Abogacía Española
CONSEJO GENERAL

AUTORIDAD DE CERTIFICACIÓN DE LA ABOGACÍA

Qualified administrative staff certificates

Certification Policy (CP2_ACA_014.0)

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	CP002_ACA_001.0	Initial version
02/03/2004	CP002_ACA_001.1	Correction of errata.
26/10/2004	CP2_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.
13/03/2006	CP2_ACA_003.0	Updating new root certificate
13/03/2006	CP2_ACA_003.0	General overhaul
13/07/2006	CP2_ACA_004.0	Inclusion of OID to reference the application CPS
30/10/2006	CP1_ACA_005.0	Change certificate profile
02/03/2009	CP2_ACA_006.0	Fax is included as a contact
12/03/2014	CP2_ACA_007.0	A description of the PKI Hierarchy is included The section on scope and uses has been modified The possibility of online renewal has been added The possibility of online application for a digital certificate is eliminated The details of the Cryptographic module model are eliminated Length of user keys increased to 2048 bits New CRL distribution points indicated Correction of errata
27/06/2016	CP2_ACA_008.0	New PKI Hierarchy is included, new CAs certificates information Aligned with eIDAS Adaptation of recognized services to qualified
03/05/2017	CP2_ACA_009.0	The following changes are made to the certificate profile: Qctype is included KeyUsage is modified to align with ETSI EN 319 412 including non-repudiation, digital signature and key encryption
02/06/2020	CP2_ACA_010	Adaptation RFC 3640 Reference is made to Other Operational and Legal issues (item 9) to the CPS

02/07/2020	CP2_ACA_011	The RA identification code is separated in a separate field with OID 1.3.6.1.4.1.16533.30.3
31/05/2022	CP2_ACA_012	Change of document template Removal of duplicate sections with CPS Legislative adaptation Law 6/2020, of November 11 Updating acronyms Update OID 1.3.6.1.4.1.16533.30.2
21/03/2023	CP2_ACA_013	Annual legislative review
01/03/2024	CP2_ACA_014	Annual review

INDEX

Contenido

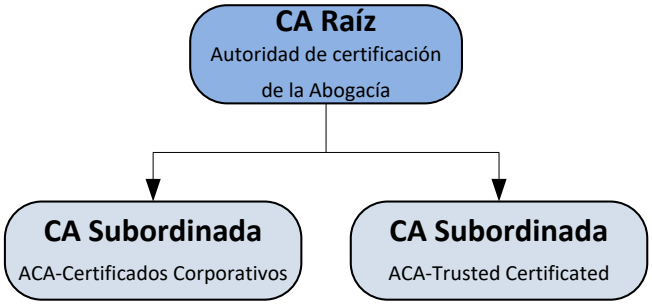
1. Introduction

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

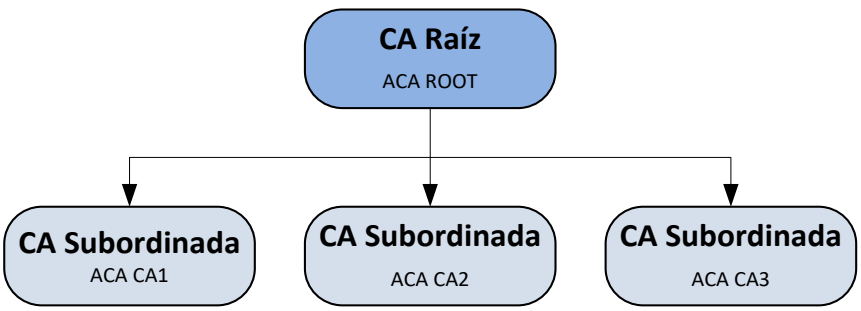


In 2014, new subordinated CAs were generated with the same denomination followed by the year of issue: *ACA - Corporate Certificates 2014 and ACA-Trusted Certificates 2014.*

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 Corporate Administrative Staff Certificate" or simply "Administrative Staff Certificate" 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 Association 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_ACA_014.0
O.I.D.	1.3.6.1.4.1.16533.10.3.1
Description:	Certification Policies (CP) of the Certification Authority of the Spanish Bar: Qualified certificates for Administrative Staff
Version:	014.0
Date of Issue:	01/03/2024
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. It acts as a trusted third party, between the Subscriber and the User, in electronic relations, linking a certain public key with a person (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, RA's are the following entities:

a) General Council of Spanish Lawyers (CGAE)

b) The Autonomous Councils of the Legal Profession

c) Bar Associations

1.3.3. Subscriber

Under this Policy the Subscriber is a natural person, linked to a Spanish Bar Association or Council of Bar Associations on the basis of a commercial or labor contract with the same or related institutions, holder of a secure signature creation device associated with a "Qualified Administrative Staff Certificate" hosted on a qualified electronic signature creation device. The subscriber is also referred to as the "Signatory", as defined in Art. 3.9 of Regulation 910/2014.

