signing request*certificate signing request
DES	*Data Encryption Standard*. Data encryption standard
DN	*Distinguished Name*distinguished name within the digital certificate
DSA	*Digital Signature Algorithm*. Signature algorithm standard
DSCF/ **DCCFE**	Secure Signature Creation Device Qualified Electronic Signature Creation Device

ReIDAS	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market
FIPS	*Federal information Processing Standard publication*
IETF	*Internet Engineering task force*
ICA	Bar Association
ISO	*International Organisation for Standardization*. International standardization body
ITU	*International Telecommunications Union.* Union International telecommunications Union.
LDAP	*Lightweight Directory Access Protocol*. Directory access protocol
OCSP	*On-line Certificate Status Protocol*. Certificate status access protocol
OID	*Object identifier*. Object Identifier
PA	*Policy Authority*. Policy Authority
PC	Certification Policy can be identified by the acronym CP (Certification Policy)
PIN	*Personal Identification Number*personal Identification Number
PKI	*Public Key Infrastructure*public Key Infrastructure
PUK	*Personal Unblocking Key*unblocking Code
RSA	*Rivest-Shimar-Adleman*. Type of encryption algorithm
SHA-256	*Secure Hash Algorithm*. Secure Hash Algorithm
TLS	*Transport Layer Security. Its predecessor is SSL(p*its predecessor is SSL (protocol designed by Netscape and made standard on the Web, allowing the transmission of encrypted information between an Internet browser and a server)
TCP/IP	Transmission Control Protocol/Internet Protocol System of Protocols, defined within the framework of the IETFT. The TCP Protocol is used to divide the information into packets at the source, and then recompose it at the destination, the IP Protocol will take care of properly routing the information to its recipient.
ENS	The purpose of the National Security Scheme is to determine the security policy for the use of electronic media by the entities within its scope of application, consisting of the basic principles and minimum requirements that adequately guarantee the security of the information processed and the services provided by such entities. Royal Decree 311/2022, of May 3, which regulates the National Security Scheme.
LOPD-GDD	Organic Law 3/2018, of December 5, on Personal Data Protection and guarantee of digital rights.

2. Publication and Repository of Certificates

2.1. Repositories

AC Abogacía will make the following information available to users:

- Certification Practices and Policies on the Web www.acabogacia.org/doc
- Terms and conditions of service.
- Certificates issued.
- Certification Authority Certificates
- Revoked certificates and certificate validity information
- The document "PKI Disclosure Statement"(PDS) at at following website at Internet site http://www.acabogacia.org/doc/EN

2.2. Certificate repository

Issued certificates may be accessed, provided that the subscriber gives his consent for his certificate to be accessible, on the Internet site http://www.acabogacia.org.

A repository will be kept of all Certificates issued during the period of validity of the issuing entity.

The CA shall maintain a secure certificate storage and retrieval system and a registry of issued certificates and their status, and may delegate these functions to a third party entity. Access to the certificate registry shall be made from the AC Abogacía website(www.acabogacia.org), or through another channel considered secure by the CA.

A copy of the Certification Practices and Policies will be available in electronic format athttp://www.acabogacia.org/doc . Previous versions may be withdrawn from on-line consultation, but can be requested by interested parties at AC Abogacía.

Users can request a copy of the Certification Practices Statement (CPS) in paper format at the AC Abogacía contact address.

2.3. Frequency of publication

AC Abogacía will immediately publish any modification in the certification policies and practices, maintaining a version history.

AC Abogacía will publish the certificates in the register of certificates immediately after they have been issued.

The CA will publish a list of certificates revoked ex officio with a periodicity of 24 hours. AC Abogacía will extraordinarily publish a new revocation list at the time it processes an authenticated request for suspension or revocation.

2.4. Access controls

AC Abogacía will use different systems for the publication and distribution of certificates and CRLs. See you will need to have access data to perform multiple queries.

On the AC Abogacía website there will be access to the directory to consult CRLs and Certificates under the control of an application and protecting the indiscriminate downloading of information.

The CRL's can be downloaded anonymously via http protocol from the following URL addresses contained in the certificates themselves in the "CRL Distribution Point" extension.

3. Identification and Authentication

3.1. Name management

3.1.1. Types of names

All certificates require a distinguished name (DN or distinguished name) according to the X.501 standard.

The DN of the ACA certificates shall contain the elements established in each Certification Policy.

3.1.2. Meaning of the names

The names included in the certificates shall be meaningful and understandable.

3.1.3. Pseudonyms

In no case may anonymous names be used. Nor may pseudonyms be used to identify an organization.

3.1.4. Rules used to interpret various name formats

AC Abogacía complies in all cases with the X.500 standard of reference in ISO/IEC 9594.

3.1.5. Uniqueness of names

The distinguished names of the issued certificates will be unique for each subscriber. The CA reserves the right not to issue a certificate with the same name as one already issued to another subscriber. The e-mail attribute, membership number or VAT number are used to distinguish between two identities when there is a problem about duplicity of names.

Applicants for certificates shall not include names in applications that may involve infringement, by the prospective subscriber, of third party rights.

The CA has no liability in the case of name dispute resolution. The CA shall not determine that a certificate applicant is entitled to the name appearing on a certificate application. It shall not act as arbitrator or mediator, nor shall it in any other way resolve any dispute concerning the ownership of personal or organizational names, domain names, trademarks or trade names.

The CA reserves the right to reject a certificate request due to name conflict. Names will be

assigned based on their order of entry.

The CA in any case complies with the provisions of section 9.13 of this Certification Practice Statement (CPS).

3.1.6. Recognition, authentication and function of registered trademarks

The CA does not assume commitments in the issuance of certificates with respect to the use by subscribers of a trademark. AC Abogacía deliberately does not allow the use of a name whose right of use is not owned by the subscriber. However, the CA is not obliged to search for evidence of trademark ownership prior to the issuance of certificates.

3.2. Initial identity validation

3.2.1. Methods of proof of possession of the private key

As provided in each Certification Policy.

3.2.2. Authentication of an organization's identity

As provided in each Certification Policy

3.2.3. Authentication of an individual's identity

As provided in each Certification Policy

3.2.4. Unverified subscriber information

As provided in each Certification Policy

3.2.5. Validation of Registration Authorities

The CA shall ensure the following aspects in relation to the Registration Authorities to be established:

- That there is a contract in force between the CA and the RA, specifying the specific aspects of the delegation and the responsibilities of each agent.
- That the identity of the RA operators has been properly verified and validated.
- That RA operators have received sufficient training for the performance of their duties. That they have attended at least one operator training session.
- Express authorization from a qualified representative of the Registration Authority shall be required to act as operator.
- That the RA has been audited by an external entity appointed by the CA.
- That the RA assumes all obligations and responsibilities relating to the performance of her duties.
- That the communication between the RA and the CA is carried out in a secure manner through the use of digital certificates.
- That the RAs undertake to comply with the general security requirements indicated by the CA.

3.2.6. Interoperability Criteria

Not stipulated

3.3. Certificate renewal identification and authentication

3.3.1. Ordinary renewal

As provided in each Certification Policy

3.3.2. Reissuance after revocation

The issuance of a new certificate to a subscriber after revocation of the previous certificate shall be treated as a new issuance. In any case, the CA reserves the right to deny the reissuance if the cause of the revocation corresponds to cases of compromise of the subscriber's private key.

3.4. Identification and authentication of a revocation request

They may request the suspension or revocation of a certificate:

- The subscriber himself, in which case he must provide the revocation key that was delivered with the certificate, or he must identify himself to the RA
- Authorized operators of the subscriber's RA.
- Authorized operators of the CA or certification hierarchy.

In either of the last two cases, the circumstances set forth in the corresponding section must be met, and the revocation requests shall be made and processed in the manner described therein.

4. Operational requirements of the certificate life cycle

4.1. Request for certificates

As provided in each Certification Policy.

4.2. Certificate application procedure

As provided in each Certification Policy.

4.3. Issuance of certificates

As provided in each Certification Policy.

4.4. Acceptance of certificates

As provided in each Certification Policy.

4.5. Key pair and certificate usage

As provided in each Certification Policy.

4.6. Renewal of certificates

As provided in each Certification Policy.

4.7. Renewal of certificates and keys

As provided in each Certification Policy.

4.8. Modification of certificates

Modification of certificates once issued is not allowed.

4.9. Suspension and Revocation of certificates

The revocation of a certificate entails the loss of its validity, and is irreversible.

Suspension, unlike revocation, involves the temporary loss of validity of a certificate, and is reversible.

When the provider decides to revoke a certificate, it shall register its revocation in its certificate database and publish the certificate revocation status in a timely manner and, in any case, within 24 hours after receipt of the request. The revocation shall be effective immediately upon publication.

Suspension and revocation of certificates will be notified to the certificate subscriber by email to the email account listed on the suspended or revoked certificate in accordance with Regulation 910/2014 (ReIDAS) and Law 6/2020, of November 11, regulating certain aspects of electronic trust services

4.9.1. Causes for revocation of certificates

The revocation of a certificate may be due to any of the following causes:

1. Circumstances affecting the information contained in the certificate

- Modification of any of the data contained in the certificate.
- Discovery that any of the data contained in the certificate request is incorrect.
- Loss or change of the subscriber's relationship with the institution, in the case of Administrative Personnel Certificates

This cause for revocation may be requested by the user through the revocation code or by the RA Operator, provided that there are reasonable doubts as to any of the aforementioned causes.

