Abogacía Española
CONSEJO GENERAL

AUTORIDAD DE CERTIFICACIÓN DE LA ABOGACÍA

Qualified certificates of electronic seal

Certification Policy (CP2_ACATC_009.0)

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
01/10/2010	CP2_ACATC_001.0	Initial version
01/03/2012	CP2_ACATC_002.0	Reference to the LAECSP and recognized certificates is eliminated
13/03/2014	CP2_ACATC_003.0	A description of the PKI Hierarchy is included Details of the Cryptographic module model are eliminated The length of user keys is increased to 2048 bits New CRL distribution points are indicated Correction of erratum
27/06/2016	CP2_ACATC_004.0	New PKI Hierarchy is included, new CAs certificates information Aligned with eIDAS Adaptation of recognized services to qualified
03/05/2017	CP2_ACATC_005.0	KeyUsage is modified to align with ETSI EN 319 412 including non-repudiation, digital signature and key encryption DN serial number is removed
03/05/2017	CP2_ACATC_006.0	RFC 3647 Adequacy All other Operational and Legal issues (item 9) are referred to the PSC
02/07/2020	CP2_ACATC_007.0	The section Authentication of an individual's identity has been updated
31/05/2022	CP2_ACATC_008.0	Change of document template Removal of duplicate sections with CPS Legislative adjustment Law 6/2020 of November 11, 2010 It is indicated in section 3.3.1 that certificates cannot be renewed
21/03/2023	CP2_ACATC_009.0	Annual legislative review

INDEX

Contenido

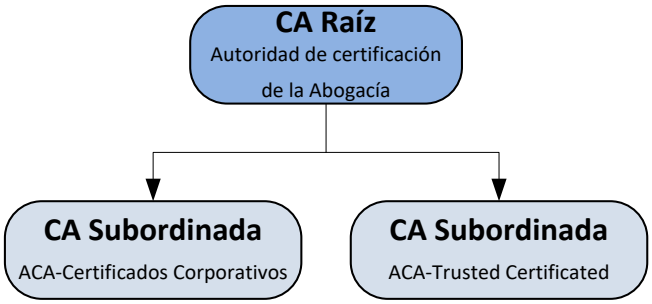
1. Introduction

1.1. Overview

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

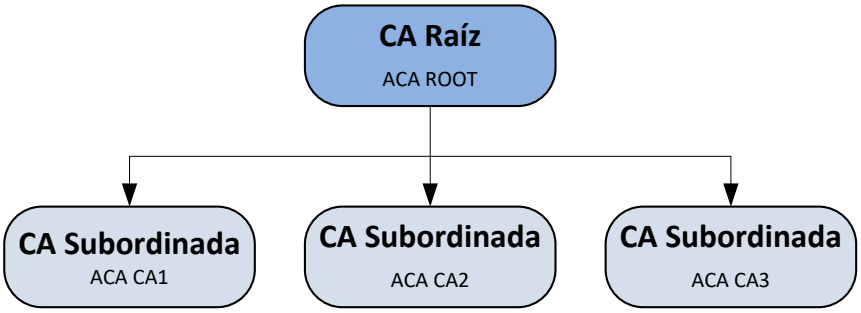


In 2014, new subordinated CAs were generated with the same denomination followed by the year of issue: *ACA - Corporate Certificates 2014 and ACA-Trusted Certificates 2014.*

The certificates issued by both subordinated CAs will 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;



This document specifies the Certification Policy of the digital certificate called "**Qualified Certificate of electronic seal**" issued by the certification authority of the General Council of Spanish Lawyers, or AC Abogacía.

The Consejo General de la Abogacía Española, as the regulatory body for the legal profession, has established its own 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 personnel, organizations and individuals representing such organizations, by Accredited Certification Providers.

This Certification Policy is in compliance with REGULATION (EU) No 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 Regulation 910/2014), Law 6/2020, of 11 November, regulating certain aspects of electronic trust services (hereinafter Law 6/2020) and the other technical standards governing digital identity and qualified signature services, meeting all the technical and security requirements demanded for issuing Qualified Certificates and is based on the specification of the RCF 3647 - Internet X standard. 509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework.