1.3.4. User

In this Policy, the 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 accreditation of the authenticity and integrity of the signed document and consequently is subject to the provisions of this Policy, the applicable Certification Practice Statement (CPS) and current legislation, so that no subsequent 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 this Policy identifies a natural person in his or her personal capacity and within the scope of his or her activity and connection to a Bar Association or Council of Bar Associations or related institutions. Administrative Staff certificates may be used under the terms established by the corresponding certification practices.

In addition to simple electronic communications, its use is authorized for commercial, economic and financial transactions, in digital media, provided that they are based on the RCF 3647 (X. 509) standard, and that they do not exceed the maximum value defined in the Certification Practices Statement (CPS), which may never be less than the provisions of this policy.

The Certificate issued under this Policy may be used for the following purposes:

- Identification of the signatory and his/her relationship with the institution: The Subscriber of the Certificate can authenticate, in front of another party, its identity and its link to the institution, demonstrating the association of its private key with the respective public key, contained in the Certificate. The subscriber may validly identify himself/herself to any person by signing an e-mail or any other file.
- Integrity of the signed document: The use of this Certificate guarantees that the signed document is intact, that is, it guarantees that the document was not altered or modified after it was signed by the Subscriber. It certifies that the message received by the User is the same as the one issued by the Subscriber
- Non-repudiation of origin: The use of this Certificate also guarantees that the person signing the document cannot repudiate it, i.e. the Subscriber who has signed it cannot deny the authorship or integrity of the document.

Although it is possible to use it for data encryption, it is not recommended because it is not possible to recover the encrypted data in case of loss of the private key by the Subscriber. The Subscriber or the User shall do so, in any case, under his own responsibility.

The Administrative Staff Certificates do not identify or bind the business entity that appears in them, but rather the natural person, and do not presuppose any type of empowerment of the natural person (Subscriber) with respect to the legal person (Applicant).

The certificates described in this policy are qualified certificates, which are also in accordance with the provisions of Article 51 of Regulation 910/2014, which states in the second paragraph that, qualified certificates issued to natural persons in accordance with Directive 1999/93/EC shall be considered Qualified Certificates of electronic signature under this Regulation until they expire. These certificates serve as the basis for the generation of qualified electronic signatures created by means of a qualified electronic signature creation device.

Administrative Staff certificates must necessarily be used with a qualified electronic signature creation device in accordance with applicable law and this policy. Guaranteeing the identity of the subscriber and of the holder of the private signature key, being suitable for providing support to the qualified electronic signature, i.e. the advanced electronic signature based on

a qualified certificate and generated by a qualified signature creation device. The qualified electronic signature shall have the same value with respect to data recorded in electronic form as a handwritten signature has with respect to data recorded on paper.

Likewise, the standards regarding recognized or qualified certificates have been taken into account, specifically:

- ETSI EN 319 412-5: Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile (replaces TS 101 862).
- RFC 3739 Internet X.509 Public Key Infrastructure: Qualified Certificates Profile

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 CA does not create, store or possess at any time the Subscriber's private key, and it is not possible to recover the data encrypted with the corresponding public key in the event of loss or disablement of the private key or the device that holds it by the Subscriber.

The Subscriber or User who decides to encrypt information shall do so in any case under his own and sole responsibility, without 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:

Lawyer certification authority. 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:	General Council of Spanish Lawyers

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 adaptation of the Certification Policies and Practices

1.5.4. Policy approval procedures

The publication of revisions to this Policy 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

2. Publication and Repository of Certificates

2.1. Repositories

AC Abogacía will make available to users the following information

- 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.

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. 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 CRLs can be downloaded anonymously via http protocol from the following URLs 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 Corporate certificates shall contain at least the elements listed in 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 Unity in Organization -OU component
- A T-Title component
- A geographic location component -ST
- A State (Country)-C component
- A Serial Number component -serialNumber
- A component Given name (Given name) - G
- One component Surname 1 "Surname" - SN
- One component Surname 2 with OID 1.3.6.1.4.1.16533.30.1
- One Organization Identifier Code component with OID 1.3.6.1.1.4.1.16533.30.2
- An RA identification code component with OID 1.3.6.1.4.1.16533.30.3.