2. Circumstances affecting the security of the CA's private key or the certificate

- Compromise of the private key or of the CA's infrastructure or systems, provided that it affects the reliability of the certificates issued as a result of this incident.
- Violation, by the CA or RA, of the requirements of the certificate management procedures established in the Certification Practices Statement (CPS) Certification Practice Statement (CPS).
- Compromise or suspected compromise of the security of the subscriber's key or certificate.
- Unauthorized access or use, by a third party, of the subscriber's private key.
- Irregular use of the certificate by the subscriber.
- Failure by the subscriber to comply with the rules of use of the certificate set forth in the policies, in the Certification Practice Statement (CPS) or in the binding legal instrument between the CA, the RA and the subscriber.

The causes of revocation relating to actions affecting the root or intermediate CA may only be made by the CA's administrators.

The causes of revocation related to user certificates may be requested by the user through the revocation code or by the RA Operator, whenever there are reasonable doubts as to any of the above-mentioned causes.

3. Circumstances affecting the security of the cryptographic device

- Compromise or suspected compromise of the security of the cryptographic device.
- Loss or disablement due to damage to the cryptographic device.
- Unauthorized access, by a third party, to the private key activation data.
- Failure by the subscriber to comply with the rules of use of the cryptographic device set forth in the policies, in the Certification Practice Statement (CPS) or in the binding legal instrument between the CA, the RA and the subscriber.

The causes of revocation related to actions affecting the cryptographic device where the keys of the root or intermediate CA are kept can only be carried out by the CA administrators

The causes of revocation related to user certificates may be requested by the user through the revocation code or by the RA Operator, whenever there are reasonable doubts as to any of the above-mentioned causes.

4. Circumstances affecting the subscriber

- Express and unequivocal manifestation of the subscriber or authorized third party
- Termination of the legal relationship between the CA, the RA and the Subscriber.
- Modification or termination of the underlying legal relationship or cause that allowed the issuance of the certificate to the subscriber, including the temporary disqualification of the member for professional practice.
- Infringement by the applicant of the certificate of the pre-established requirements for its application.
- Infringement by the subscriber of its obligations, responsibilities and guarantees, established in the corresponding legal instrument or in the Certification Practices Statement (CPS) of the CA.
- The supervening disability, total or partial.
- Upon the death of the subscriber.

The causes of revocation related to user certificates may be requested by the user through the revocation code or by the RA Operator, whenever there are reasonable doubts about any of the causes described above

5. Other circumstances

- The suspension of the digital certificate for a period longer than that established in the Certification Practice Statement (CPS).
- By judicial or administrative resolution ordering it.
- For the concurrence of any other cause specified in the Certification Practice Statement (CPS).

6. As well as those indicated in the applicable regulations.

The causes for revocation as a consequence of any of these circumstances shall be carried out by the RA Authorized Operators or the Administrators of the CA, provided that there are well-founded reasons.

If the RA or CA to which the revocation request is addressed does not have all the information necessary to determine the revocation of a certificate, but has indications of its compromise, it may decide to suspend it. When the subscriber becomes aware of the suspension of the certificate, he/she must refrain from using it, and contact the RA or CA to proceed with its revocation or the lifting of the suspension, if applicable.

The legal instrument that binds the CA and the RA with the subscriber shall establish that the subscriber must request the revocation of the certificate in case he/she becomes aware of any of the circumstances mentioned above.

4.9.2. Who can request revocation

They may request the revocation of a certificate:

- The subscriber himself, in which case he must provide the revocation key that was delivered with the certificate, or he must identify himself to the RA
- Authorized operators of the subscriber's RA provided that they have good cause

- Authorized Administrators of the CA whenever there is good reason to do so.

4.9.3. Revocation request procedure

The procedure for requesting revocations or suspensions can be initiated in person, by telephone or online, on the AC Abogacía website.

Face-to-face procedure:

- Application by the subscriber. The subscriber shall prove his identity before an operator of his RA, and shall state in writing his desire to revoke the suspension or revocation of the certificate. The operator will proceed to carry out the suspension or revocation, informing the subscriber that the procedure has been carried out.
- Suspend by a third party: In the event that the request is made by a third party, the operator will ask a series of questions to determine the cause of the request, receive the pertinent documentation, and if he considers that the established causes are met, he will proceed to carry out the suspension, a precautionary suspension pending further inquiries. It will also send a message to the subscriber informing him/her of the circumstance.

Online procedure:

The subscriber of a Member or employee certificate will have a web page at www.acabogacia.org from which he/she will be able to request the revocation of his/her certificate.

To do so, you must:

- Access to http://www.acabogacia.org
- Select: Revoke your signature in the user's area section
- Enter the Revocation Code provided during the certificate generation process.

The system the certificate. At the time the certificate is revoked, the subscriber shall be notified, stating the reasons, date and time when the certificate will become void.

The revocation management service will be available 24 hours a day, 7 days a week. In the event of system failure, or any other factor beyond the CA's control, the CA will make every effort to ensure that this service is not unavailable for longer than the maximum period of 24 hours.

Information regarding the status of the revocation will be available 24 hours a day, 7 days a week. In the event of system failure, or any other factor beyond the CA's control, the CA will make every effort to ensure that this information service is not unavailable for longer than the maximum period of 24 hours.

4.9.4. Grace period for revocation request

No stipulation

4.9.5. Time set for processing a revocation request

When the provider decides to revoke a certificate, it shall register its revocation in its certificate database and publish the revocation status of the certificate in a timely manner and, in any case, on a

within 24 hours after receipt of the request. The revocation shall be effective immediately upon publication. If a revocation request cannot be confirmed within 24 hours the certificate will not be revoked.

4.9.6. Obligation for users to check revocation status

Users are obliged to check the status of the certificates they are going to trust, checking in any case the last CRL issued, which can be downloaded from the URL addresses contained in the certificate itself, in the "*CRL Distribution Point*" extension.

The CRL is signed by the certificate authority that issued the certificate. The user must additionally check the relevant CRL(s) in the hierarchy certification chain.

The user should check that the revocation list is the most recent one issued as several valid revocation lists can be found at the same time. The certificates include the information necessary for access to the CRL.

The user must ensure that the revocation list is signed by the authority that issued the certificate to be validated.

4.9.7. Frequency of CRL issuance

The root CA of the AC Abogacía certification hierarchy will issue a CRL (ARL) each time the certificate of a CA in the hierarchy is revoked. In any case, it will issue a CRL (ARL) with a minimum frequency of three years.

ACA SubCAs shall issue a CRL whenever there is a change in the status of a certificate in their hierarchy.

In particular, a new CRL will be issued immediately after a change in the status of a certificate occurs.

The CA will maintain a history of CRl's and ARl's issued.

Finally, the Certification Authority of the Spanish Bar (AC ABOGACÍA), as a qualified trust service provider that issues qualified certificates, will provide any user party information on the validity or revocation status of qualified certificates issued by it. This information shall be available at least for each certificate at any time and beyond the validity period of the certificate in an automated form that is reliable, free of charge and efficient through the OCSP http://ocsp.redabogacia.org

4.9.8. Maximum latency time for CRLs

The publication of the CRLs will be immediate upon issuance.

4.9.9. Availability of certificate status checking services

The CA provides an on-line revocation checking service, which will be available 24 hours a day, 7 days a week. The CA will make every effort to ensure that the service is never continuously unavailable for more than 24 hours.

The user who does not use the certificate validation systems enabled for this purpose to check the validity of a certificate must consult the Certificate Register to trust it.

4.9.10. Requirements for checking the status of the certificates

No stipulation.

4.9.11. Other forms of revocation information disclosure available

No stipulation.

4.9.12. Special requirements for revocation due to key compromise

In the case of compromise of the CA keys, the qualified trust service provider shall, without undue delay but in any event within 24 hours of becoming aware of the security incident, notify the supervisory body and, where appropriate, other relevant bodies such as the national information security authority, or the data protection authority, of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data concerned.

Where the breach of security or loss of integrity may be directed against a natural or legal person to whom the trust service has been provided, the trust service provider shall also notify the natural or legal person, without undue delay, of the breach of security or loss of integrity.

4.9.13. Causes for suspension of a certificate

Suspension, unlike revocation, involves the temporary loss of validity of a certificate, and is reversible.

The suspension period shall be clearly indicated in the certificate database and the suspension status shall be visible, during the suspension period, from the service providing the certificate status information.

The decision to revoke or not a suspended certificate will be taken by the RA or CA within a maximum period of 30 calendar days. During this time the certificate remains suspended.

AC Abogacía decides on the status after the suspension of the certificate (active, if the request does not proceed or definitively revoked) based on the information obtained up to that moment regarding the causes given for the revocation request.

If the RA or CA to which the revocation request is addressed does not have all the information necessary to determine the revocation of a certificate, but has indications of its compromise, it may decide to suspend it.

The CA or RA may suspend a certificate if the compromise of a key is suspected, until this fact is confirmed or denied.

Suspended certificates are listed in the CRL with revocation cause "Certificate Hold (6)" (RFC 5280).

4.9.14. Who can request the suspension

They may request the suspension of a certificate:

- The authorized operators of the subscriber's RA provided that they have reasonable grounds and as a preventive measure
- The Authorized Administrators of the CA whenever there is good reason to do so and as a preventive measure.

4.9.15. Suspension request procedure

The Subscriber will go to an RA Operator and request that the suspension be requested as a precautionary measure and for a limited period of time.

A third party who contacts, by telephone or in person, an authorized ACA operator may request the suspension of a certificate, the Operator will ask a series of questions to ensure the legitimacy of the suspension and will proceed to suspend it and contact the subscriber of the Certificate to act accordingly.

