Autoridad de Certificación de la Abogacía

Consejo General de la Abogacía Española

Reference: **CP2_ACA_006.0**
Date: **02/03/2009**
Document status: **Published**

CERTIFICATE POLICIES (CPS) OF THE SPANISH BAR ASSOCIATION CERTIFICATION AUTHORITY (*AC ABOGACÍA*)

CP2_ACA_006.0

ADMINISTRATIVE PERSONNEL

QUALIFIED CERTIFICATES

(VERSION 006.0)

Change control

Date	Version	Changes
27/03/2003	CP002_ACA_001.0	Initial version.
02/03/2004	CP002_ACA_001.1	Corrigenda.
26/10/2004	CP2_ACA_002.0	General revision. Amendments for better adaptation to the provisions of Act 59/2003 governing electronic signatures and greater clarity for subscribers and users.
01/09/2005	CP2_ACA_003.0	Updating of new root certificate.
13/03/2006	CP2_ACA_003.0	General revision.
13/07/2006	CP2_ACA_004.0	Inclusion of OID to reference the applicable CPS.
30/10/2006	CP2_ACA_005.0	Amendment to certificate profile.
02/03/2009	CP2_ACA_006.0	Fax number is included as a contact.

Contents

1. Introduction

1.1. Overview

The National Council of Spanish Bar Associations (CGAE) is the superior representative, coordinating and executive body of the Spanish Bar Associations and has, for all purposes, the status of public corporation, with its own legal personality and full capacity to comply with its objectives.

This document specifies the Certificate Policy in respect of the digital certificate called "Administrative Personnel Qualified Certificate" or simply "Administrative Personnel Certificate" issued by the Certification Authority of the National Council of Spanish Bar Associations, or *AC Abogacía*.

In its capacity as the entity regulating the Spanish Bar Associations, the National Council of Spanish Bar Associations (CGAE) has established its own certification system for the purpose of issuing certificates for diverse uses and different end users. For this reason, different types of certificates are generated. Certificates are issued by Accredited Certification Service Providers to end entities, including Bar members, administrative and service personnel, organisations and natural persons representing said organisation.

This Certificate Policy is compliant with the legal provisions governing electronic signatures in the European Community (Directive 1999/93/EC) and in Spain (Act 59/2003 of 19th December 2003 governing Electronic Signatures), while complying with all of the technical and security prerequisites required for Qualified Certificate issuance and is based on the specifications of standard RFC 2527 – *Internet X. 509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework.*

The CPS of the Spanish Bar Association Certification Authority (*AC Abogacía*), which sets out the concrete terms of the service provided, may be found at http://www.acabogacia.org/doc

In respect of the content of this CP, it is assumed that readers have a basic understanding of PKI, certification and digital signatures while if otherwise, we recommend that they become familiar with this subject.

1.2. Identification

Name:	CP2_ACA_006.0
OID	1.3.6.1.4.1.16533.10.3.1
Description:	Certificate policies (CPs) of the Spanish Bar Association Certification Authority (*CA Abogacía)*: Administrative Personnel qualified certificates
Version:	006.0
Date of issue:	02/03/2009
Location:	www.acabogacia.org/doc

Related CPS	
OID	1.3.6.1.4.1.16533.10.1.1
Description:	Certification Practice Statement of the Spanish Bar Association Certification Authority (*CA Abogacía*)
Location:	www.acabogacia.org/doc

1.3. Community and Applicability

1.3.1 Certification Authority (AC or CA)

This is the entity responsible for issuing and managing digital certificates. It acts as a third trusted party between the subscriber and the user in electronic relations, associating a certain public key with a person (subscriber) related to a specific professional association by virtue of the issuance of a certificate.

Information on the *AC* may be found at the website www.acabogacia.org.

1.3.2 Registration Authority (RA)

This is an entity that acts in compliance with this Certificate Policy and, as the case may be, by virtue of an agreement subscribed with the *AC*, which entity is responsible for the management of applications, the identification and registration of certificate applicants and the functions indicated in the related certification practices.

For the purpose hereof, the RAs are the following entities:
a) The National Council of Spanish Bar Associations (CGAE)
b) The Regional Councils of Spanish Bar Associations
c) The Spanish Bar Associations

1.3.3 Certification Service Provider (CSP)

In accordance herewith, a CSP is understood to be any entity that provides concrete services relating to the certificate life cycle.

The functions of the CSP may be exercised directly by the *AC* or by a delegated entity.

1.3.4 Subscriber

In accordance herewith, the "subscriber" is a natural person, bound to a Spanish Bar Association or Council of Bar Associations consequent on a commercial or labour contract therewith or with institutions bound thereto, who holds a secure signature-creation device associated with an "Administrative Personnel Qualified Certificate" that is located in said device. The subscriber is also called "signatory" as defined in section 6 of Act 59/2003.

1.3.5 User

In accordance herewith "user" is understood to be a third relying party, the person who voluntarily relies on the certificate by virtue of his trust in the AC. He uses it as a means of verifying the authenticity and integrity of the signed document, consequent on which he is bound by the provisions of this policy, of the CPSs applicable and the laws in force, wherefore no subsequent agreement of any kind is required.

1.3.6 Applicant

For the purpose hereof, the "applicant" is the institution, a legal entity, which applies for the Administrative Personnel qualified certificate.

1.3.7 Applicability and Uses

The certificate issued under this Policy enables a natural person to be identified in the scope of his activity and relationship with a Bar Association, Council of Bar Associations or institutions bound thereto. Administrative Personnel certificates may be used in accordance with the terms set forth under the corresponding certification practices.