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.

With regard to the content of this COP, it is considered that the reader is familiar with the basic concepts of PKI, certification and digital signature, and it is recommended that, in case of ignorance of these concepts, the reader should inform him/herself in this regard.

1.2. Document identification

Name:	CP2_ACATC_009.0
O.I.D.	1.3.6.1.4.1.16533.20.3.1
Description:	Certification Policies (CP) of the Certification Authority of the Bar: Qualified certificates of electronic seal
Version:	009,0
Date of Issue:	21/03/2023
Location:	www.acabogacia.org/doc

Related CPS	
O.I.D.	1.3.6.1.4.1.16533.10.1.1

Description:	Certification Practices Statement of the Certification Authority of the Lawyers' Bar
Location:	www.acabogacia.org/doc

1.3. Community and Scope of Application.

1.3.1. Certification Authority (CA)

It is the entity responsible for the issuance and management of digital certificates. Acting as a trusted third party, between the Subscriber and the User, in electronic relations, this Policy allows to identify and link a certain system or platform to a certain entity (Subscriber) related to a specific Professional Association through the issuance of a Certificate.

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

1.3.2. Registration Authority (RA)

Entity that acts in accordance with this Certification Policy and, where appropriate, by agreement signed with the CA, whose functions are the management of applications, identification and registration of certificate applicants and those provided for in the specific Certification Practices.

For the purposes of this Policy, the RA is the Consejo General de la Abogacía Española (CGAE)

1.3.3. Subscriber

Under this Policy, subscribers may be the Professional Associations, the General Council of the professions and the Autonomous Councils holding a "qualified certificate of electronic seal" and, in general, any legal entity linked or related in any way to the professions.

1.3.4. User

In this Policy, User, trusted third party, is understood as the person who voluntarily trusts the Certificate, by virtue of the trust placed in the CA, uses it as a means of identification and authentication of a system or application as well as a means to authenticate the electronic documents produced by it. and therefore is subject to the provisions of this Policy, the applicable Certification Practice Statement (CPS) and current legislation, so no further agreement is required.

1.3.5. Other participants

Not stipulated

1.4. Scope of Application and Uses

1.4.1. Permitted uses of certificates

The Certificate issued under the present Policy allows to identify and link a certain system or platform to a certain entity, whether it is a Professional Association, a General Council of a profession or an Autonomous Council, as well as any legal person linked to the professional practice of the legal profession, also allowing to authenticate the electronic documents produced by the System.

1.4.2. Prohibited and Unauthorized Uses

Under the present Policy, use contrary to Spanish and Community regulations, international agreements ratified by the Spanish State, customs, morality and public order is not permitted. The use other than what is established in this Policy 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.

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

The Subscriber or User who decides to encrypt information shall 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:	Tel. 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 Policy (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
eIDAS	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-2	*Secure Hash Algorithm*. Secure Hash Algorithm
TLS	*Transport Layer Security. Its ancestor is SSL (Secure Socket Layer is a p*protocol designed by Netscape and made standard on the Web, it allows 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 be in charge of properly routing the information to its recipient
ENS	National Security Scheme. Adaptation of the ISO 27001 information security standard to the Spanish State. Royal Decree 3/2010, of January 8, 2010, which regulates the National Security Scheme in the field of Electronic Administration
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 available to users the following information

- Web Certification Policies and Practices 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.

2.3. Frequency of publication

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

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

Ordinarily, 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 for the consultation of CRLs and Certificates under the control of an application and protecting the indiscriminate downloading of information. CRLs may be downloaded anonymously via http protocol from the 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.509 standard, and the attributes specified in the ITU-T X.520 recommendation [1]

The DN of the qualified certificates of electronic seal shall contain the elements cited with the following format. All component values will be authenticated by the Registration Authority:

- A component Common Name (Common Name) -CN
- An E-mail component -E
- One component Organization -O
- A component Organizational Identifier -OI
- A Unity in Organization -OU component
- A State (Country)-C component
- A locality component - L