At the time the certificate is suspended, the subscriber shall be notified, stating the reasons, date and time when the certificate will be terminated. It shall also indicate its maximum duration, and the validity of the certificate shall expire if the suspension has not been lifted after this period has elapsed.

4.9.16. Limits of the suspension period

The maximum period of suspension of a certificate is 30 calendar days.

4.10.Certificate status checking services

The ACA will make information regarding the status of its certificates available through the OCSP service.

Information on the suspension or revocation of certificates will also be provided through the periodic publication of the corresponding CRLs.

4.11.Termination of subscription

The end of the service subscription will be understood as the end of the validity period of the certificate or when the certificate is revoked

4.12.Custody and key recovery

AC Abogacía does not keep any private key of the users so they cannot be recovered in any case.

5. Physical, Procedural and Personnel Security Controls

5.1. Physical Security Controls

The CA has established physical and environmental security controls to protect the resources of the facilities where the systems and equipment used for operations are located.

The physical and environmental security policy applicable to certificate generation services provides protection against:

- ✓ Unauthorized physical access
- ✓ Natural disasters
- ✓ Fires
- ✓ Failure of support systems (power electronics, telecommunications, etc.)
- ✓ Floods
- ✓ Theft
- ✓ Unauthorized removal of equipment, information, media and applications related to components used for the services of the Certification Service Provider

The data center facilities meet TIER III and IV specifications and are equipped with preventive and corrective maintenance systems with 24h-365 days a year assistance with 24-hour assistance following notification.

5.1.1. Location and construction

The data center facilities are located in the Madrid metropolitan area.

5.1.2. Physical access

Physical access to the premises of the Certification Service Provider where certification processes are carried out is limited and protected by a combination of physical and procedural measures.

It is limited to expressly authorized personnel, with identification at the time of access and registration thereof, including CCTV filming and archiving.

The facilities have private security personnel.

Access to the rooms is through badge readers and is managed by a computer system that keeps a log of entrances and exits.

5.1.3. Power supply and air conditioning

The power supply is provided by 3 independent inputs, 2 electrical inputs are used directly to power the Professional Hosting rooms (routers, switches and servers) and the third input powers the air conditioners as well as the lighting of the rooms.

In addition, each electrical input passes through two inverters (UPS) that allow, in case of power failure, to keep the power supply of the facilities in operation while waiting for the genset to start, thus achieving that in case of total power failure to keep all equipment with energy, not producing service failure in case of a total power failure by the power plant.

The data center is equipped with redundant cooling equipment, underfloor air propulsion ensures maximum cooling of the equipment, keeping the room at an ambient temperature between 18 and 25ºC, with a humidity level of 40-60%.

Each rack has an individual air inlet at the bottom of the rack to allow air to flow inside the rack to the top. The room has general air outlets to regulate the overall temperature of the entire room.

5.1.4. Water exposure

The AC facilities are located in a low flood risk zone.

5.1.5. Fire protection and prevention

The data center has a gas fire detection and extinguishing system as a first barrier against fire. The gases used are FM-200 or CEA. If any of the sensors detects a possible fire, the fire prevention system is automatically activated and empties for a few moments all the oxygen in the room where the alert has occurred.

As additional fire protection, the Smoke Early Smoke Detection Alarm System (VESDA) is used. In the event of fire detection, this system immediately informs data center personnel of the presence of smoke so that they can act accordingly.

5.1.6. Storage system.

A cloud storage system with data redundancy in different geographic regions is available.

5.1.7. Waste disposal

When it is no longer useful, sensitive information is destroyed in the manner most appropriate to the medium containing it.

Printed matter and paper: by means of shredders or in garbage cans provided for this purpose, to be destroyed later, under control.

Storage media: before being discarded or reused, they must be processed for erasure, physically destroyed or the information contained therein rendered unreadable.

5.1.8. External backup

The CA has data backup in the cloud with data redundancy in different geographic regions

5.2. Procedural controls

5.2.1. Roles of trust

The roles of trust are those described in the respective Certification Policies of the hierarchy so as to ensure a segregation of duties that disseminates control and limits internal fraud, not allowing a single person to control from start to finish all certification functions.

As specified in CEN CWA 14167-1, the minimum roles established are:

- ✓ **Security Officer:** Maintains overall responsibility for the administration and implementation of security policies and procedures
- ✓ **Certification System Administrators (System Administrators):** Authorized to make changes to the system configuration, but without access to system data.
- ✓ **System Operators (System Operator):** Responsible for the day-to-day management of the system (Monitoring, backup, recovery,...)
- ✓ **Internal Auditor (System Auditor):** Authorized to access the system logs and verify the procedures performed on the system.
- ✓ **CA Operator - Certification Operator:** Responsible for activating CA keys in the Online environment.
- ✓ **RA Operator (Registration Officer)**: Responsible for approving, issuing, suspending and revoking Final Entity certificates

5.2.2. Number of people required per task

The CA guarantees at least two people to perform the tasks that require multi-person control and are detailed below:

The following tasks will require only one authorized person.

- Review of logs except for those of the CA
- Restarting services except for AC services
- Viewing CCTV recordings

The following tasks will require at least dual control by reliable persons:

- Activation of the CA's private key for the issuance of CA certificates
- Activation of the CA's private key for changing or creating new certification profiles
- Activation of the private key of root CAs for the issuance of ARLs

- Review of CA logs.
- Installation or update of certification software
- Configuration of certification software

The following tasks will require at least a control of three or more reliable persons:

- CA key generation.
- The recovery of the CA's private key back-up.
- The generation of new Operator's Card Sets
- The elimination of a set of Operator Cards

5.2.3. Identification and authentication for each role

The persons assigned to each role are identified by the internal auditor who will ensure that each person performs the operations for which he/she is assigned.

Each person only controls the assets necessary for his role, thus ensuring that no one person accesses unallocated resources.

Access to resources is provided depending on the asset by login/password, digital certificates, physical access cards and keys

5.2.4. Roles requiring task separation

With a definition of functions in Roles of Trust and separation of duties, control is spread and internal fraud is limited, not allowing a single person to control all certification functions from start to finish.

Specifically, the following task separations between roles are defined:

The tasks of Auditor are incompatible in time with the tasks of Certification and incompatible with Systems.

Persons involved in Systems Administration may not perform any activity in the Audit or Certification tasks.

5.3. Personnel security controls

5.3.1. Background, qualification, experience, and accreditation requirements

All personnel who perform tasks qualified as reliable have been working at the production center for at least four months.

All personnel are qualified and properly instructed to perform the operations assigned to them.

The CA ensures that the registration personnel are reliable personnel from a College or the body delegated to perform the registration tasks. For this purpose, a declaration to that effect is required from the Entity assuming RA functions.

The registration clerk will have taken a training course to prepare him/her to perform the tasks of registration and validation of requests. At the end of the course, an external auditor will evaluate your knowledge of the process.

In general, the CA will remove an employee from his or her functions of trust when it becomes aware of the existence of a criminal act that could affect the performance of these functions.

The CA shall also employ staff and, where appropriate, subcontractors, who possess the necessary expertise, reliability, experience and qualifications and who have received appropriate training in security and personal data protection rules and who apply administrative and management procedures that correspond to European or international standards.

5.3.2. Background check procedures

The CA conducts appropriate investigations prior to the hiring of any individual. The CA never assigns reliable tasks to personnel with less than four months seniority. The RAs may establish different criteria, provided that they request it and the CA approves it after studying the case.

5.3.3. Training requirements

The personnel in charge of trust tasks have been trained in accordance with the terms established in the hierarchy's Certification policy.

5.3.4. Requirements and frequency of training updates

The employees of the CA and the RAs take the necessary refresher courses to ensure the correct performance of certification tasks, especially when substantial modifications are made to them and at least once a year.

5.3.5. Frequency and sequence of task rotation

Not stipulated.

5.3.6. Penalties for unauthorized actions

The CA and the CSPs have an internal sanctioning regime for unauthorized actions.

5.3.7. Recruitment requirements

Employees hired to perform reliable tasks must previously sign the confidentiality clauses and operational requirements used by the CA. Any action that compromises the safety of accepted critical processes may result in sanctions.

5.3.8. Documentation provided to personnel

The CA shall make available to all personnel the documentation detailing the functions entrusted to them, the policies and practices governing these processes and the security documentation.

In addition, the documentation required by the personnel at all times will be provided, so that they can perform their duties competently.

5.4. Log Audit Procedure

5.4.1. Types of events recorded

AC Abogacía records and saves the logs of all events related to the security system of the AC. These include the following events:

- Switching the system on and off.
- Attempts to create, delete, set passwords or change privileges.
- Login and logout attempts.
- Attempts to gain unauthorized access to the CA system through the network.
- Unauthorized access attempts to the CA's internal network.
- Unauthorized access attempts to the file system.
- Access to logs.
- Changes in system configuration and maintenance.
- Certification Authority application records.
- Switching the AC application on and off.
- Changes in the details of the CA and/or its keys.
- Changes in the creation of certificate profiles.
- Key generation.
- Certificate life cycle events.
- Events associated with the use of the cryptographic module of the CA.
- Records of destruction of media containing keys, activation data.

Additionally, the CA retains, either manually or electronically, the following information:

- CA key creation ceremonies and key management databases.
- Maintenance and system configuration changes.
- Changes in the personnel performing trust tasks in the CA.

- Records of the destruction of material containing password information, activation data or personal subscriber information, if such information is managed.
- Possession of activation data, for operations with the private key of the CAs.

5.4.2. Frequency of audit log processing

Audit logs shall be reviewed periodically and in any case when a system alert occurs due to the existence of an incident, in search of suspicious or unusual activity.