In addition to simple electronic notifications, their use is authorised for commercial, economic and financial transactions by digital media provided that they are based on the standard RFC 3647 (X. 509) and that they do not exceed the maximum value defined under the CPS, which may never be less than that set forth hereunder.

The Certificate issued by virtue hereof may be used for the following purposes:

- Identification of the signatory and his connection with the institution: The subscriber of the certificate may authenticate to another party his identity and connection with the institution by demonstrating the association of his private key with the respective public key contained in the certificate. The subscriber may identify himself validly 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 integral, i.e., it guarantees that the document has not been altered or modified after the signing thereof by the subscriber. The message received by the user is certified to be the same as that issued by the subscriber.
- Non-repudiation of origin: The use of this certificate also guarantees that the person who signs the document cannot repudiate it, namely, the subscriber who has signed may not deny the authorship or integrity thereof.
- Although said certificate may be used to encrypt data, this is not recommended since encrypted data cannot be recovered in cases of loss of the private key on the part of the subscriber. Should the subscriber or the user encrypt, they do so under their own responsibility at all times.

Administrative Personnel Certificates neither identify nor bind the commercial entity that is indicated therein vis-à-vis third parties, but rather the natural person, and they do not presuppose any type of empowerment of the natural person (subscriber) in respect of the legal entity (applicant).

The certificates described hereunder are qualified certificates in accordance with the provisions of section 11 of Act 59/2003. They correspond to qualified certificates (with a secure signature-creation device if required), issued to the public, in compliance with technical standard TS 101 456 v1.2.1 of the European Telecommunications Standards Institute.

Administrative Personnel certificates must be used, of necessity, with a secure electronic signature-creation device that complies with the requirements set forth in section 24 of Act 59/2003 and hereunder. They guarantee the identity of the subscriber and the holder of the private signature key and are suitable for offering support to the qualified electronic signature, namely the advanced electronic signature that is based on a qualified certificate and has been generated using a secure device, consequent on which, pursuant to section 3 of Act 59/2003, it ranks equally with a handwritten signature by operation of law, without the need to satisfy any additional requirement of any kind.

1.3.7.1 Certificate usage constraints and prohibitions

In accordance herewith, use is not permitted that is contrary to Spanish and Community law, to international conventions ratified by the Spanish State or to custom, moral and public order. Neither is the use other than that set forth under this Policy and the Certification Practice Statement permitted.

The certificates have not been designed, they cannot be used and their use or resale is not authorised as dangerous situation control devices or for uses that require failsafe operations, such as the operation of nuclear installations, navigation systems or air communications or arms control systems, where a failure could lead directly to death, bodily harm or severe environmental damage.

Modifications to the certificates are not authorised; they must be used as provided by the *AC*.

The *AC* does not generate, store or possess the subscriber private key at any time and it is not possible to recover enciphered data with the corresponding public key in the event of loss or disablement of the private key or the device storing said key on the part of the subscriber.

Any subscriber or user who decides to encipher information shall do so under his own, exclusive responsibility while the *AC* shall on no account be liable in the event of information encipherment using the keys associated with the certificate.

1.4. Contact details

Organisation responsible:
Autoridad de certificación de la Abogacía (Spanish Bar Association Certification Authority)
Consejo General de la Abogacía Española (The National Council of Spanish Bar Associations)

Contact person:
Administrador AC Abogacía (Administrator *AC Abogacía*)
Departamento de Operaciones (Operations Department)

E-mail:	info@acabogacia.org
Telephone:	902 41 11 41
Fax	915327836
Address:	Consejo General de la Abogacía Española Paseo de Recoletos, 13 28004 Madrid

2. General Provisions

2.1. Obligations

2.1.1 AC

The *AC* is bound by the provisions of the Certification Practices and those of the regulations governing the provision of certificate services and Act 59/2003, where applicable.

2.1.2 RA

The Registration Authorities are delegated by the *AC* to exercise this function, consequent on which the RA is also bound by the terms set forth under the Certification Practices for certificate issuance.

2.1.3 Applicant

As required by the Certification Practice Statement (CPS). Consult http://www.acabogacia.org/doc

2.1.4 Subscriber

As required by the Certification Practice Statement (CPS). Consult http://www.acabogacia.org/doc

2.1.5 User

As required by the Certification Practice Statement (CPS). Consult http://www.acabogacia.org/doc

2.1.6 Certificate Register

As required by the Certification Practice Statement (CPS). Consult http://www.acabogacia.org/doc

2.2. Liability

In the performance of its activity of Certification Service Provider in its capacity as *AC*, the National Council of Spanish Bar Associations shall be responsible in accordance with the rules on liability set forth by Act 59/2003 governing electronic signatures and any other laws applicable thereto.

In accordance therewith, the *AC* shall be responsible in compliance with the Certification Practice Statement (CPS). Consult http://www.acabogacia.org/doc

2.2.1 Release from liability

The relations between the *AC* and the RAs shall be governed by the special contractual relations between both. The *AC* and the RAs shall be released from their responsibility in accordance with the terms set forth under the CPS and the certificate policies. In particular neither the *AC* nor the RAs shall on any account be liable under any of the following circumstances:

1. State of war, natural disasters or any other circumstance of force majeure.
2. The use of certificates when said use exceeds the provisions of the laws in force and the CPS, particularly the use of a certificate that has been suspended or revoked or when it is trusted without verifying beforehand the status thereof.
3. The unlawful or fraudulent use of the certificates or CRLs (Certification Revocation Lists) issued by the Certification Authority.
4. The unlawful use of the information contained in the certificate or the CRL.
5. Failure to comply with the obligations set forth for the subscriber or users by the laws in force, the CPS or this certificate policy.
6. The content of the messages or documents signed.
7. The failure to recover enciphered documents with the subscriber public key.
8. Fraud in the documentation submitted by the applicant.