- The authenticated value of the Common Name -CN component will contain the name of the system or automatic processing application
- The authenticated value of the E-mail -E component will contain the contact e-mail address of the subscribing entity of the certificate
- The authenticated value of the Organization -O component will contain the name of the organization (certificate subscriber)
- The authenticated value of the Organization Identifier -OI component will contain a subscriber ID different from the organization name (certificate subscriber). This value shall comply with the semantics defined in section 5 of ETSI EN 319 412-1 [i.4]
- The authenticated value of the Unity in the Organization -OU component will contain the nature of the certificate (electronic seal for automated performance).
- The authenticated value of the State (Country)-C component shall contain "EN"
- The authenticated value of the L-L Locality component will contain the location of the head office of the subscribing entity

3.1.2. Meaning of the names

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

3.1.3. Pseudonyms

Qualified certificates of electronic seal do not admit pseudonyms.

3.1.4. Rules used to interpret various name formats

In all cases, the X.500 standard of reference in ISO/IEC 9594 is followed.

3.1.5. Uniqueness of names

The distinguished names of the issued certificates will be unique for each subscriber. The CA shall make reasonable efforts to confirm the uniqueness of the names of the certificates issued. The attribute of the Company Name of the entity, and/or the Tax ID will be 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 Certification Service Provider / Qualified Trust Service Provider shall not determine that a certificate applicant is entitled to the name that appears in a certificate request. 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 Certification Service Provider / Qualified Trust Service Provider reserves the right to reject a certificate request due to name conflict.

Names will be assigned based on their order of entry.

3.1.6. Recognition, authentication and function of registered trademarks

Trademarks will not be accepted as identification data of the Subscriber. In any case, it shall be identified through the Corporate Name.

3.2. Initial identity validation

3.2.1. Methods of proof of possession of the private key

The sending of the PKCS10 by the subscriber will constitute the guarantee that the subscriber is in possession of the private key.

3.2.2. Authentication of an organization's identity

The company's Tax Identification Number (CIF) will be required for all companies.

3.2.3. Authentication of an individual's identity

For a correct verification of the applicant's identity, documentation that accredits him/her and his/her physical appearance before the RA and the presentation of the National Identity Card or Foreigner's Card before an operator or duly authorized personnel of the Registration Authority and proof of his/her relationship with the legal entity will be required.

The RA shall verify with its own sources of information the rest of the data and attributes to be included in the certificate (distinguished name of the certificate), and shall keep the documentation accrediting the validity of those data that cannot be verified by means of its own sources of data.

Pursuant to Article 7 of Law 6/2020, The provisions of the preceding paragraphs may not be enforceable in the following cases:

a) When the identity or other permanent circumstances of the applicants for the certificates were already known to the RA by virtue of a pre-existing relationship, in which, for the identification of the applicant, the RA had a pre-existing relationship with the applicant

the means indicated in the first paragraph have been used and the period of time that has elapsed since the identification is less than five years.

b) When, in order to request a certificate, another certificate is used for the issuance of which the signatory has been identified in the manner prescribed in the first paragraph and the RA is satisfied that the period of time that has elapsed since the identification is less than five years.

3.2.4. Unverified subscriber information

All information contained in the certificates will be verified.

3.2.5. Validation of Registration Authorities

CSaccording to the provisions of the Certification Practice Statement (CPS).

3.2.6. Interoperability criteria

Not stipulated

3.3. Certificate renewal identification and authentication

3.3.1. Ordinary renewal

Certificates may not be renewed.

3.4. Reissuance after revocation

As stipulated in the Certification Practice Statement (CPS). See http://www.acabogacia.org/doc

3.5. Identification and authentication of a revocation request

They may request the suspension or revocation of a certificate:

- The subscriber himself who must identify himself/herself to the RA to request the revocation of his/her certificate.
- Authorized operators of the 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

4.1.1. Who can apply for a certificate

The RA manages applications for e-Stamp Certificates

The application for a digital certificate may be made by the applicant in person at the Registration Authority to a duly authorized operator.