5.4.3. Retention Periods for Audit Logs

Audit log information will be stored for at least 15 years.

5.4.4. Protection of Audit Logs

System logs are protected from tampering by signing the files that contain them.

The devices are operated at all times by authorized personnel.

5.4.5. Audit log backup procedures

The CA has an adequate backup procedure so that, in the event of loss or destruction of relevant files, the corresponding backup copies of the logs are available within a short period of time.

The CA has implemented a secure back-up procedure for audit logs, making a copy of all logs on a daily basis.

Additionally, copies of audit logs are kept in different geographic regions.

5.4.6. Audit information collection system

Event audit information is collected internally and automated by the operating system and certification software.

5.4.7. Notification to the subject causing the event

Not stipulated.

5.4.8. Vulnerability analysis

The CA will perform periodic vulnerability scans on its systems, record the tests and prepare reports of the results obtained.

5.5. Archive of records

5.5.1. Type of events recorded

Events occurring during the life cycle of the certificate, including renewal of the certificate, shall be retained. It will be stored by the CA or, by delegation of the CA to the RA:

- all audit data
- all data relating to the certificates, including contracts with subscribers and data relating to their identification
- requests for issuance and revocation of certificates
- all certificates issued or published
- CRL's issued, responses from online validation methods, or records of the status of the certificates generated
- the documentation required by the auditors
- communications between PKI elements
- events related to the time synchronization of the systems.

The CA is responsible for the proper archiving of all such material and documentation.

5.5.2. Retention period for the file

All system data relating to the life cycle of the certificates shall be retained for the period established by the legislation in force when applicable. Certificates shall be kept published in the repository for at least one year after their expiration.

Contracts with subscribers and any information relating to subscriber identification and authentication will be retained for at least 15 years or the period established by applicable law.

The CA shall also record and keep accessible for an appropriate period of time, even when the activities of the qualified trust service provider have ceased, all relevant information concerning the data issued and received by the qualified trust service provider, in particular in order to serve as evidence in legal proceedings and to ensure continuity of service. This registration activity may be carried out by electronic means.

5.5.3. File protection

The CA ensures the correct protection of the files by assigning qualified personnel for their treatment and the duplication of files in different geographical regions.

The CA has technical and configuration documents detailing all actions taken to ensure file protection.

5.5.4. Archive backup procedures

The backup of the files is performed according to the technical instructions and backup procedure established by the CA in compliance with this CPS.

5.5.5. Requirements for time stamping of records

A time server based on the NTP protocol is available to keep the different elements that make up the reliable certification systems synchronized.

The synchronization server of the AC server is time.windows.com

5.5.6. Record collection system

Not stipulated.

5.5.7. Procedures for obtaining and verifying archived information

During the audit required by this Certification Practice Statement (CPS), the auditor shall verify the integrity of the information filed.

Access to archived information is granted only to authorized personnel.

The CA will provide the information and means to the auditor to be able to verify the information filed.

5.6. Change of password

The change of user passwords is done by performing a new issuance process.

5.7. Recovery in the event of a key compromise or disaster

5.7.1. Incident management and recovery procedures

The CA has developed a contingency plan and incident management procedure to recover all systems within a maximum of five days, although revocation and publication of certificate status information is assured in less than 24 hours.

Any failure to achieve the goals set by this contingency plan shall be treated as reasonably unavoidable unless such failure is due to a breach of the CA's obligations to implement such processes.

5.7.2. Corruption of resources, applications or data

As stipulated in point 5.7.1 Incident Management and Recovery Procedure.

5.7.3. The key of an entity is committed

The CA contingency plan treats the compromise of the CA private key as a disaster. In case of compromise of the CA key, the CA:

- It shall inform all subscribers, users and other CA's with which it has agreements or other types of relationship of the commitment, at least by publishing a notice on the CA's website.
- It will indicate that certificates and revocation status information signed using this key are invalid.
- Without undue delay but in any event within 24 hours of becoming aware of the security incident, notify the supervisory body and, where appropriate, other relevant bodies such as the national information security authority, or the data protection authority, of any breach of security or loss of integrity that has a significant impact on the trust service provided or the personal data concerned.

5.7.4. Business continuity after a disaster

The CA will re-establish critical services (Revocation and publication of revoked) in accordance with this Certification Practice Statement (CPS) within 24 hours of a disaster or unforeseen emergency based on the existing contingency and business continuity plan.

5.8. Termination of service

Prior to the cessation of its activity, the CA will carry out the following actions:

- Inform the supervisory body of any change in the provision of qualified trust services, and of its intention to cease such activities;
- Carry out its cessation plan to ensure continuity of service in accordance with Regulation 910/2014 (eIDAs).
- It will provide the necessary funds (through liability insurance) to continue the completion of the revocation activities until the definitive cessation of the activity, if applicable.
- It shall inform all subscribers, applicants, users, other CA's or entities with which it has agreements or any other type of relationship of the termination at least 2 months in advance, or the period established by the legislation in force. This information will be made available to other trusted third parties through official communication channels and at least through the website of the General Council of Spanish Lawyers (Consejo General de la Abogacía Española)
- It shall revoke any authorization to subcontracted entities to act on behalf of the CA in the certificate issuance procedure.
- In accordance with Article 9.3c of Law 6/2020, of November 11, regulating certain aspects of electronic trust services, the CA may transfer, with the express consent of the subscribers, the management of the certificates that are still valid on the date on which the termination occurs to another certification services provider that assumes them

or, otherwise, to terminate its validity. The CA shall inform, where applicable, on the characteristics of the provider to which the transfer of certificate management is proposed.

- It shall inform the competent administration, with the indicated advance notice, of the cessation of its activity and the destination to be given to the certificates, specifying, if applicable, whether management is to be transferred and to whom.
- Prior to the definitive termination of the activity, it shall communicate to the competent administration the information related to the recognized certificates issued to the public whose validity has been terminated so that the latter may take custody of them for the purposes of the provisions of the ReIDAS and Article 9.3c of Law 6/2020, of November 11, regulating certain aspects of electronic trust services,

6. Technical Safety Controls

The Certification Authority of the Bar uses reliable hardware, software and processes, to form a system that ensures the integrity, confidentiality and availability of information and certification processes.

6.1. Key pair generation and installation

6.1.1. Key pair generation

The generation of the CA's key is performed, according to the documented key ceremony process, within the cryptographic room of the PSC, by appropriate personnel according to the roles of trust and, at least with dual control and witnesses from the CA holder organization and the external auditor.

The key generation of the delegated CA's is performed on a device that complies with the following requirements
requirements detailed in FIPS 140-2, 3. and CC EAL4+

Keys are generated using the RSA public key algorithm.

CA keys have a minimum length of 4096 bits.

In the Member and Administrative Staff Policies, subscriber and operator keys are self-generated in a secure manner using a CC EAL4+, FIPS 140-2 level 3, ITSEC High4 or equivalent cryptographic device.

The SSCD device has been evaluated according to the Protection Profile - Secure Signature Creation Device Type 3, version 1.05, in accordance with CC, version 3.1 révision 3, up to an Evaluation Assurance Level EAL 4 enhanced with AVA_VAN.5.

User keys are generated using the RSA public key algorithm, with appropriate parameters. The keys have a minimum length of 2048 bits.

6.1.2. Delivery of the private key to the subscriber

As provided in each Certification Policy.

6.1.3. Delivery of the public key to the certificate issuer

The public key is sent to the CA for certificate generation using a standard format, preferably in PKCS#10 or X509 self-signed format, using a secure channel for transmission.

6.1.4. CA Public Key Delivery to Users

The certificate of the CAs in the certification chain and their fingerprint will be available to users at http://www.acabogacia.org.

6.1.5. Key size

ACA uses keys based on the RSA algorithm with a length of 4096 bits in CA certificates.

6.1.6. Public key generation parameters

The public keys of the Root CA, Subordinate CAs and signers' certificates are encrypted in accordance with RFC 5280 and PKCS#1. The key generation algorithm is RSA.

Quality verification in both cases is performed according to the technical specification ETSI TS 102 176. The signature algorithms and parameters used by the Cas and the signature certificates are as follows.

- RSA Signature Algorithm
- Key size = minimum 4,096
- Key generation algorithm: rsagen1
- Filling method: emsa-pkcs1-v1_5
- Summary cryptographic functions: SHA-256

6.1.7. Purposes of the use of the key

The certificates include the Key Usage and Extended Key Usage extension, indicating the enabled uses of the Keys

6.2. Private key protection and cryptographic module controls

6.2.1. cryptographic module standards and controls

The cryptographic modules used in the issuing CA to end entities are FIPS-140-2 level 3 and/or CCEAL4+ approved

Cryptographic device storage:

In order to prevent unauthorized manipulation of the cryptographic module, it is located in a secure place with the following characteristics:

- There is an inventory with the control of handling, entry and exit of the device
- Access to the device is limited to trusted personnel.
- All failed accesses are recorded in a log of the system that manages the device
- There is a procedure for managing incidents and abnormal events in the use of the device, proceeding to a subsequent investigation and the issuance of an incident report.
- The correct functioning of the hardware is checked by means of the test procedures offered by the manufacturer at least on a weekly basis.
- Manipulation of the cryptographic device is performed in the presence of at least two reliable employees

- The cryptographic device is protected with tamper detection mechanisms.

Installation of the cryptographic device:

The installation of the cryptographic device is performed in the presence of at least two reliable employees.