Administrative Staff Certificates

- The authenticated value of the common Name -CN component will contain the subscriber's name (First Name and Surname) and Tax ID number.
- The authenticated value of the E-mail -E component will contain the subscriber's e-mail address
- The authenticated value of the Organization -O component will contain the name of the institution with which the subscriber maintains the relationship, i.e. the Bar Association or Bar Council.
- The authenticated value of the Unit in Organization -OU component will contain the Department or Unit to which the subscriber belongs.
- The authenticated value of the T-Title component will contain the subscriber's position, title or role in the organization.
- The authenticated value of the geographic location component -ST will contain the town where the RA's main office is located.
- The authenticated value of the State (Country)-C component will contain "ES".
- The authenticated value of the serialNumber component shall contain the subscriber's TIN or identifier in accordance with ETSI EN 319 412-1

CIF of the Organization, represented by the following OID (1.3.6.1.4.1.16533.30.2), which will contain the CIF corresponding to the institution linked to the subscriber.

- The authenticated value of the Given name - G component will contain the first name of the Subscriber.
- The authenticated value of the component Surname 1 "Surname" -SN will contain the Subscriber's first surname. The authenticated value of the component with OID 1.3.6.1.4.1.16533.30.1 will contain the Subscriber's second surname.
- The value of the component with OID 1.3.6.1.4.1.16533.30.3 shall contain the numeric code of the Registration Authority defined in the O field. It shall be composed of a code corresponding to an internal coding of ACA, a slash "/" and the code of the EJIS Compatibility Test of the General Council of the Judiciary, if any.

3.1.2. Pseudonyms

Corporate certificates for Administrative Staff do not accept pseudonyms. Nor may pseudonyms be used to identify an organization.

3.1.3. Rules used to interpret various name formats

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

3.1.4. 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 e-mail attribute and/or the NIF 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.

3.1.5. Recognition, authentication and function of registered trademarks

The CA will not assume commitments in the issuance of certificates with respect to the use by subscribers of a trademark. The use of a name whose right of use is not owned by the subscriber will not be deliberately allowed. However, the CA is not required to search for evidence of trademark ownership prior to issuance of certificates.

3.2. Initial identity validation

3.2.1. Methods of proof of possession of the private key

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

The RA delivers (if it does not have one) a kit containing the qualified device for the creation of electronic signatures. If the device has not been previously initialized, the subscriber initializes the qualified electronic signature creation device in the RA itself and before the operator. During this process, the device activation data is generated, or if the initialization is performed by an external entity, it will be delivered to you through a process that ensures its confidentiality to third parties. Initialization of the device completely deletes any previous information contained in the device.

The subscriber then generates the key pair and a CSR on its qualified electronic signature creation device, sending the public key along with the verified data to the CA in PKCS10 or equivalent format via a secure channel. The generation of the key pair will require the correct entry of the device activation data, and the entry of a device identification code that links the device to the subscriber authorized to use it.

Therefore, the method of proof of possession of the private key by the subscriber will be PKCS#10.

3.2.2. Authentication of an organization's identity

In order to carry out a correct verification of the identity of an organization for the issuance of Administrative Staff certificates, it shall be properly justified before the Registration Entity, unless the Requesting Organization is the College or Council itself:

- The accreditation by a reliable means of the existence of the entity in accordance with the law.
- The identity of the natural person representing the organization for the application,
- The relationship of the applicant organization with respect to the RA, certified by an authorized representative of the RA

3.2.3. Authentication of an individual's identity

For a correct verification of the identity of the subscriber of personal certificates, the subscriber will be required to appear in person before the RA and present the National Identity Document, Spanish passport or Foreigner's Card before an operator or duly authorized personnel of the Registration Authority.

Additionally, the RA will require the justification of the authorization of the requesting Organization with respect to the natural person (Subscriber).

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.

In accordance with Article 7 of Law 6/2020, the provisions of the preceding paragraphs may be waived 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

As stipulated in the Certification Practice Statement (CPS).

3.2.6. Interoperability Criteria

Not stipulated.

3.3. Identification and authentication for certificate renewal

3.3.1. Ordinary renewal

The renewal of certificates will consist of the issuance of a new certificate to the subscriber at the expiration date of the original certificate. Before renewing a certificate, the RA shall verify that the information used to verify the subscriber's identity and other subscriber data is still valid.