4.2. Certificate application procedure

Upon receipt of the request and before starting the issuance process, the RA informs the applicant of the issuance process, the responsibilities and conditions of use of the certificate and the device, as well as verifies the identity of the applicant, and the data to be included in the certificate.

If the verification is correct, a binding legal instrument is signed between the applicant and the CA - AR.

4.3. Issuance of certificates

The process followed for the issuance of certificates is as follows:

- The RA receives the request for issuance of the certificate.
- The RA operator verifies again the content of the same and if the verification is correct, validates it and processes the approval of the issuance for the CA. If the request is not correct, the operator denies the request.
- The RA sends through a secure channel the request to the CA for the issuance of the corresponding certificate.
- The CA issues the certificate. The generated certificate is securely sent to the applicant
- The CA notifies the subscriber/applicant of the issuance.
- The generated certificate is securely sent to the Certificate Registry, which makes it available to users

4.4. Acceptance of certificates

Upon delivery of the certificate, the subscriber will have a period of seven calendar days to review the certificate, determine whether it is adequate and whether the data corresponds to reality. In case there is any difference between the data provided to the CA and the content of the certificate, this must be immediately communicated to the CA so that it can proceed to its revocation and the issuance of a new certificate.

The CA will deliver the new certificate at no cost to the subscriber in the event that the difference between the data is caused by an error not attributable to the subscriber.

Once this period has elapsed without any communication, it shall be understood that the subscriber has confirmed acceptance of the certificate and all its contents. By accepting the certificate, the subscriber confirms and assumes the accuracy of the content of the certificate, with the consequent obligations arising therefrom vis-à-vis the CA or any third party who in good faith relies on the content of the Certificate.

4.5. Key pair and certificate usage

4.5.1. Use of private keys and certificate by the subscriber

The private key will be generated by the subscriber and will remain in the exclusive possession of the subscriber at all times.

The CA or RAs does not create, store or possess at any time the subscriber's private key, nor the activation data of the device that holds it.

4.5.2. Use of public key and certificate by a trusted third party

Third parties who rely on a certificate will always do so voluntarily ensuring that they perform the appropriate checks to ensure the validity of the certificate they are relying on, subject always to the limitations indicated in this policy.

4.6. Renewal of certificates

Certificates may not be renewed.

4.7. Renewal of certificates and keys

Certificates and keys may not be renewed.

4.8. Modification of certificates

Modification of certificates once issued is not allowed

4.9. Suspension and Revocation of certificates

As stipulated in the Certification Practice Statement (CPS). See http://www.acabogacia.org/doc

4.10.Certificate status checking services

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

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

The details of the service shall be governed by the provisions of the Certification Practice Statement (CPS).

4.11.Termination of subscription

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

4.12.Custody and recovery of keys

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

As stipulated in the Certification Practice Statement (CPS). See http://www.acabogacia.org/doc

6. Technical Safety Controls

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 a 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.

The subscribers' passwords are generated by the subscribers themselves. The CA will make reasonable efforts to confirm that the keys are generated in accordance with the standards. The key pair will be generated and kept by or under the control of the subscriber.

6.1.2. Delivery of the private key to the subscriber

There is no delivery of private keys by the CA.

6.1.3. Delivery of the public key to the certificate issuer

The PKCS10 generated by the subscriber has to be transferred to the CA, so as to ensure that:

- It has not been modified during shipment.
- The sender is in possession of the private key that corresponds to the transferred public key.
- The provider of the public key is the legitimate user listed in the certificate.

6.1.4. Delivery of the CA public key to the Users

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

6.1.5. Key size

The subscriber's private keys are based on the RSA algorithm with a minimum length of 2048 bits.

6.1.6. Public key generation parameters

As stipulated in the Certification Practice Statement (CPS). See http://www.acabogacia.org/doc

6.1.7. Purposes of the use of the key

All certificates will include the 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

As stipulated in the Certification Practice Statement (CPS). See http://www.acabogacia.org/

6.2.2. Custody of private keys

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

6.2.3. Private key backup

As stipulated in the Certification Practice Statement (CPS). See http://www.acabogacia.org/doc

6.2.4. Private key file

As stipulated in the Certification Practice Statement (CPS). See http://www.acabogacia.org/doc

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

As stipulated in the Certification Practice Statement (CPS). See http://www.acabogacia.org/doc

6.2.6. Storage of the private key in cryptographic module.

As stipulated in the Certification Practice Statement (CPS). See http://www.acabogacia.org/doc

6.2.7. 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.