Repair of the cryptographic device:

The cryptographic device will be repaired under the conditions stipulated in the maintenance contracts in force with the original supplier of the device. The initial test and operation control procedures will be executed once the device is recovered.

A device in a test environment will never be used in a production environment unless it is initialized in such a way that its state is identical to what it would be if it were received new.

Withdrawal of a cryptographic device:

The removal of the cryptographic device is performed in the presence of at least two reliable employees.

If the device is to be permanently removed the tamper control mechanisms will be destroyed. The device will be stored in a protected place until its destruction.

Reuse of a cryptographic device:

A cryptographic device may be reused as long as it is ensured that it is initialized in such a way that its state is identical to that which it would have had if it were received new.

6.2.2. Control by more than one person (n of m) over the private key'

The access and activation of the private keys of the CAs requires the simultaneous competition of two cryptographic devices controlled by different people out of a possible five, protected by an access key. Additionally, physical access to the devices requires the presence of a third party.

6.2.3. Custody of the private key

In no case will the CA store the subscriber's or the CA's private key in the so-called key escrow mode.

6.2.4. Private key backup

There is a back up that allows the recovery of the CA keys in case of destruction or disabling of the HSM, this is recovered only by authorized personnel according to the trusted roles, using at least a control of three trusted persons.

Back-up copies of the CA's private key signature are securely stored. This procedure is described in detail in the CA safety documentation.

6.2.5. Private key file

The CA will not archive the private key of Certificate Signing and CRLs after the expiration of the validity period of the same.

6.2.6. Private key transfer into or out of the cryptographic module

Private keys are generated directly in the cryptographic modules as prototyped in the key generation document and following the manufacturer's specifications.

The private key can be transferred between the same type of cryptographic module following the manufacturer's instructions.

6.2.7. Storage of the private key in cryptographic module.

According to manufacturer's specifications

6.2.8. Private key activation method

CA keys are activated by an m of n process.

The subscriber's private key is activated by entering the PIN in the secure signature creation device.

6.2.9. Private key deactivation method

As provided in the Certification Policies.

6.2.10. Private key destruction method

The CA's private keys will be destroyed according to the procedures enabled by the HSM for this purpose.

6.2.11. Evaluation of the cryptographic module

Not stipulated

6.3. Other aspects of key pair management

6.3.1. Public key file

The CA shall keep all public keys for the period required by the legislation in force, when applicable, or as long as the certification service is active and at least 6 months more, otherwise.

6.3.2. Period of use for public and private keys

The period of use of a certificate will be determined by the temporary validity of the certificate

6.4. Activation data

6.4.1. Generation and installation of activation data

The qualified electronic signature creation device uses an activation key to access the private keys.

The secure signature creation devices (card) have a factory built-in key activation system by means of a transport PIN that must be modified by the subscriber at the time of physical delivery of the card.

6.4.2. Activation data protection

In the event that the device is not delivered in person to the RA, the activation data will be delivered through a process that ensures its confidentiality to third parties. In no case, the RAs shall keep the activation data of the qualified device for the creation of electronic signatures.

6.4.3. Other aspects of activation data

Not specified

6.5. Computer security controls

The CA uses reliable systems and products that are protected against any alteration and that guarantee the technical safety and reliability of the processes they support.

The equipment used is initially configured with the appropriate security profiles by the systems personnel in the following aspects:

Operating system security settings. Application

security configuration.

Correct sizing of the system.

Configuration of Users and permissions.

Configuration of log events.

Backup and recovery plan.

Network traffic requirements.

The CA's technical and configuration documentation details the architecture of the equipment offering the certification service, both in terms of physical and logical security.

6.5.1. Specific IT security technical requirements

Each CA server includes the following functionalities:

- ✓ access control to CA services and privilege management.

- ✓ enforcing segregation of duties for privilege management.
- ✓ identification and authentication of roles associated with identities.
- ✓ subscriber and CA history file and audit data.
- ✓ auditing of security-related events.
- ✓ self-diagnosis of safety related to CA services.
- ✓ Key recovery mechanisms and the CA system.

The above functionalities are provided through a combination of operating system, PKI software, physical protection and procedures.

6.5.2. Computer security assessment

The security of the equipment is reflected by an initial risk analysis so that the security measures implemented are a response to the probability and impact produced when a group of defined threats can take advantage of security breaches.

Physical security is guaranteed by the facilities already defined above and personnel management.

6.6. Life cycle of cryptographic devices

6.6.1. System development controls

The CA has a procedure for controlling changes in the versions of operating systems and applications that involve an improvement in their security functions or that correct any vulnerability detected.

6.6.2. Security management controls

6.6.2.1. Security management

The CA develops the necessary activities for the training and awareness of employees in safety matters. Training materials and process descriptions are updated after approval by a safety management forum.

The CA requires by contract the equivalent security measures to any external supplier involved in certification work.

6.6.2.2. Classification and management of information and assets

The CA maintains an inventory of assets and documentation and a procedure for the management of this material to ensure its use.

The CA's security policy details the information management procedures where information is classified according to its level of confidentiality.

The documents are catalogued at three levels: PUBLIC, INTERNAL USE and CONFIDENTIAL.

6.6.2.3. Management operations

The CA has an adequate incident management and response procedure, through the implementation of an alert system and the generation of periodic reports. In the CA security document, the incident management process is developed in detail.

The CA has fireproof safety boxes for the storage of physical media.

The CA has documented all the procedures related to the functions and responsibilities of the personnel involved in the control and handling of elements contained in the certification process.

Treatment of supports and security

All media will be handled securely in accordance with information classification requirements. Media containing sensitive data is securely destroyed if it will not be required again.

System planning

The CA technical department maintains a record of equipment capacities.

In conjunction with the resource control application of each system, a possible resizing can be foreseen.

Incident reporting and response

The CA has a procedure for the follow-up of incidents and their resolution in which the responses and an economic evaluation of the resolution of the incident are recorded.

Operational procedures and responsibilities

The CA defines activities assigned to persons with a role of trust other than the persons in charge of day-to-day operations that are not confidential.

6.6.2.4. Access system management

The CA makes every reasonable effort to confirm that system access is limited to authorized persons. In particular:

AC General

a) High-availability firewall-based controls are available.

b) Sensitive data is protected by cryptographic techniques or access controls with strong identification.

c) The CA has a documented procedure for managing user registrations and cancellations and an access policy detailed in its security policy.

d) The CA has a procedure to ensure that operations are carried out in compliance with the role policy.

e) Each person has an associated identifier to perform certification operations according to his or her role.

f) CA personnel will be held accountable for their actions, e.g., for withholding event logs.

Certificate generation

The CA facilities are equipped with continuous monitoring systems and alarms to detect, record and be able to act immediately in the event of an unauthorized and/or irregular access attempt to its resources.

Authentication for the issuance process is performed by a system m of n operators for the activation of the CA's private key.

Revocation management

The CA facilities are equipped with continuous monitoring systems and alarms to detect, record and be able to act immediately in the event of an unauthorized and/or irregular attempt to access its resources and/or the revocation system.

Revocation refers to the permanent loss of effectiveness of a digital certificate. The log systems will generate the evidence that guarantees the non-repudiation of the action performed by the CA operator.

Revocation status

The revocation status application has an access control based on certificate authentication to prevent attempts to modify revocation status information.

6.6.2.5. Cryptographic hardware lifecycle management

The CA ensures that the cryptographic hardware used for signing certificates is not tampered with during transport.

The cryptographic hardware is built on supports prepared to prevent any tampering.

The CA records all pertinent device information to add to the lender's asset catalog.

The use of cryptographic certificate signing hardware requires the use of at least two trusted employees.

The CA performs periodic test runs to ensure correct operation of the device. The cryptographic

device is only manipulated by reliable personnel.

The CA's private signing key stored in the cryptographic hardware will be deleted once the device has been removed.

The configuration of the CA system as well as its modifications and updates are documented and controlled.

The CA has a maintenance contract for the device for its proper maintenance. Changes or updates are authorized by the security manager and are reflected in the corresponding work minutes. These configurations shall be performed by at least two reliable persons.

6.6.3. Life cycle safety level assessment

AC Abogacía evaluates the level of security through audits.

6.7. Network security controls

The CA protects physical access to network management devices and has an architecture that sorts the generated traffic based on its security characteristics by creating clearly defined network sections. This division is made through the use of firewalls.

Confidential information transferred over unsecured networks is encrypted.

6.8. Time stamping

Not stipulated

7. Certificate and CRL and OCSP Profiles

7.1. Certificate Profile

All certificates issued under this policy are in compliance with the X.509 version 3 standard, RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", ETSI TS 101 862 known as "European profile for Qualified Certificates" and RFC 3039 (superseded) and 3739 "Qualified Certificates Profile". The 319 412 family has also been taken into account in relation to certificate profiles. The size of the fields can be larger than those established in RFC 5280.

The content of the qualified certificates is in accordance with Article 28 of Regulation 910/2014 (ReIDAS).

Clarifications on the "x509v3 KeyUsage" extension:

RFC 5280, which defines X509 certificate profiles, replaces RFC 2459 and RFC 3280 due to obsolescence. An important change is that the use of the "digital signature" key as defined in RFC 5280 does not declare such use as that appropriate to digital signatures for security services other than "non-repudiation", as expressed in the corresponding clause in RFC 2459.

Consistent with the old RFC 2459, RFC 3039 required that if the usage defined as "non-repudiation" was present, it did so exclusively as opposed to any other usage. The above change generated a request to the ITU to correct the error and harmonize RFC 3039 with the updated RFC 3280 and later RFC 5280.