2.2.2 Limitation of liability in the event of losses arising from transactions

The *AC* limits its responsibility in accordance with the Certification Practice Statement (CPS). Consult http://www.acabogacia.org/doc

2.3. Financial Responsibility

In the performance of its activity of Certification Service Provider, the *AC* has sufficient economic resources to cover any risk of liability for damages vis-à-vis the users of its services and third parties, thereby guaranteeing its responsibilities in its activity of CSP as required by the laws currently in force.

Said guarantee is covered by virtue of a Civil Liability Insurance Policy to cover an amount equal to or greater than € 3,000,000.

2.4. Interpretation and enforcement

2.4.1 Governing law

The interpretation, enforcement, amendment and validity of this Policy shall be governed by the laws of Spain currently in force.

2.4.2 Severability

Should any of the provisions set forth hereunder be found invalid, the rest of the document shall not be affected. In such event, the invalid provision shall be considered as not included.

2.4.3 Notifications

Any notification relating hereto shall be made by electronic post or registered letter sent to the address indicated in the sub-component on contact details.

2.4.4 Dispute resolution procedure

Any controversy or dispute that might arise herefrom shall be resolved definitively by the arbitration de jure of an arbitrator within the framework of the Spanish Court of Arbitration in accordance with the regulations and by-laws governing said court, to which shall be commended the administration of the arbitration and the appointment of the arbitrator or arbitration tribunal. The parties hereby place on record their undertaking to comply with the decision awarded.

2.5. Fees

2.5.1 Certificate issuance and renewal fees

The prices of certification services or any other related service shall be available for users at the different Registration Authorities.

2.5.2 Certificate access fees

Access to certificates issued shall be gratuitous, although the *AC* may charge a fee in cases of massive certificate downloading or under any other circumstance that, in the opinion of the *AC*, should be charged, in which case, said fees shall be published on the *AC*'s website.

2.5.3 Information access fees in respect of certificate or revoked certificate status

The *AC* shall provide access to the information relating to certificate or revoked certificate status free of charge by publishing the CRL. The *AC* may, however, charge a fee for other

means of checking certificate status or any other circumstance that, in the opinion of the *AC*, should be charged, in which case, said fees shall be published on the *AC*'s website.

2.5.4 Fees for other services

Fees for other services shall be published on the *AC*'s website.

2.5.5 Refund policy

No stipulation.

2.6. Certificate Publication and Registration

2.6.1 Publication of *AC* information

2.6.1.1 Certification policies and practices

This Certificate Policy and the different versions hereof are available to the public on the website http://www.acabogacia.org/doc

2.6.1.2 Terms and conditions

AC Abogacía shall place at the disposal of subscribers and users the terms and conditions of the service on the website http://www.acabogacia.org/doc

2.6.1.3 Dissemination of certificates

In accordance with the Certification Practice Statement (CPS). Consult http://www.acabogacia.org/doc

2.6.2 Frequency of publication

AC Abogacía shall publish forthwith any modification to the certification policies and practices while keeping a record of earlier versions.

AC Abogacía shall publish the certificates in the Certificate Register immediately after issuing them.

Ordinarily, the *AC* shall publish a list of certificates revoked ex oficio every 24 hours. *AC Abogacía* shall, on an extraordinary basis, publish a new revocation list as soon as an authenticated suspension or revocation request is processed.

2.6.3 Access controls

AC Abogacía shall use diverse systems for publishing and distributing certificates and CRLs. Certain access data shall be required to make multiple consultations.

On the website of *AC Abogacía* there shall be access points to the directory for CRL and certificate consultation under the control of a software application, which prevents the indiscriminate downloading of information.

The CRLs may be downloaded anonymously by http protocol.

2.7. Compliance Audits

As required by the Certification Practice Statement (CPS). Consult http://www.acabogacia.org/doc

2.8. Confidentiality and the Protection of Personal Data

As required by the Certification Practice Statement (CPS). Consult http://www.acabogacia.org/doc

2.8.1 Type of information to be kept confidential

The *AC* shall consider any information that is not expressly classified as public to be confidential. Information declared to be confidential shall not be disseminated without express written consent from the entity or organisation that indicated the confidential nature of such information unless by legal requirement.

2.8.2 Type of information considered to be non-confidential

The information indicated below shall be considered as non-confidential:

- The content of this Policy and the Certification Practices.
- The information contained in the certificates, since for the issuance thereof the subscriber gives his consent beforehand, including by way of illustration and not limitation:
    - The certificates issued or in the process of being issued.
    - The binding of the subscriber to a certificate issued by the Certification Service Provider.
    - In cases of individual certificates, the name and surnames of the subscriber of the certificate as well as any other circumstance or personal datum of the holder thereof in the event that this is significant in accordance with the purpose of the certificate.

- In cases of individual certificates, the electronic mail address of the subscriber of the certificate or, in cases of collective certificates, that of the holder of the keys or, in cases of device certificates, that designated by the subscriber.
- The uses and economic restrictions indicated in the certificate.
- The validity period of the certificate as well as the date of issuance and the expiry date thereof.
- The serial number of the certificate.
- The different certificate statuses and the commencement date of each one, particularly: pending generation and/or delivery, valid, revoked, suspended or expired and the reason for the change of status.