If any subscriber information has changed, the new information will be appropriately recorded.

The subscriber may renew online from one month prior to expiration as long as the subscriber's identification data remains the same and the period of time elapsed since the initial identification is less than five years.

3.3.2. Reissuance after revocation

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

3.4. Identification and authentication of a revocation request

As provided in the Certification Practice Statement (CPS)=

4. Operational requirements of the certificate life cycle

4.1. Request for certificates

4.1.1. Who can apply for a certificate

The request for a digital certificate may be made by the applicant in person at his Bar Association before a duly authorized operator.

4.2. Certificate application procedure

Once the certificate request is received 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, and the applicant becomes a subscriber.

The RA delivers to you (if you do not have one) a kit containing the qualified device for the creation of electronic signatures supporting the private key and the access devices to it, if any.

If the device has not been previously initialized, the subscriber initializes the qualified electronic signature creation device at the RA itself and before the operator. During the initialization process, the device activation data and access to the private key it will contain are generated. The subscriber will generate the activation data, or if the initialization takes place in an external entity, it will be delivered to the subscriber 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. Initialization of the device completely deletes any previous information contained in the device.

The subscriber then generates the key pair and a CSR on its qualified electronic signature creation device, sending the public key along with the verified data to the CA in PKCS10 or equivalent format via a secure channel. The generation of the key pair will require the correct entry of the device activation data, and the entry of a device identification code that links the device to the subscriber authorized to use it.

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 request and if the verification is correct, validates it and processes the approval of the issuance for the CA, by digitally signing the request with its operator certificate. 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, if the request received does not contain technical errors, in the format or content of the request, securely linking the certificate with the registration information, including the certified public key, in a system that uses protection against forgery and maintains the confidentiality of the exchanged data.
- The generated certificate is securely sent to the RA for downloading to the Qualified Electronic Signature Creation Device in the presence of the Subscriber.
- The CA notifies the subscriber of its issuance.
- The generated certificate is securely sent to the Certificate Registry, which makes it available to users. Acceptance of certificates

With the delivery of the card, the subscriber accepts his certificate in the qualified device for the creation of electronic signatures that holds the private key.

4.4. Acceptance of certificates

A subscriber shall be deemed to accept his certificate when he downloads his certificate to the qualified electronic signature creation device that holds the private key, by accessing the AC-AR certificate download system and performs the technical steps provided by the system for the download.

Without prejudice to what is indicated in the previous paragraph, the subscriber shall have a maximum period of seven calendar days to notify the RA of any defect in the certificate data, or in the publication of the certificate data in the Register of Certificates.

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. It is stored in a qualified electronic signature creation device requiring for its use the activation data that only the subscriber knows.

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 the 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

4.6.1. Circumstances for renewal of certificates

The renewal of certificates still in force will be done online as long as the data contained in the certificate is still valid. In case of data changes or expiration of the certificate, a new one will be issued by an RA Operator.

All regular renewals will involve the generation of new subscriber keys.

4.6.2. Who can apply for certificate renewal

Renewal can be requested by the certificate subscriber himself, provided that he has a valid certificate, has not changed any certificate data and the deadlines established in art. 7.6 of Law 6/2020 are met.

4.6.3. Certificate renewal procedure

The certificate subscriber accesses the online renewal procedure by identifying himself/herself with his/her still valid certificate and signs the certificate renewal request, initiating at that moment the generation of a new one with the same data.

4.6.4. Notification of certificate renewal

Once the renewal process is completed, the user will be informed of the successful renewal of the certificate.

4.6.5. Acceptance of renewal

A subscriber shall be deemed to accept the renewal of the certificate when he/she downloads the certificate to his/her qualified electronic signature creation device that holds the private key, once the technical steps provided by the system for the renewal have been carried out.

4.6.6. Publication of certificate renewals

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

4.6.7. Notification of renewal to other entities

Not stipulated

4.7. Renewal of certificates and keys

According to the provisions of section 4.6 Renewal of certificates

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

5. Physical, Procedural and Personnel Security Controls

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

6. Technical Safety Controls

6.1. Key pair generation and installation

6.1.1. Subscriber key pair generation

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.