The subscriber's private key shall be maintained in a qualified electronic signature creation device and shall be controlled and managed by the subscriber. It shall have a protection system against access attempts that block the device when a wrong access code is entered several times.

6.2.8. Private key deactivation method

For qualified electronic signature certificates, by logging out of the CPS or PKCS#11. This will occur when the card is removed from the reader or when the application closes it.

6.2.9. Private key destruction method

The CA's private key as provided in the Certification Practice Statement (CPS). See http://www.acabogacia.org/doc

The CA's private key is destroyed in the certificate renewal process or by physical destruction of the cryptographic device.

6.2.10. Evaluation of the cryptographic module

Not stipulated

6.2.11. Evaluation of the cryptographic module

Not stipulated

6.3. Other aspects of key pair management

6.3.1. Public key file

As stipulated in the Certification Practice Statement (CPS). See http://www.acabogacia.org/doc

6.3.2. Period of use for public and private keys

Determined by the period of 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

As stipulated in the Certification Practice Statement (CPS). See http://www.acabogacia.org/doc

6.5.1. Specific IT security technical requirements

As stipulated in the Certification Practice Statement (CPS). See http://www.acabogacia.org/doc

6.5.2. Computer security assessment

As stipulated in the Certification Practice Statement (CPS). See http://www.acabogacia.org/doc

6.6. Life cycle of cryptographic devices

6.6.1. System development controls

As stipulated in the Certification Practice Statement (CPS). See http://www.acabogacia.org/doc

6.6.2. Life cycle safety level assessment

As stipulated in the Certification Practice Statement (CPS). See http://www.acabogacia.org/doc

6.6.3. Life cycle safety level assessment

As stipulated in the Certification Practice Statement (CPS). See http://www.acabogacia.org/doc.

6.7. Network security controls

As stipulated in the Certification Practice Statement (CPS). See http://www.acabogacia.org/doc.

6.8. Time stamping

Not stipulated

7. Certificate, 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 EN 319 412-5: Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile. and RFC 3739 (replacing RFC 3039) "*Qualified Certificates Profile*". The 319 412 family has also been taken into account in relation to certificate profiles.

Qualified certificates of electronic seal shall include, at least, the following data:

an indication, at least in a format suitable for automatic processing, that the certificate has been issued as a qualified certificate of electronic seal;

a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates, including at least the Member State in which the qualified trust service provider is established, and

a. for legal entities: the name and, where applicable, the registration number as recorded in the official registers,
b. for natural persons, the name of the person;
c. at least the name of the creator of the seal and, where applicable, the registration number, as recorded in the official registers;
d. the electronic seal validation data corresponding to the electronic seal creation data;
e. the data relating to the beginning and end of the period of validity of the certificate;
f. the identity code of the certificate, which must be unique to the qualified trust service provider;
g. the advanced electronic signature or advanced electronic seal of the issuing trust service provider;
h. the place where the certificate supporting the advanced electronic signature or the advanced electronic seal referred to in letter g) is freely available;

i. the location of the services that can be used to check the validity status of the qualified certificate;

j. where the electronic seal creation data related to the electronic seal validation data are contained in a qualified electronic seal creation device, an appropriate indication of this, at least in a form suitable for automatic processing.