- The certificate revocation lists (CRLs) and any other information on revocation status.
- The information contained in the certificate repositories
- Any information the publication of which is required by law.

2.8.3 Dissemination of certificate revocation/suspension information

Information relating to the revocation or suspension of a certificate shall be disseminated by periodically publishing the corresponding CRLs. The details of this service shall be governed by the Certification Practice Statement (CPS).

2.8.4 Release to the Competent Authority

Information requested by the competent authority shall be provided under the circumstances and in the manner required by law.

2.9. Intellectual property rights

The intellectual property of these Policies belongs to the National Council of Spanish Bar Associations (CGAE). The *AC* shall be the only entity to enjoy the intellectual property rights over the certificates it issues.

The *AC* shall grant non-exclusive licences to reproduce and distribute certificates at no cost provided that the reproduction is integral and does not modify any element of the certificate, that it is necessary for digital signatures and/or encipherment systems within the scope of application of this policy and that it is compliant with the pertinent binding instrument between *AC Abogacía* and the party that reproduces and/or distributes the certificate.

The foregoing rules shall be indicated in the binding instruments between the *AC* and the subscribers and third relying parties.

3. Identification and Authentication

3.1. Initial register

3.1.1 Name types

All certificates require a distinguished name (DN) in accordance with standard X.501.

The DN of the Administrative Personnel certificates shall contain the elements in the format indicated below. All the values of the attributes shall be authenticated by the Registration Authority:

- A name component (Common Name) –CN
- An e-mail component –E
- An organisation component –O
- An organisational unit component –OU
- A title component -T
- A geographic location component -ST
- A state component (Country) -C
- A serial number component –serialNumber
- A first name component (Given name) - G
- A 1st surname component Surname – SN
- A 2nd surname component with OID 1.3.6.1.4.1.16533.30.1

Administrative Personnel certificates

- The authenticated value of the name component (Common Name) –CN shall contain the subscriber's name (Name and Surnames) and identity card number (NIF or NIE).
- The authenticated value of the e-mail component –E shall contain the subscriber's electronic mail address.
- The authenticated value of the organisation component –O shall contain the name of the institution to which the subscriber is bound, i.e., the Bar Association or Council of Bar Associations, and a reference to the identification code of the RA.

- The authenticated value of the organisational unit component –OU shall contain the Department or Unit to which the subscriber belongs.

- The authenticated value of the title component -T shall contain the subscriber's responsibility, title or role in the organisation.

- The authenticated value of the geographic name component -ST shall contain the town or city where the main headquarters of the AR are located.

- The authenticated value of the state component (Country)-C shall contain "ES"

- The authenticated value of the serial number component –serialNumber shall contain the subscriber's identity card number (NIF or NIE). In addition, a tax number component of the organisation shall be included, represented by the following OID (1.3.6.1.4.1.4710.1.3.2), which shall contain the tax number of the institution bound to the subscriber.

- The authenticated value of the first name component (Given name)- G shall contain the subscriber's first name.

- The authenticated value of the 1st surname component "Surname" –SN shall contain the subscriber's first surname

- The authenticated value of the component with OID 1.3.6.1.4.1.16533.30.1 shall contain the subscriber's second surname.

3.1.2 Pseudonyms

Administrative Personnel certificates may not contain pseudonyms. Neither may a pseudonym be used to identify an organisation.

3.1.3 Rules used for interpreting different name formats

Those set forth in standard X.500 referenced in ISO/IEC 9594 are followed.

3.1.4 Uniqueness of names

The distinguished names indicated in the certificates issued shall be unique to each subscriber. The AC shall make every endeavour that is reasonably within reach to confirm the uniqueness of the names in the certificates issued. The e-mail attribute, and/or the identity/tax card number shall be used to differentiate between identities when there might be a problem regarding name duplicity.

3.1.5 Name claim dispute resolution procedure

Certificate applicants shall not include names in requests that might involve an infringement of third party rights for the future subscriber.

The *AC* is not responsible in cases of name claim dispute resolutions. The Certification Service Provider shall not determine whether a certificate applicant has any right over the name that is indicated in a certificate request. Neither shall said provider act as arbitrator or mediator, nor in any other manner shall it resolve any dispute concerning the ownership of names of persons or organisations, domain names, trade marks or business names.

The Certification Service Provider reserves the right to refuse a certificate request due to a name claim dispute.

Names shall be designated according to their order of entry.

3.1.6 Recognition, authentication and role of trademarks

The AC shall not undertake commitments when issuing certificates in respect of the usage by subscribers of a trademark. Deliberate usage of a name, the use right over which is not the subscriber's property is not permitted. The AC, however, is not required to search for evidence of the ownership of registered trademarks prior to certificate issuance.

3.1.7 Methods to prove possession of private key

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

The test method for proving the subscriber's possession of the private key shall be PKCS#10.

3.1.8 Authentication of an individual's identity

For correct verification of the identity of the subscriber of personal certificates, said subscriber's appearance in person before the RA shall be required and the presentation of his national identity card, Spanish passport or residence card for foreigners to an operator or personnel duly authorised by the Registration Authority.

Additionally, the RA shall require certified evidence of authorisation from the applicant organisation in respect of the natural person (the subscriber).

The RA shall verify with its own sources of information the remaining data and attributes to be included in the certificate (distinguished name indicated in the certificate), while it shall keep the documentation accrediting the validity of data that it cannot check against its own data sources.