RFC 3739 "Qualified Certificates Profile" (March 2004, replaces RFC 3039) does not state in the corresponding section on the use of "non-repudiation", referring to the policies of the PSC or to specific legal requirements applicable to the scope of issuance, and making a consideration of the possible risks of combining the use of "non-repudiation" with others.

On the other hand, the non-repudiation functionality is achieved by the application of the digital signature mechanism to the data to be signed, and by the existence of a non-repudiation service or application. This service will require the existence of the Key Usage "non-repudiation" in the signatory's certificate, as well as the application of additional mechanisms (such as time stamps issued by a Time Stamping Authority, OCSP validation, etc.), according to the technical standards.

The certificates will have the content and fields described in each Certification Policy. The data related to the certificates of Root CAs and Subordinate CAs are found in section 1.3.1 Certification Authority

7.1.1. Version number

The CA issues X.509 Version 3 certificates.

7.1.2. Certificate extensions

As provided in each Certification Policy.

7.1.3. Object Identifiers (OID) of the algorithms

The object identifier of the signature algorithm is 1. 2. 840. 113549. 1. 1. 11 SHA-256 with RSA Encryption

The object identifier of the public key algorithm is 1.2.840.113549.1.1.1.1 rsaEncryption

7.1.4. Name format

Not stipulated.

7.1.5. Name restrictions

As provided in each Certification Policy.

7.1.6. Certificate policy object identifier

As provided in each Certification Policy.

7.1.7. Use of extension policy restrictions

The "Policy Constrains" extension of the CA Root Certificate is not defined.

7.1.8. Syntax and semantics of policy qualifiers

The "Certificate Policies" extension includes.

- Policy containing the policy OID
- CPS containing a URL to the policy repository and CPS

7.1.9. Semantic treatment for the extension "Certificate policy"

The "Certificate Policy" extension includes the Policy OID field, which identifies the policy associated to the Certified by ACA

7.2. CRL Profile

The CRL profile corresponds to that proposed in the corresponding certification policies, and to the X.509 version 3 standard of RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile". CRL's are signed by the certification authority that issued the certificates.

7.2.1. Version number

The CRLs issued by the CA are compliant with the X.509 version 2 standard.

7.2.2. CRL and extensions

As provided in each Certification Policy.

7.3. OCSP Profile

The OCSP certificate profile corresponds to that proposed in the corresponding certification policies, and to the X.509 version 3 standard of RFC 6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP". CRL's are signed by the certification authority that issued the certificates.

7.3.1. Version number

OCSP Responder certificates will use the X.509 version 3 (X.509 v3) standard.

7.3.2. OCSP and extensions

The extensions for OCSP used in the certificate profile are:

- Key Usage, marked as mandatory and critical.
- Enhanced Key usage, marked as mandatory only.

8. Compliance audits

8.1. Frequency of audits

An audit is performed on a regular basis. On the other hand, the certification service provider/qualified trust service provider shall be audited, at least every 24 months in compliance with Regulation 910/2014.

Notwithstanding the foregoing, the Provider shall conduct internal audits at its own discretion or at any time, due to a suspected breach of any security measure or due to a key compromise.

8.2. Auditor identification and qualification

Audits in compliance with Regulation 910/2014 are performed by a conformity assessment body and its auditors must comply with the requirements indicated in the European standard ETSI EN 319 403 Electronic Signatures and Infrastructures (ESI);

Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers.

In addition, WebTrust audits can be performed by a top-tier auditing firm, according to WebTrust for Certification Authorities criteria, which can be downloaded and consulted at http://www.aicpa.org , developed by the AICPA (American Institute of Certified Public Accountants, Inc.) and the CICA (Canadian Institute of Chartered Accountants).

The WebTrust Principles and Criteria for CA are consistent with the standards developed by the American National Standards Institute (ANSI) and the Internet Engineering Task Force (IETF)

8.3. Relationship between the auditor and the CA

The auditor shall be a well-known company with departments specialized in computer auditing of recognized prestige, without any conflict of interest that may distort its performance in its relationship with AC Abogacía.

8.4. Topics covered by the audit

The audit verifies the following principles:

- Publication of Information: That the CA makes public the Business and Certificate Management Practices (Policies and Certification Practice Statement (CPS)), as well as the protection of personal data and provides its services in accordance with such statements.
- Service Integrity. That the CA maintains effective controls to reasonably assure that:
    - Subscriber information is properly authenticated (for registration activities performed by the CA).
    - The integrity of the keys and certificates managed and their protection throughout their life cycle.

- General controls. That the CA maintains effective controls to reasonably assure that:
  - Subscriber and user information is restricted to authorized personnel and protected from uses not specified in published CA business practices.
  - Continuity of operations related to key and certificate lifecycle management is maintained.
  - The operation, development and maintenance tasks of the CA's systems are adequately authorized and carried out to maintain the integrity of the systems.
- As well as the audit criteria listed in the European standard ETSI EN 319 403 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers.

Audit in the Registration Authorities. All Registration Authorities may be audited prior to their effective start-up. In addition, periodic audits may be carried out to verify compliance with the requirements of the certification policies for the development of the registration tasks set forth in the signed service contract.

8.5. Incident resolution

In the event that incidents or non-conformities are detected, the appropriate measures will be implemented to resolve them as soon as possible.

8.6. Communication of results

In any case, the qualified trust service provider shall, without undue delay but in any event within 24 hours of becoming aware of the security incidents, notify the supervisory body and, where appropriate, other relevant bodies such as the national information security authority, or the data protection authority, of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data concerned.

Where the breach of security or loss of integrity may be directed against a natural or legal person to whom the trust service has been provided, the trust service provider shall also notify the natural or legal person, without undue delay, of the breach of security or loss of integrity.

9. Other legal and operational issues

9.1. Rates

9.1.1. Certificate issuance and renewal fees

The prices of certification services or any other related services will be available to users at the different Registration Authorities.

9.1.2. Certificate access fees

Access to the issued certificates shall be free of charge, however, the CA may impose a fee for cases of massive downloading of certificates or any other circumstance that in the CA's opinion should be charged, in which case such fees shall be published on the CA's website.

9.1.3. Fees for access to information regarding the status of certificates or revoked certificates

The CA shall provide any user party with information on the validity or revocation status of qualified certificates issued by them. This information is available at least for each certificate at any time and beyond the validity period of the certificate in an automated form that is reliable, free of charge and efficient.

9.1.4. Fees for other services

Fees applicable to other services will be published on the CA website.

9.1.5. Refund policy

No stipulation.

9.2. Financial responsibility

The CA, in its activity as a qualified provider of trust services, maintains sufficient economic resources to face the risk of liability for damages to the users of its services and to third parties, guaranteeing its responsibilities in its activity as a Provider as established in the applicable legislation.

9.2.1. Insurance coverage

Specifically, the guarantee mentioned in the preceding paragraph is established by means of an insurance policy
Civil Liability with coverage equal to or greater than 3,000,000 €.

9.2.2. Other assets

Not stipulated

9.2.3. Insurance or guarantee coverage for end entities

Not stipulated

9.3. Confidentiality of business information

The General Council of the Spanish Bar is Responsible for the processing of the data of the Certification Authority of the Advocacy (the CA), and complies with data protection regulations specifically with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter the General Data Protection Regulation) and the Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights (hereinafter the LOPD-GDD),

The CA has an adequate information treatment policy and model agreements to be signed by all persons having access to confidential information.

9.3.1. Type of information to be kept confidential

The CA shall consider confidential all information that is not expressly classified as public. Information declared as confidential is not disseminated without the express written consent of the entity or organization that has granted it the confidentiality status, unless there is a legal requirement.

9.3.2. Type of information considered non-confidential

The following information will be considered non-confidential:

- That contained in this Policy and in the Certification Practices.
- The information contained in the certificates, since for their issuance the subscriber previously grants his consent, including but not limited to
    - Certificates issued or in the process of being issued.
    - The binding of the subscriber to a certificate issued by the Certification Service Provider / Qualified Trust Service Provider.
    - The name, surname and national identity card number of the certificate subscriber, in the case of individual certificates, as well as any other circumstance or personal data of the holder, in the event that it is significant in terms of the purpose of the certificate.
    - The e-mail address of the certificate subscriber, in the case of individual certificates, or of the key holder, in the case of group certificates, or the e-mail address of the certificate subscriber, in the case of individual certificates, or of the key holder, in the case of group certificates

e-mail address assigned by the subscriber, in case of device certificates.

- The uses and economic limits outlined in the certificate.
- The period of validity of the certificate, as well as the date of issuance of the certificate and the expiration date.
- The serial number of the certificate.
- The different statuses or situations of the certificate and the start date of each one of them, specifically: pending generation and/or delivery, valid, revoked, suspended or expired and the reason for the change of status.

- Certificate Revocation Lists (CRL's), as well as other certificate status information, can be used to revocation.
- The information contained in the certificate deposits.
- Any information whose disclosure is required by law.

9.3.3. Responsibility to protect confidential information

ACA and its Registration Authorities shall have the obligation to protect all information considered confidential

The certificates will be published in accordance with the provisions of Article 9.2 of Law 6/2020, of November 11, regulating certain aspects of electronic trust services.

9.4. Protection of personal data

9.4.1. Personal data protection policy

The General Council of the Spanish Bar is Responsible for the processing of the data of the Certification Authority of the Advocacy (the CA), and complies with data protection regulations specifically with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter the General Data Protection Regulation) and the Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights (hereinafter the LOPD-GDD),

Identity and contact details of ACA's Data Controller

General Council of Spanish Lawyers

Address: Paseo de Recoletos, 13, 28004 - Madrid.