7.1.1. Version number

X509 Version V3

7.1.2. Certificate extensions

7.1.2.1. Fields

The certificates will follow the X509 standard, defined in RFC 5280, and will have the following fields described in this section:

Certificates issued by ACA - Trusted Certificates

FIELDS	
Version	V3
Serial No	(serial no., which will be a unique code with respect to the distinguished name of the issuer)
Signature Algorithm	Sha1WithRSAEncryption
Issuer	CN = ACA - Trusted Certificates OU = Advocacy Certifying Authority O = Consejo General de la Abogacia NIF:Q-2863006I E = ac@acabogacia.org L = Madrid C = EN
Valid from (notBefore)	(valid from date, UTC time)
Valid until (notAfter)	(validity end date, UTC time)
Subject	(According to specifications in section **3.1.1**)

Public key	RSA (1024 bits)

Certificates issued by ACA - Trusted Certificates 2014

FIELDS	
Version	V3
Serial No	(serial no., which will be a unique code with respect to the distinguished name of the issuer)
Signature Algorithm	Sha1WithRSAEncryption
Issuer	CN = ACA - Trusted Certificates - 2014 SERIALNUMBER = Q2863006I OU = Attorney Certification Authority O = General Council of the Bar O = General Council of the Bar C = EN
Valid from (notBefore)	(valid from date, UTC time)
Valid until (notAfter)	(validity end date, UTC time)
Subject	(According to specifications in section **3.1.1**)
Public key	RSA (2048 bits)

Certificates issued by ACA CA2

FIELDS	
Version	V3
Serial No	(serial no., which will be a unique code with respect to the distinguished name of the issuer)

Signature Algorithm	Sha256WithRSAEncryption
Issuer	CN = ACA CA2 OI = VATES-Q2863006I OU = BAR CERTIFICATION AUTHORITY O = GENERAL COUNCIL OF THE BAR O = GENERAL COUNCIL OF THE BAR C = EN
Valid since (notBefore)	(valid from date, UTC time)
Valid until (notAfter)	(validity end date, UTC time)
Subject	(According to specifications in section **3.1.1**)
Public key	RSA (2048 bits)

7.1.2.2. Extensions

The following extensions will be included:

Certificates issued by ACA - Trusted Certificates

EXTENSIONS	
Alternative name of issuer (IssuerAlternativeName)	Name RFC822=ac@acabogacia.org URL address=http://www.acabogacia.org
Alternate name of subject (SubjectAlternativeName)	Name RFC822=xxxx.xxxxx@cgae.es
KeyUsage	Digital Signature, Non-repudiation, Key Encryption, Data Encryption
Enhanced Key Usage (ExtendedKeyUsage)	Client authentication (1.3.6.1.5.5.7.3.2) Secure mail (1.3.6.1.5.5.7.7.3.4)

Issuing entity key identifier (AuthorityKeyIdentifier)	5a f6 34 ce 96 76 56 b7 7c e9 dc dc 1d 13 6c 79 de 0f 30 76
Subject key identifier (SubjectKeyIdentifier)	
Certificate bases (SubjectStatement)	Certificate Directive: Directive identifier=1.3.6.1.4.1.16533.20.3.1 [1,1]Directive qualifier information: Directive qualifier ID=CPS Qualifier: http://www.acabogacia.org/doc [1,2]Directive qualifier information: Policy qualifier ID=User notice
CCC distribution point (CRLDistributionPoint)	http://www.acabogacia.org/crl/acatrusted.crl http://crl.acabogacia.org/crl/acatrusted.crl
BasicConstraints	Type of case= Final entity Route length restriction= None
Access to Authority Information (Authority Information Access)	[1]Access to authority information Access method=Certificate issuing entity issuer (1.3.6.1.5.5.7.48.2) Alternate name: Address URL=http://www.acabogacia.org/certificados/ACAtrusted.crt
qcStatements x.509v3 certificate extension from RFC 3039	

Certificates issued by ACA - Trusted Certificates 2014

EXTENSIONS	
Alternate name of subject (SubjectAlternativeName)	Optional
BasicConstraints	Type of case= Final entity Route length restriction= None
Holder's key identifier (SubjectKeyIdentifier)	
Issuing entity key identifier (AuthorityKeyIdentifier)	81 8F D1 63 00 4A CA 4D 20 97 A6 52 00 60 2E D2 CC 36 8B 6D
Enhanced Key Usage (ExtendedKeyUsage)	Client authentication (1.3.6.1.5.5.7.3.2) Secure mail (1.3.6.1.5.5.7.7.3.4)
Access to Authority Information (Authority Information Access)	[1] Access to authority information Access method=Online certificate status protocol (1.3.6.1.5.5.7.48.1) Alternate name: Address URL=http://ocsp.redabogacia.org [2] Access to authority information Method of access=Certificate issuing entity issuer (1.3.6.1.5.5.7.48.2) Alternate name: Address URL=http://www.acabogacia.org/certificados/ACAtrustedV2.crt
Certificate Policies	Certificate Directive: Directive identifier= 1.3.6.1.4.1.16533.20.3.1 [1,1]Directive qualifier information: Directive qualifier ID=CPS