The stipulations of the foregoing paragraphs might not be required in cases of certificates issued subsequent to the coming into force of Act 59/2003 governing electronic signatures under the following circumstances:

a) When the identity or other permanent circumstances of certificate applicants are already on file with the RA due to a prior relationship in which the measures indicated in

paragraph one were taken to identify the person concerned and the period of time elapsed since this identification is less than five years.

b) When to request a certificate another is used for the issuance of which the signatory was identified in the manner set forth in paragraph one and the RA is satisfied that the period of time elapsed since this identification is less than five years.

3.1.9 Authentication of an organisation's identity

For correct verification of the identity of an organisation for the issuance of Administrative Personnel certificates, appropriate documentary evidence shall be provided to the Registration Entity unless the applicant organisation is the Bar Association itself or a Council of Bar Associations:

- The accreditation by reliable means of the existence of the entity in accordance with the law.

- The identity of the natural person representing the organisation for the request in accordance with component 3.1.8.

- The applicant organisations' binding relationship in respect of the RA, certified by an authorised representative of the RA.

3.1.10 Requirements applicable to external RAs

When the *AC* employs external RAs it must ensure the following:

- That there is a contract in force between the *AC* and the RA in which the specific aspects of the delegation and the responsibilities of each agent are set forth.
- That the identity of the RA and the RA's operators has been correctly checked and validated.
- That the RA's operators have been sufficiently trained to exercise their functions.
- That the RA assumes all of the obligations and responsibilities relating to the exercise of its functions.
- That communication between the RA and the *AC* is made in a secure manner through the use of digital certificates.

3.2. Certificate renewal

Certificate renewal shall consist in issuing a new certificate to the subscriber on the date on which the original certificate expires. Prior to renewing a certificate, the RA shall check that the information used to verify the identity of and the other data relating to the subscriber continues to be valid.

Should any information relating to the subscriber have changed, the new information shall be duly recorded.

3.3. Re-issuance after a revocation

As required by the Certification Practice Statement (CPS). Consult http://www.acabogacia.org/doc

3.4. Revocation requests

The suspension or revocation of a certificate may be requested by:

- The subscriber himself, in which case, he shall provide the revocation key that was delivered to him with the certificate or he shall identify himself to the RA in accordance with the stipulations of the pertinent sub-component.

- The operators authorised by the subscriber's RA.

- The operators authorised by the *AC* or the certification hierarchy.

In either of the latter two cases, the circumstances indicated in the pertinent sub-component of the CPS shall concur, and the revocation requests shall be submitted and processed in the manner described therein.

4. Operational Requirements

4.1. Certificate requests

The RAs manage requests for Bar Membership Certificates and Administrative Personnel Certificates.

Requests for a digital certificate may be made in either of the following manners:

- Online: Accessing the website http://www.acabogacia.org in the online application sub-component, the applicant may request his Registration Authority to issue a digital certificate and the system will send an electronic mail to the operators authorised by the RA, notifying this request. The RA then notifies the applicant of the disposition to process the registration.
- In person at the applicant's Bar Association before a duly authorised operator:

Prior to commencing the issuance process, the RA informs the applicant of said process, and the responsibilities and terms of use in respect of the certificate and the device while it verifies the applicant's identity and the data to be included in the certificate.

If the verification is correct, the legal instrument binding the applicant and the *AC* – RA is signed by virtue of which the applicant becomes a subscriber.

The RA delivers to the subscriber (should the latter not already have it) a kit containing the cryptographic device support for the private key and the access devices thereto, should there be any.

If the device has not been initialized beforehand, the subscriber initializes the cryptographic device at the RA itself in the presence of the operator. During the initialization process the data for activating the device and accessing the private key said device will contain are generated. The subscriber will generate the activation data, or if the device is initialised in an external entity, they will be delivered to him by a process that ensures confidentiality in respect thereof vis-à-vis third parties. The initialization of the device completely erases any prior information contained therein.

Then the subscriber generates the key pair and a CSR in his cryptographic device, sending the public key together with the data verified to the *AC* in PKCS10 format or another equivalent format over 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 associates it with the subscriber authorised to use said device.

4.2. Certificate issuance

The process followed for certificate issuance is as follows:

- The RA receives the request for certificate issuance.
- The RA's operator verifies the content of said certificate again and if the verification is correct he validates it and processes the approval of the issuance for the *AC* by digital signature of the request with his operator's certificate. If the request is not correct the operator refuses said request.
- The RA sends the request to the *AC* over a secure channel for the issuance of the pertinent certificate.
- If the request received does not contain technical errors in the format or content thereof, the *AC* issues the certificate while securely associating it with the registration information, including the certified public key, in a system that is protected against falsification and keeps the data interchanged confidential.
- The certificate generated is sent to the RA over a secure channel so that it can be downloaded on to the cryptographic device in the presence of the subscriber.
- The *AC* notifies the subscriber of the issuance of said certificate.
- The certificate generated is securely sent to the Certificate Register, which places it at the disposal of the users.

With the delivery of the collegial card the subscriber accepts his certificate in the cryptographic device that stores the private key.

4.3. Certificate acceptance

A subscriber is considered to have accepted his certificate when he downloads it on to the cryptographic device that stores his private key, by access to the *AC*-RA certificate download system, and implements the technical steps provided by the system for the download.

Without prejudice to the foregoing, the subscriber shall have a maximum period of seven calendar days to notify the RA of any fault in the certificate data or in the publication of the data thereof in the Certificate Register.