Subscriber keys are generated by qualified electronic signature creation devices. 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 augmented with AVA_VAN.5. In accordance with paragraph 1 of the transitional measure of Article 51 of Regulation 910/2014 (eIDAs), secure signature creation devices whose compliance has been determined in accordance with Article 3(4) of Directive 1999/93/EC shall be considered as qualified electronic signature creation devices under this Regulation.

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

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

Cryptoprocessor cards will be used as SSCD for the subscriber to generate and store the signature creation data, i.e. the private key:

a) Cards are prepared and stamped by an external card supplier.

b) The distribution of the media is managed by the external card supplier who distributes it to the registration authorities for personal delivery to the subscriber. The RA can perform graphical customization of the card.

c) The subscriber initializes the card and uses it to generate the key pair and send the public key to the CA.

d) The CA sends a public key certificate to the subscriber that is inserted in the card.

e) The card is reusable and can securely hold multiple key pairs.

f) The useful life of the user cards will have an average life of 6 years

6.1.2. Delivery of the private key to the certificate subscriber

AC Abogacía does not deliver the private key to the subscriber

6.1.3. Delivery of the public key to the certificate issuer

The public key is sent to the CA for certificate generation using the standard PKCS#10 format

6.1.4. Delivery of the CA public key to the 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

The subscriber's private keys are based on the RSA algorithm with a 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/doc

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

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

6.2.3. 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

6.2.4. Private key backup

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

6.2.5. Private key file

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

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

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

6.2.7. Storage of the private key in cryptographic module.

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

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.

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.

6.2.9. 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.

6.2.10. 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.

6.2.11. 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. CRL and OCSP Certificate Profiles

7.1. Certificate Profile

All certificates issued under this policy are in compliance with the X.509 version 3 standard, RFC 5280Internet*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 shall include, at least, the following data:

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

b) 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

— for legal entities: the name and, where applicable, the registration number as recorded in the official registers,

— for natural persons, the name of the person;

c) at least the name of the signatory or a pseudonym; if a pseudonym is used, it shall be clearly indicated;

d) validation data of the electronic signature that correspond to the creation data of the electronic signature;

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 signature creation data related to the electronic signature validation data are contained in a qualified electronic signature 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 - Corporate 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
Emitter	CN = ACA - Corporate Certificates

(issuer)	OU = Advocacy Certifying Authority O = Consejo General de la Abogacia NIF:Q-2863006I E = ac@acabogacia.org L = Madrid 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 (1024 bits)

Certificates issued by ACA - Corporate 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 - Corporate 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	(validity end date, UTC time)

(notAfter)	
Subject	(According to specifications in section **3.1.1**)
Public key	RSA (2048 bits)

Certificates issued by ACA CA1

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 CA1 OI = VATES-Q2863006I OU = BAR 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)

7.1.2.2. Extensions

The following extensions will be included:

Certificates issued by ACA - Corporate Certificates

EXTENSIONS	
Issuer's alternative name (IssuerAlternativeName)	Name RFC822=ac@acabogacia.org URL address=http://www.acabogacia.org
SubjectAlternativeName (SubjectAlternativeName)	Name RFC822=xxxx.xxxxx@cgae.es
KeyUsage	Digital Signature, Non-Repudiation, Key Encryption, Data Encryption, Key Contract
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)
Netscape Certificate Type (NetscapeCertType)	SSL client authentication, SMIME (a0
Netscape Certificate Authority policy URL (netscape-ca-policy-url**)**	http://www.acabogacia.org/doc
Netscape Comment (NetscapeComment)	This is a recognized personal certificate. See http://www.acabogacia.org/doc
Issuing entity key identifier (AuthorityKeyIdentifier)	5a794ca10cfc08162cc285454f 32abe72b45c011
SubjectKeyIdentifier (SubjectKeyIdentifier)	
Certificate bases (SubjectStatement)	Certificate Directive: Policy identifier=1.3.6.1.4.1.16533.10.3.1 [1,1]Policy qualifier information: Directive qualifier ID=CPS Qualifier:

	http://www.acabogacia.org/doc [1,2]Directive qualifier information: Policy qualifier ID=User Notice Qualifier: Warning text=This is a recognized personal certificate. See http://www.acabogacia.org/doc
CRL Distribution Point (CRLDistributionPoint)	http://www.acabogacia.org/crl/acacorporativos.crl http://crl.acabogacia.org/crl/acacorporativos.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/ACAcorporativos.crt
1.3.6.1.5.5.7.1.3 qcStatements x.509v3 certificate extension from RFC 3039	0 Euros