	Certifier: http://www.acabogacia.org/doc
CCC distribution point (CRLDistributionPoint)	http://www.acabogacia.org/crl/ACAtrustedV2.crl http://crl.acabogacia.org/crl/ACAtrustedV2.crl
KeyUsage	Digital Signature, Non-Repudiation, Key Encryption, Data Encryption, Key Contract

Certificates issued by ACA CA2

EXTENSIONS	VALUE
Alternate name of subject (SubjectAlternativeName)	Optional
Basic restrictions (BasicConstraints)	Type of case= Final entity Route length restriction= None
Holder's key identifier (SubjectKeyIdentifier)	
Issuing entity key identifier (AuthorityKeyIdentifier)	8A 15 1F AF 74 EF 1F 01 07 73 2A 90 2A 41 09 7E 1B 48 D0 C0
Improved use of keys (ExtendedKeyUsage)	Customer authentication (1.3.6.1.5.5.7.3.2) Secure Mail (1.3.6.1.5.5.5.7.3.4)
Access to Authority Information (Authority Information Access)	[1]Access to authority information Access method=Online certificate status protocol (1.3.6.1.5.5.7.48.1) Alternate name: Address URL=http://ocsp.redabogacia.org [2]Access to authority information

	Access method=Certificate issuing entity issuer (1.3.6.1.5.5.7.48.2) Alternate name: Address URL=http://www.acabogacia.org/certificados/aca_ca2.crt
Certificate Policies	Certificate Directive: Directive identifier= 1.3.6.1.4.1.16533.20.3.1 [1,1]Directive qualifier information: Directive qualifier ID=CPS Certifier: http://www.acabogacia.org/doc
Statement of Qualified Certificates qcStatements x.509v3 certificate extension from RFC 3039	1.- id-etsi-qcs-QcCompliance 2.- id-etsi-qcs-QcPDS URL=http://www.acabogacia.org/doc/EN
CCC distribution point (CRLDistributionPoint)	http://www.acabogacia.org/crl/aca_ca2.crl http://crl.acabogacia.org/crl/aca_ca2.crl
KeyUsage	Digital Signature, Non-repudiation, Key Encryption

7.1.3. Object Identifiers (OID) of the algorithms

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

The object identifier of the public key algorithm will be 1.2.840.113549.1.1.1.1 rsaEncryption

7.1.4. Name format

Not stipulated.

7.1.5. Certificate policy object identifier

According to the OID indicated in paragraph 1.2

7.1.6. Use of extension policy restrictions

Not defined

7.1.7. 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

7.1.8. Semantic treatment for the extension "Certificate policy"

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

7.2. CRL Profile

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

For Certificates issued by the ACA - Trusted Certificates CA

http://www.acabogacia.org/crl/ACAtrusted.crl

http://crl.acabogacia.org/crl/ACAtrusted.crl

For Certificates issued by the CA ACA - Trusted Certificates 2014

http://www.acabogacia.org/crl/ACAtrustedV2.crl

http://crl.acabogacia.org/crl/ACAtrustedV2.crl

For certificates issued under the ACA CA2

http://www.acabogacia.org/crl/aca_ca2.cr

http://crl.acabogacia.org/crl/aca_ca2.crl

The following extensions will be included

Extensions

Version
Effective Date
Validity End Date
Signature Algorithm
Serial Number
Distribution points

7.3. OCSP Profile

7.3.1. Version number

The Certificates used by the Certificate Validity Status Query and Information Service, via OCSP, are compliant with the X.509 version 3 standard.