4.4. Certificate suspension and revocation

As required by the Certification Practice Statement (CPS). Consult http://www.acabogacia.org/doc

4.5. Security audit procedures

As required by the Certification Practice Statement (CPS). Consult http://www.acabogacia.org/doc

5. Physical, Procedural and Personnel Security Controls

As required by the Certification Practice Statement (CPS). Consult http://www.acabogacia.org/doc

6. Technical Security Controls

6.1. Key pair generation and installation

6.1.1 Subscriber key pair generation

Subscriber and operator keys are generated by the party concerned himself in a secure manner using a CC EAL4+, FIPS 140-1 level 2, ITSEC High4 cryptographic device or another of an equivalent level.

The cryptographic devices storing subscriber or operator private keys provide a security level equal to or exceeding that required by the laws in force governing signature-creation devices. The European regulation of reference governing subscriber devices is CEN CWA 14169.

The cryptographic device uses an activation key to access the private keys. In the event that the device is not delivered in person at the RA, the activation data are sent to the delivery point separately from the devices.

The keys are generated using the RSA public-key algorithm with the required parameters. The minimum key length is 1024 bits.

6.1.2 Delivery of the public key to the certificate issuer

The public key is sent to the *AC* for certificate generation by standard PKCS#10 format.

6.1.3 Delivery of the CA public key to users

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

6.1.4 Key size and validity period

6.1.4.1 Issuer key size and validity period

As required by the Certification Practice Statement (CPS). Consult http://www.acabogacia.org/doc

6.1.4.2 Subscriber key size and validity period

Subscriber private keys are based on the RSA algorithm and have a length of 1024 bits.

The public and private key usage period may correspond to the validity time horizon indicated in the certificates, but on no account may it exceed 3 years.

6.1.5 Public key generation parameters

No stipulation.

6.1.6 Parameter quality checking

No stipulation.

6.1.7 Hardware/software key generation

Subscriber and operator keys are generated by the subscriber himself in a secure manner, using a CC EAL4+, FIPS 140-1 level 2, ITSEC High4 cryptographic device or another of an equivalent level.

The cryptographic devices storing the private key of the subscriber or operator provide a security level equal to or exceeding that required by the laws in force governing signature-creation devices. The European regulation of reference governing subscriber devices is CEN CWA 14169.

The associated CA keys are generated in an nCipher nShield cryptographic module FIPS 140-1 level 3 compliant.

6.1.8 Key usage purposes

All certificates shall include the Key Usage extension, indicating the key usage authorised.

6.2. Private key protection

AC private key

As required by the Certification Practice Statement (CPS). Consult http://www.acabogacia.org/doc

Subscriber private key

The subscriber private key is stored in a cryptographic device and controlled and managed by the subscriber. It is protected by a system against access intents that will block the device when an erroneous access code is entered three times.

The subscriber has a device-unlock code. If this code is entered erroneously three times, the device becomes definitively blocked, rendering it useless.

6.3. Cryptographic module standards

In accordance with the Certification Practice Statement (CPS). Consult http://www.acabogacia.org/doc

6.3.1 Private key archival

The CA shall not archive the private key corresponding to certificate signatures and CRLs once the validity period of said key has expired.

The CA does not take custody of user private keys.

6.3.2 Entry of the private key in to the cryptographic module

There is a CA key ceremony document in which the private key generation processes and the use of cryptographic hardware are described.

6.3.3 Private key activation method

The subscriber private key is accessed by a PIN (see component 6.2).

The CA keys are activated by an m of n process. See component 6.3.1

6.3.4 Private key deactivation method

The subscriber private key becomes deactivated once the cryptographic signature creation device is removed from the reading device.

6.3.5 Private key destruction method

The CA private keys shall be destroyed in accordance with the procedures enabled by the HSM for this purpose.

6.4. Life cycle of cryptographic devices

6.4.1 Life cycle of secure signature-creation devices (SSCDs)

SSCDs shall comprise crypto-processor cards that enable the subscriber to generate and store the signature-creation data, i.e., the private key:

a) The cards are prepared and stamped by an external card provider.
b) The external card provider manages the distribution of the support, which it distributes to the registration authorities to be delivered personally to the subscriber. The RA may personalise images on the card.
c) The subscriber initializes the card and uses it to generate the key pair and to send the public key to the CA.

d) The CA sends a public key certificate to the subscriber, which is then entered in to the card.
e) The card is reusable and can securely store several key pairs.

The user cards have an average useful life of 6 years.

6.5. Security controls

As required by the Certification Practice Statement (CPS). Consult http://www.acabogacia.org/doc

6.6. Cryptographic module engineering controls

As required by the Certification Practice Statement (CPS). Consult http://www.acabogacia.org/doc

7. Certificate Profiles

7.1. Certificate profile

All of the certificates issued in accordance herewith comply with the standard X.509 version 3, RFC 3280 "*Internet X.509 Public Key Infrastructure Certificate and CRL Profile*", ETSI TS 101 862 known as "*European profile for Qualified Certificates"* and RFC 3739 (which replaces RFC 3039) "*Qualified Certificates Profile*". The provisions of standard TS 101 862 shall prevail in cases of contradiction.

All of the Administrative Personnel certificates described hereunder are **qualified certificates** in accordance with the provisions of section 11 of Act 59/2003, having the content required by section 11 of Act 59/2003, and issued in a device that is compliant with the definitions of section 24 of Act 59/2003. The certificates that correspond to qualified certificates are in compliance with the definition in clauses 5.2 and 5.3 of the technical specification TS 101 456 of the European Telecommunication Standards Institute (ETSI).