Contact telephone number: 915232593

E-mail address: informacion@abogacia.es

Contact details of the data protection delegate

Paseo de Recoletos, 13. 28004- Madrid.

informacion@abogacia.es

The data contained in the directory of certificates that are considered personal data for the purposes of the provisions of the General Data Protection Regulation.

9.4.2. Personal information treated as private

Any information of a personal nature that is not contained in the following section will be considered personal information and will be treated as private.

9.4.3. Personal information treated as public

The following information will be considered public:

- That contained in this Policy and in the Certification Practices.
- The information contained in the certificates, since for their issuance the subscriber previously grants his consent, including but not limited to:
    - Certificates issued or in the process of being issued.
    - The binding of the subscriber to a certificate issued by the Certification Service Provider/ Qualified Trust Service Provider.
    - The name, surname and national identity card number of the certificate subscriber, in the case of individual certificates, as well as any other circumstance or personal data of the holder, in the event that it is significant in terms of the purpose of the certificate.
    - The e-mail address of the certificate subscriber, in the case of individual certificates, or of the key holder, in the case of group certificates, or the e-mail address assigned by the subscriber, in the case of device certificates.
    - The uses and economic limits outlined in the certificate.
    - The period of validity of the certificate, as well as the date of issuance of the certificate and the expiration date.
    - The serial number of the certificate.
    - The different statuses or situations of the certificate and the start date of each one of them, specifically: pending generation and/or delivery, valid, revoked, suspended or expired and the reason for the change of status.
- Certificate Revocation Lists (CRL's), as well as other certificate status information, can be used to revocation.
- The information contained in the certificate deposits.

9.4.4. Responsibility to protect private information

The CA will consider private all information that is not expressly catalogued as public. No information declared confidential is disseminated without the express written consent of the company

entity or organization that has granted it confidentiality, unless there is a legal requirement to do so.

9.4.5. Notification and consent to the use of private personal data

Without prejudice to other obligations, the Registration Authorities that are established shall verify that the applicant for a certificate gives his consent to the processing of his personal data, after having been informed by the Data Controller of its legitimacy, the purpose for which it is to be used, and the rights to which he is entitled in accordance with Article 13 of the General Data Protection Regulation.

In those cases in which the data have not been collected directly from the interested parties, the CA will expressly, precisely and unequivocally inform them, within three months from the time the data were recorded, of the above paragraph.

9.4.6. Disclosure of information by judicial or administrative order

The information requested by the competent authority shall be provided in the cases and form established by law.

9.4.7. Other circumstances of disclosure

Requested information will be provided when permitted by this Certification Practice Statement (CPS) or the ACA Certification Policies.

9.5. Intellectual property rights

The intellectual property of this Certification Practice Statement (CPS) belongs to the CGAE.

AC Abogacía will be the only entity that will have intellectual property rights over the certificates it issues.

AC Abogacía grants a non-exclusive license to reproduce and distribute certificates, free of charge, provided that the reproduction is complete and does not alter any element of the certificate, and is necessary in connection with digital signatures and/or encryption systems within the scope of this policy, as defined in section 1 and in accordance with the corresponding binding instrument between AC Abogacía and the party reproducing and/or distributing the certificate.

9.6. Liability and Warranties

The Consejo General de la Abogacía Española (CGAE), in its activity of qualified provision of trust services, will be liable for non-compliance with the provisions of the Certification Policies and Practices and, where applicable, with the provisions of Regulation n 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and Law 6/2020, of November 11, regulating certain aspects of electronic trust services

Likewise, the Consejo General de la Abogacía Española shall assume all liability to third parties for the actions of the persons to whom they delegate the execution of any or some of the functions necessary for the provision of certification services.

Notwithstanding the foregoing, the General Council of Spanish Lawyers shall not guarantee the algorithms and cryptographic standards used nor be liable for damages caused by external attacks on them, provided that it has applied due diligence according to the state of the art at all times, and has acted in accordance with the provisions of the Certification Policies and Practices and the ReIDAS Law 6/2020, of November 11, regulating certain aspects of electronic trust services, and its implementing regulations, where applicable.

9.6.1. CA liability and warranties

The CA is bound by the provisions of articles 20 to 24 of ReIDAS and article 9 of Law 6/2020, of November 11, regulating certain aspects of electronic trust services and other regulations on the provision of certification services, as well as the provisions of the Certification Policies and this Certification Practices Statement (CPS). Specifically, the CA is required to:

- Not to store or copy the Subscriber's signature creation data, when required by applicable law.
- Provide the applicant with the following minimum information prior to the issuance of the certificate, which must be transmitted free of charge, in writing or electronically:
    - The signatory's obligations, the way in which the signature creation data must be kept, the procedure for revocation or suspension of its certificate and the electronic signature creation and verification devices compatible with the certificate issued.
    - Mechanisms to ensure the reliability of a document's electronic signature over time.
    - The method used by the CA to verify the identity of the signatory or other data contained in the certificate.
    - The precise conditions of use of the certificate, its limits of use and the way in which the CA guarantees its liability.
    - The certifications obtained by the CA.
    - The applicable procedures for judicial or extrajudicial resolutions.
    - Or any other information contained in this Certification Practice Statement (CPS) or in the Certification Policies.
- Maintain an updated directory of certificates, indicating which certificates have been issued and whether they are current or whether their validity has been suspended or terminated.
- Put in place reasonable security mechanisms to maintain the integrity of the certificate directory
- Ensure the availability of a fast and secure certificate validity query service
- Suspend and revoke certificates according to the provisions of the Certification Practice Statement (CPS) and publish the aforementioned revocations in the certificate validation systems enabled for this purpose.

- Inform Subscribers of the revocation or suspension of their certificates, in a timely manner in accordance with current Spanish legislation.
- Publish the Certification Policies and Practices on the CA website free of charge.
- Inform about the modifications of this Certification Practices Statement to Subscribers, RA's that are linked to it and users, through the publication of these and its modifications on its website.
- Ensure that the date and time at which a certificate was issued, expired or suspended can be determined.
- Employ personnel with the necessary qualifications, knowledge and experience to provide the certification services offered by the CA.
- Use reliable systems for storing qualified certificates to verify their authenticity and prevent unauthorized persons from altering the data, restrict their accessibility in the cases or to the persons indicated by the signatory, and detect any change affecting these security conditions.
- Use reliable systems and products that are protected against tampering and that guarantee the technical and, where appropriate, cryptographic security of the certification processes they support
- Take measures against forgery of certificates and ensure their confidentiality during the generation process and their delivery by a secure procedure to the signatory.
- To have liability insurance that must cover a minimum amount as required by the regulations in force
- Retain the information on the certificate issued for the minimum period required by the regulations in force, when applicable
- Issue certificates in accordance with these Practices and the application standards.
- Protect your private keys securely.
- Issue certificates according to the information in its possession and free of data entry errors.
- Issue certificates whose minimum content is the one defined by current regulations, when applicable.
- Protect, with due care, the signature creation data while it is in their custody if so contemplated.
- Respect the provisions of the Certification Policies and Practices.
- Comply with those requirements of Article 24 (ReIDAS) not mentioned above for qualified trust service providers.

9.6.2. RA liability and warranties

The Registration Authorities are delegated by the CA to perform this task, therefore the RA is also bound by the terms defined in the Certification Practices for the issuance of certificates, mainly:

- Pay the established fees for the certification services requested.
- Respect the provisions of this Certification Practice Statement (CPS).
- Verify the identity of subscribers and certificate applicants.
- Verify the accuracy and authenticity of the information provided by the applicant.
- Archive, for the period stipulated in the legislation in force, the documents provided by the subscriber.
- Respect the provisions of the contracts signed with the CA.
- Respect the provisions of the contracts signed with the Subscriber.
- Inform the CA of the causes of revocation, if and when they become aware of them.
- That the RAs undertake to comply with the general security requirements indicated by the CA.

9.6.3. Liability and warranties of subscribers

The Subscriber of a Certificate shall be obliged to comply with the provisions of the regulations in force and also to:

- Diligently guard your private key.
- Use the certificate as established in this Certification Practice Statement (CPS) and the applicable Certification Policies.
- Respect the provisions of the documents signed with the RA.
- Inform as soon as possible of the existence of any cause for suspension / revocation.
- Notify any change in the data provided for the creation of the certificate during its period of validity.
- Not to use the private key or the certificate from the moment it is requested or warned by the CA or the RA of its suspension or revocation, or once the certificate's validity period has expired.

9.6.4. User liability and warranties

It shall be the obligation of the Users to comply with the provisions of the regulations in force and also:

- Verify the validity of the certificates at the time of performing any operation based on them.
- To know and be subject to the guarantees, limits and responsibilities applicable to the acceptance and use of the certificates on which it relies.
- Verify by its own mechanisms, that the hierarchy with which the certificate is issued is in the list of qualified certificates of the European Union (TSL).

9.6.5. Liability and warranties of other participants

The applicant for a Certificate shall be obliged to comply with the provisions of the regulations in force and also to:

- Provide the RA with the necessary information to make a correct identification.
- Make reasonable efforts to confirm the accuracy and truthfulness of the information provided.
- Notify any change in the data provided for the creation of the certificate during its period of validity.