7.3.2. OCSP extensions

The OCSP responses of the Certificate Validity Status Query and Information Service include, for requests that request it, the global extension "nonce", which is used to link a request to a response, so that replay attacks can be prevented.

8. Compliance audits

As stipulated in the Certification Practice Statement (CPS). See ://www.acabogacia.org/doc

9. Other legal and operational issues

As stipulated in the Certification Practice Statement (CPS). See ://www.acabogacia.org/doc

ANNEX 1: Technical information

In compliance with the provisions of Regulation 910/2014 and Law 6/2020, subscribers and users are informed of certain aspects in relation to electronic signature creation and verification devices that are compatible with the signature data and the certificate issued, as well as mechanisms considered secure for the creation and verification of signatures.

Subscriber devices

Not stipulated.

Signature creation and verification

Supported standards and parameters

Not stipulated**.**

Signature verification methods

Verification of the electronic signature is essential to determine that it was generated by the key holder, using the private key corresponding to the public key contained in the subscriber's certificate, and to ensure that the signed message or document has not been modified since the generation of the electronic signature.

The verification shall normally be performed automatically by the verifying user's device, and in any case, and in accordance with the Certification Practice Statement (CPS) and current legislation, with the following requirements:

- It is necessary to use an appropriate device to verify a digital signature with the algorithms and key lengths authorized in the certificate and/or perform any other cryptographic operation. Such devices must comply with the provisions of Article 25 of the Electronic Signature Law
- It is necessary to establish the certificate chain on which the electronic signature to be verified is based and to ensure that the certificate chain identified is the most appropriate for the electronic signature being verified. It is the responsibility and decision of the user who verifies the choice of the appropriate chain if more than one is possible.
- It is necessary to check the integrity, digital signature and validity status (not expired, not revoked or not suspended) of all the certificates in the chain with the information provided by AC Abogacía in its certificate publication service. An electronic signature can only be considered correctly verified if all or each of the certificates in the chain are correct and valid.
- It is necessary to verify that the certificates of the chain have been used within the conditions and limits of use imposed by the issuer of each one of them, and by authorized signatories. Each certificate in the certification chain has information about its conditions of use and links to documentation about them.
- It is necessary to verify the adequacy of the algorithms and signature parameters of all the certificates in the chain and of the signed document itself.
- It is necessary to determine the date and time of generation of the electronic signature, since the correct verification requires that all the certificates in the chain were valid at the time the signature was generated.

- Finally, it is necessary to determine the signed data and technically verify the electronic signature itself with respect to the certificate used for signing, associated to a valid certification chain.

The user verifying a signature must act with the utmost diligence before relying on certificates and digital signatures, and use an electronic signature verification device with sufficient technical, operational and security capacity to execute the signature verification process correctly.

Finally, the requirements for the validation of qualified electronic signatures are determined in Article 32 of Regulation 910/2014 (eIDAs).

The user who verifies shall be exclusively responsible for any damage he/she may suffer due to the incorrect choice of the verification device, unless it has been provided by AC Abogacía.

The verifying user has to take into account the limitations of use of the certificate indicated in any way in the certificate, including those not automatically processed by the verification device and incorporated by reference. If circumstances require additional assurances, the verifier shall obtain these assurances to provide reasonable reliance.

In any case, the final decision as to whether or not to trust a verified electronic signature rests solely with the user.

Verification of Electronic Signatures over time

- If the user wishes to have guarantees over time that allow him to verify the validity of an electronic signature, he must use additional mechanisms, among others:
- If the Signatory has generated the signature in a format capable of being verified over time, such as those defined in EN 319 122-2 "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures" of the European Telecommunications Standards Institute (www.etsi.org), which AC Abogacía recommends.
- Use by the signatory and the verifier of third party mediation services, trusted by both, such as:Certificate validation services
    - Time stamping services
    - Transaction Notarization Services
    - Etc
- Preservation, in a secure and complete manner, together with the signature of all data necessary for verification:
    - All certificates in the certification chain.
    - All CRLs in effect immediately before and after the time of signing.
    - The policies and practices in effect at the time of signing.

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)