The qualified certificates shall include at least the following data:

a) An indication that they are issued as such.

b) The unique identity code of the certificate.

c) Identification of the CA that issues the certificate.

d) Identification of the subscriber in accordance with component 3.1.1. in the DN field of the certificate.

e) The commencement and termination of the certificate validity period.

f) The certificate usage constraints, if any.

g) The limits on the transaction value for which the certificate can be used, if any.

7.1.1 Profile description

The certificates shall be compliant with standard X509, defined in RFC 3280, and shall have the following fields described in this component:

FIELDS	
Version	V3
Serial number	(serial no., which shall be a unique code in respect of the issuer's distinguished name)
Signature algorithm	Sha1WithRSAEncryption
Issuer	CN = ACA – Collegial Certificates OU = Bar Association Certification Authority O = National Council of Spanish Bar Associations, tax number:Q-2863006I E = ac@acabogacia.org L = Madrid C = ES
Not before (notBefore)	(validity commencement date, UTC time)
Not after (notAfter)	(validity termination date, UTC time)
Subject	(In accordance with specifications of component **3.1.1**)
Public key	RSA (1024 bits)

7.1.2 Certificate extensions

The following extensions shall be included:

EXTENSIONS	
Issuer alternative name (IssuerAlternativeName)	Name RFC822=ac@acabogacia.org URL Address =http://www.acabogacia.org
Subject alternative name (SubjectAlternativeName)	Name RFC822=xxxx.xxxxx@cgae.es
Key usage (KeyUsage)	Digital signature, Non-repudiation, Key encipherment, Data encipherment, Key agreement
Extended key usage (ExtendedKeyUsage)	Client authentication (1.3.6.1.5.5.7.3.2) Secure mail (1.3.6.1.5.5.7.3.4)
Netscape certificate type (NetscapeCertType)	SSL Client authentication, SMIME (a0
URL of entity manager issuing Netscape certificates (netscape-ca-policy-url**)**	http://www.acabogacia.org/doc

Netscape comment (NetscapeComment)	This is a personal qualified certificate. Consult http://www.acabogacia.org/doc
Authority key identifier (AuthorityKeyIdentifier)	5a794ca10cfc08162cc285454f 32abe72b45c011
Subject key identifier (SubjectKeyIdentifier)	
Subject statement (SubjectStatement)	Certificate manager: Manager identifier=1.3.6.1.4.1.16533.10.3.1 [1,1]Manager qualifier information: Manager qualifier ID=CPS Qualifier: http://www.acabogacia.org/doc [1,2]Manager qualifier information: Manager qualifier ID=User notification Qualifier: Notification text=This is a personal qualified certificate. Consult http://www.acabogacia.org/doc
CRL distribution point (CRLDistributionPoint)	http://www.acabogacia.org/crl/acacorporativos.crl http://crl.acabogacia.org/crl/acacorporativos.crl
Basic constraints (BasicConstraints)	Subject type= End entity Path length constraint= None
Authority Information Access (Authority Information Access)	[1]Authority information access Access method=Certification authority issuer (1.3.6.1.5.5.7.48.2) Alternative 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

7.1.3 Algorithm object identifiers

The signature algorithm object identifier shall be:
1. 2. 840. 113549. 1. 1. 5 SHA-1 with RSA Encryption

The public key algorithm object identifier shall be:
1.2.840.113549.1.1.1 rsaEncryption

7.1.4 Name constraints

No stipulation.

7.2. CRL Profiles

7.2.1 Version number

The CRLs issued by the *AC* are version 2.

7.2.2 Issuance and validity period

They are issued ex oficio daily and when they suffer a change of status. They are valid for one week.

7.2.3 Publication.

They are published immediately after issue.

The distribution points are:

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

7.2.4 CRL and extensions

The following extensions shall be included:

Extensions
Version
Valid-From
Valid-To
Signature Algorithm
Serial Number
Distribution Points

8. Specification administration

8.1. Policies authority

The CGAE is responsible for formulating certification policies and it may be contacted at the address specified in sub-component 1.

8.2. Specification change procedures

Any proposed changes that might substantially affect the users of this policy shall be notified forthwith to the subscribers by publication on the website of *AC Abogacía*, making express reference in the home page to the existence of the change in question.

The users affected may submit their comments to the policy administration organisation within 45 days of the date on which the notification is received.

8.3. Publication and copy of the policy

A copy of this policy shall be available in electronic format at the website: http://www.acabogacia.org/doc. Earlier versions shall be withdrawn from online consultation, but may be requested by interested parties at the *AC Abogacía*.

8.4. Policy approval procedures

The publication of any revisions of this policy must be approved by the CGAE.

ANNEX 1: Technical information

Pursuant to the provisions of Act 59/2003 governing electronic signatures, 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 the mechanisms considered to be secure for signature creation and verification..

Subscriber devices

Prior to the request for the qualified certificate and the issuance thereof, the subscriber must have the corresponding data generating device for creating signatures.

A. Secure signature-creation devices:

The issuance of Qualified Certificates identified by the OID of policy 1.3.6.1.4.16533.10.3.1 require that the signature-creating data have been generated by the subscriber and are stored in a device that is compliant with the provisions of section 24.3 of Act 59/2003, which devices are called “secure signature-creation devices” (SSCDs)”.

The advanced electronic signature generated by said devices, based on a qualified certificate, is called “Qualified Electronic Signature” and, in respect of the data recorded electronically, ranks equally with the handwritten signature in respect of those set down on paper.