9.7. Disclaimer of liability

The relationship between the CA and the RAs shall be governed by their special contractual relationship. The CA and the RA's shall be exonerated from their responsibility under the terms established in the Certification Practice Statement (CPS) and the certification policies. In particular, the CA and the RA's shall not be liable in any case when faced with any of these circumstances:

1. For the use of certificates if and when it exceeds the provisions of the current regulations and this Certification Practice Statement (CPS), in particular for the use of a suspended or revoked certificate, or for placing trust in it without previously verifying its status.
2. For the improper or fraudulent use of certificates or certificate validation systems enabled for such purpose.
3. For the improper use of the information contained in the Certificate or in the certificate validation systems enabled for such purpose.
4. Failure to comply with the obligations established for the Subscriber or Users in the current regulations, this Certification Practice Statement (CPS) or in the corresponding Certification Policy.
5. For the content of digitally signed or encrypted messages or documents.
6. Failure to recover documents encrypted with the Subscriber's public key.
7. Fraud in the documentation submitted by the applicant.

9.8. Limit of liability

The General Council of the Spanish Bar, in its activity as Certification Service Provider / Qualified Trust Service Provider, will respond in accordance with the liability regime established by ReIDAS, Law 6/2020, of November 11, regulating certain aspects of electronic trust services, in other regulations on the provision of certification services and other applicable legislation.

The CA shall be liable for the damage caused to the Subscriber or any person who, in good faith, relies on the certificate, provided that on the part of the CA itself there is intent, fault or negligence, with respect to:

1. The accuracy of all information contained in the certificate at the date of issuance.

2. The guarantee that, at the time of delivery of the certificate, the Subscriber holds the private key corresponding to the public key given or identified in the certificate.
3. The guarantee that the public and private key work together and complementarily.
4. Correspondence between the certificate requested and the certificate delivered
5. Any liability established by current legislation

9.9. Indemnifications

Not stipulated

9.10. Period of validity of this document

9.10.1. Deadline

This Certification Practice Statement (CPS) and the different Certification Policies shall become effective upon publication.

9.10.2. Termination

This Certification Practice Statement (CPS) and the different Certification Policies will be repealed at the time a new version of any document is published. The new version will replace the previous document in its entirety. ACA is committed to submitting this Declaration to a periodic review process

9.10.3. Effects of termination

For current certificates issued under a previous Certification Policy and Practices Statement, the new version shall prevail over the previous one in all that does not oppose it.

9.11.Individual notifications and communication with Users

ACA establishes in the binding legal instrument with the subscriber the means and deadlines for notifications.

In general, the Abogacia website, www.abogacia.es will be used for any type of notification and communication.

9.12.Modifications to this document

Modifications to this Certification Practice Statement (CPS) shall be made when there is any relevant technical, legal or procedural change in the activity of the Certification Authority.

In addition, an annual review will be performed independently of the revisions made for changes.

Any element of this Certification Practices Statement (CPS) may be changed unilaterally by AC Abogacía without prior notice. Modifications must be justified from a legal, technical or commercial point of view.

9.12.1. Notification procedure

All proposed changes that may substantially affect the users of this policy will be immediately notified to subscribers through publication on the AC Abogacía website, making express reference on the "home page" of the same to the existence of the change.

Affected users may submit comments to the policy administration organization within 15 days of receiving notification.

Any action taken as a result of comments is at the discretion of the CA.

9.12.2. Elements that can change without notification

The only changes that may be made to this policy without notice are typographical or editorial corrections or changes to contact details.

9.12.3. Circumstances in which the OID will be changed

The OID will be changed in those circumstances in which any of the procedures described in this document are significantly altered.

The OID will be changed whenever it is considered that a new type of certificate is being issued.

9.13. Dispute resolution

Any controversy or conflict arising from this document shall be definitively resolved by means of a mediation process requested to the Mediation Center of the Bar Association or a legal arbitration process by an arbitrator, within the framework of the Spanish Court of Arbitration, in accordance with its Regulations and Statutes, which is entrusted with the administration of the arbitration and the appointment of the arbitrator or arbitral tribunal.

The parties state their commitment to comply with the award to be rendered.

9.14.Applicable legislation

This document specifies the Certification Practices Statement of the Certification Authority constituted by the General Council of the Spanish Bar, called the Certification Authority of the Spanish Bar (AC Abogacía), for the issuance of personal certificates, and is based on the specification of the RCF 3647 standard - *Internet X. 509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework*, of the IETF.

Likewise, for the development of its content, European standards have been taken into account, among which the following are worth mentioning:

- ETSI EN 319 412-5: Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile.
- ETSI EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates.
- ETSI EN 319 412-1: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.
- ETSI EN 319 412-2: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.
- ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- ETSI AT 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

Likewise, it has been considered as the basic regulations applicable to the matter:

- Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (hereinafter ReIDAS) and repealing Directive 1999/93/EC.
- law 6/2020, of November 11, 1920, regulating certain aspects of electronic trust services, in other regulations on the provision of certification services
- Royal Decree-Legislative 1/1996, of April 12, 1996, approving the Revised Text of the Intellectual Property Law.
- Law 39/2015, of October 1, 2015, on the Common Administrative Procedure of Public Administrations
- Royal Decree 311/2022, of May 3, which regulates the National Security Scheme.
- .
- Law 40/2015, of October 1, 2015, on the Legal Regime of the Public Sector.

9.15.Compliance with applicable legislation

In any case, ACA declares compliance with the indicated regulations as well as strict compliance with the Certification Practices Statement (CPS) and each of the Certification Policies.

9.16.Other provisions

Each clause of this Certification Practices Statement is valid in itself and does not invalidate the rest. The invalid or incomplete clause may be replaced by an equivalent clause.

Annex 1: Security Document

PREAMBLE

The Bar Council, is Data Controller of the Bar Certification Authority (the CA) and complies with data protection regulations specifically with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter the General Data Protection Regulation) and the Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights (hereinafter the LOPD-GDD).

The data processing carried out by the Certification Authority of the Bar is included in the Register of Processing Activities of the Bar (RAT) found in the Transparency Portal of the Bar and the security measures implemented correspond to those provided in Annex II (Security Measures) of Royal Decree 311/2022, of May 3, which regulates the National Security Scheme, and are described in the documents that make up the policy of data protection and information security of the General Council of the Bar.

ACA is ENS certified by an accredited entity and will be available to users.

Users (third parties who trust the certificates) can consult the data contained in the certificates as well as the status of validity in the certificate directory, which is publicly accessible according to the provisions of Law 6/2020, of November 11, regulating certain aspects of electronic trust services and other regulations on the provision of certification services. Users may only use the information to verify the validity of the certificate or signatures generated in accordance with current legislation, the Certification Practices Statement (CPS) and the Certification Policies. It should be noted, in general, that any processing, recording or use for purposes other than the above requires the prior consent of the owners of the data.

Users of an ACA certificate have the right to obtain confirmation as to whether or not we are processing personal data concerning them. Likewise and in relation to your personal data you have the right to:

- Access to them.
- Request its rectification or suppression.
- Request the limitation of your treatment.
- Oppose your treatment.
- Request portability in a structured, commonly used, machine-readable format.

You may exercise such rights before the Consejo General de la Abogacía Española. To do so, you must write to the Board at the address indicated above, attaching a copy of your identification document to your request, or sending an e-mail including an electronic signature, in order to prove your identity, to informacion@abogacia.es.

SCOPE OF APPLICATION OF THE SECURITY DOCUMENT

The purpose of this document, an integral part of the Certification Practices Statement (CPS) of AC Abogacía, is to establish the technical and organizational measures required for

guarantee the security that must be met by automated files, premises, equipment, systems and persons involved in the automated processing of personal data.

The Certification Practices Statement (CPS) details the measures, norms, procedures, rules and standards aimed at ensuring the level of security required by the aforementioned Regulation, in order to ensure the security of personal data for which this institution is responsible.

Additionally, the general security measures applicable to any information system in use in the General Council of Spanish Lawyers are established, even if such system is not included among those that directly support the provision of certification services.

The Certification Practice Statement (CPS), of which this Security Document is a part, is mandatory for all personnel of the institution included in section 5.2.1.

TYPE OF PERSONAL DATA USED BY THE CERTIFICATION AUTHORITY

The personal data that constitute the object of processing are the following:

Identification Data:

- Name, Surname and

NIF Contact information:

- E-mail address
- Alternative e-mail address for contact Professional data:
- College or Institution
- Member / Associate No. (where applicable)
- Status with respect to the corporation/entity (where applicable)
- Position, Title or specialty (where applicable)
- Department to which it belongs (where applicable)

Public key digital key certificate data:

- Certificate serial number
- Start and end date of validity
- Public key associated with private key held by user
- Petition and certificate status (Pending Approval, Approved, Valid, Suspended, Revoked).

<u>Description of the treatment system</u>

- The system that supports the provision of certification services is based on centralized servers located in a highly secure data center. The system has local access through controlled workstations located in the secure area of the DPC, and through the Internet.
- The certificate publishing system query operations are adequately protected as described in section 2.6 of this Certification Practice Statement (CPS).

- Registration, modification or deregistration operations by remote operators of Registration Authorities are protected by means of access with a digital certificate managed by an operator card.
- Certification request submission operations by applicants are protected by a pre-submission access password.
- The process is described in chapter 4 of this document.

MEASURES TO ENSURE THE LEVEL OF SECURITY

The security measures implemented correspond to those provided for in Annex II (Security measures) of Royal Decree 311/2022, of May 3, which regulates the National Security Scheme and which are described in the documents that make up the data protection and information security policy of the General Council of Lawyers.

This document has been translated by an automatic translation system. Although it has been reviewed, the correct translation of all terms cannot be guaranteed.
Please contact us if you need any clarification on terminology Contacto - Abogacía Española (abogacia.es)
Original document can be found at Políticas y prácticas de certificación - Abogacía Española (abogacia.es)