Certificates issued by ACA - Corporate Certificates 2014

EXTENSION	VALUE
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)	33 6D D0 E9 CD 18 D7 B4 EB 4E FC F3 E3 CD FB 3D 5B C0 A3 9E
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 Access method=Certificate issuing entity issuer (1.3.6.1.5.5.7.48.2) Alternate name: Address URL=http://www.acabogacia.org/certificados/ACAcorporativosv2.crt
Certificate Policies	Certificate Directive: Policy identifier= 1.3.6.1.4.1.16533.10.3.1 [1,1]Policy 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-QcSSCD
CCC distribution point (CRLDistributionPoint)	http://www.acabogacia.org/crl/acacorporativosv2.crl http://crl.acabogacia.org/crl/acacorporativosv2.crl
Use of the Key	Digital Signature, Non-Repudiation, Key Encryption, Data Encryption, Contract

(KeyUsage)	of keys

Certificates issued by ACA CA1

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)	72 A9 E7 D6 8E 02 67 A0 4A 4C 1A 67 31 BC B7 FE CB 84 B4 9B
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_ca1.crt
Certificate directives	Certificate Directive:

(Certificate Policies)	Policy identifier= 1.3.6.1.4.1.16533.10.3.1 [1,1]Policy 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-QcSSCD 3.- id-etsi-qcs-QcPDS URL=http://www.acabogacia.org/doc/EN
CCC distribution point (CRLDistributionPoint)	http://www.acabogacia.org/crl/aca_ca1.crl http://crl.acabogacia.org/crl/aca_ca1.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 with the CA ACA-Corporate

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

http://crl.acabogacia.org/crl/ACAcorporativos.crl

http://crl.acabogacia.org/crl/ACAcorporativos.crl

For certificates issued with the ACA Corporate CA 2014

http://www.acabogacia.org/crl/ACAcorporativosV2.crl

http://crl.acabogacia.org/crl/ACAcorporativosV2.crl

For certificates issued with the ACA CA1

http://www.acabogacia.org/crl/aca_ca1.crl

http://crl.acabogacia.org/crl/aca_ca1.crl

The following extensions will be included

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

7.2.3. Issuance period and validity

They are issued ex officio on a daily basis and when there is a change of status. Validity is weekly.

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 http://www.acabogacia.org/doc

9. Other legal and operational issues

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

Prior to the request and issuance of the qualified certificate, the subscriber must have the corresponding signature creation and signature creation data generation device.

A. Qualified Electronic Signature Creation Devices:

The Qualified Certificates identified by Policy OID 1.3.6.1.4.16533.10.3.1 require, for their issuance, that the signature creation data have been generated by the subscriber and are stored in a device that complies with the provisions of Annex II of eIDAS, and are called "Qualified Electronic Signature Creation Devices (DCCFE)".

The advanced electronic signature generated with such devices, and based on a qualified certificate, is called "Qualified Electronic Signature. The qualified electronic signature shall have a legal effect equivalent to that of a handwritten signature.

The CA considers suitable devices that comply with the following:

That they have the corresponding device certification as established in article 51 of eIDAS, in which case it will be admitted without further ado.

B. Other Signature Creation Devices:

Not stipulated

In both cases (A) and (B), the CA will only issue certificates in response to requests that comply with the provisions of the following section for the key generation algorithms and signature algorithm parameters considered appropriate (2048-bit RSA keys), even if the device has the technical capacity to generate another type of set of signature parameters.

Signature creation and verification

Supported standards and parameters

The correct use of devices for the creation of secure Electronic Signatures is associated with the use of a subset of standards and parameters among those approved by ETSI in the document "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites" ETSI TS 119 312 and "Electronic Signatures and Infrastructures (ESI);

Guidance on the use of standards for cryptographic suites" ETSI TR 119 300 (www.etsi.org)

Third parties relying on generated signatures must ensure that the signature received complies with the provisions of the preceding paragraphs.

In the event that the signature creation device allows different types of signatures or the export of the signature creation data to another device that could generate electronic signatures with parameters other than those specified (such as a signature with type "rsa" with hash function "md5"), subscribers and users are informed that such signatures cannot be considered as signatures

it is the responsibility of the former to ensure that the above requirements are complied with, and of the latter that the signatures received are technically adequate.

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.

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 ETSI EN 319 122-2 "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures" by the European Telecommunications Standards Institute (www.etsi.org), which AC Abogacía recommends.
- Use by the signatory and the verifier of third party mediation services in which they both place their trust, 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)