The AC considers the devices that comply with the conditions indicated below to be adequate:

- That they have been validated as such by the AC, for which a statement from the manufacturer or importer in respect thereof is required, together with the provision of the pertinent technical documentation and the execution of any tests that are deemed to be necessary during the validation process.
- That they have the pertinent device certificate pursuant to the provisions of section 27 of Act 59/2003, in which case they are definitively admitted.

B. Other signature-creation devices:

No stipulation

In both cases (A) and (B), the AC shall only issue certificates in response to requests that comply with the provisions of the sub-component below in respect of the key-generation algorithms and signature algorithm parameters considered to be satisfactory (RSA keys with a length of 1024 bits) even though the device might have the technical capacity to generate another set of signature parameters.

Signature creation and verification

Standards and parameters admitted

The correct use of the devices for creating electronic signatures considered to be secure is associated with the use of a subset of standards and parameters among those approved by the ETSI in the document "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures" ETSI SR 002 176 (www.etsi.org)

Signature suite entry index	Signature algorithm	Signature algorithm parameters (key length)	Key generation algorithm	Padding method	Cryptographic hash function
001	rsa	MinModLen=1020	rsagen1	emsa-pkcs1-v1_5	sha1
002	rsa	MinModlen=1020	rsagen1	emsa-pss	sha1
003	rsa	MinModLen=1020	rsagen1	emsa-pkcs-v1_5	ripemd160
004	rsa	MinModLen=1020	rsagen1	emsa-pss	ripemd160

The appropriate method for generating random numbers for the key generation algorithm of the table above is as follows:

Key generation algorithm	Signature algorithm	Random number generation (RNG)	RNG parameters
rsagen1	rsa	trueran or pseuran	EntropyBits≥128 or SeedLen≥128

Third parties that trust generated signatures must ensure that the signature received complies with the provisions of the foregoing paragraphs.

In the event that the signature-creation device enables different types of signatures to be created or the export of signature-creating data to another device that can generate electronic signatures with parameters other than those specified (such as a signatures with an "rsa" parameter, having an "md5" cryptographic hash function), subscribers and users are informed that said signatures may not be considered to be secure, while the former shall be responsible for ensuring that the rules above are complied with and the latter, that the signatures received are technically satisfactory.

Signature verification methods

It is essential to verify the electronic signature to ensure 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 guarantee that the message or document signed has not been modified since the electronic signature was generated.

This verification shall usually be done automatically by the verifying user's device, and in any event, in accordance with the CPS and the laws in force, while meeting the following requirements:

- An appropriate device must be used to check a digital signature against the algorithms and key lengths authorised in the certificate and/or to execute any other cryptographic operation necessary. Said devices must comply with the provisions of section 25 of the Spanish Electronic Signature Act.
- The certificate chain on which the electronic signature is based must be established while verifying and ensuring that the certificate chain identified is the most suitable for the electronic signature being checked. It is the verifying user's responsibility and decision to select the appropriate chain if more than one is possible.
- The integrity, the digital signature and the validity status (not expired, not revoked or not suspended) of all the certificates in the chain must be checked against the information provided by *AC Abogacía* by virtue of its certificate publication service. An electronic signature may only be considered to be correctly verified if each of the certificates in the chain is in order and valid.
- It must be verified that the certificates in the chain have been used in accordance with the terms and usage restrictions imposed by the issuer of each of them and by authorised signatories. Each certificate in the chain has information regarding its conditions of usage and links to documentation thereon.
- It must be verified that the signature algorithms and parameters of all the certificates in the chain correspond to those of the signed document itself.
- The date and the time the electronic signature was generated must be determined since correct verification requires that all the certificates in the chain were valid at the time the signature was generated.
- Lastly the data signed must be determined and the corresponding electronic signature must be technically checked against the certificate used to sign, associated with a valid certificate chain.

The user verifying a signature must act with the utmost diligence before trusting certificates and digital signatures and use an electronic signature verification device that has sufficient technical, operative and security capacity to check the signature correctly.

The verifying user shall be exclusively responsible for any harm that it might suffer consequent on the incorrect selection of the verification device unless said device is provided thereto by *AC Abogacía*.

The verifying user must bear in mind the certificate usage constraints indicated in any manner in the certificate, including those not processed automatically by the verification device and included therein by reference. Should circumstances require additional guarantees, the verifier must obtain these guarantees so that the trust is reasonable.

In any event, the final decision regarding whether or not to trust a verified electronic signature is taken exclusively by the user.

Long-term electronic signature verification

If the user wishes to have long-term guarantees to be able to check the validity of an electronic signature, it must use additional mechanisms including the following:

- Whether the signatory has generated the signature in a format capable of being verified over time, such as those defined in standard ETSI TS 101 733 "Electronic signature formats" of the European Telecommunications Standards Institute (www.etsi.org), which *AC Abogacía* recommends.
- Use by the signatory and the services verifier of mediation by third parties that both trust, such as:
    - Certificate validation services
    - Time-stamping services
    - Transaction sealing services
    - And so forth
- Conservation of the signature, in a secure and integral manner, together with all the data required for the verification thereof:
    - All the certificates in the certificate chain.
    - All the CRLs in force immediately prior to and subsequent to the generation of the signature.
    - The policies and practices in force at the time of the signature.

Annex 2: ACRONYMS

AC	Spanish acronym for Certification Authority, the English acronym (CA) is also used
ACA	Spanish Bar Association Certification Authority
RA	Registration Authority
ARL	Authority Revocation List (list of certificates that have been revoked, issued by the Root Certification Authority)
CGAE	National Council of Spanish Bar Associations
CPS	Certification Practice Statement
CRL	Certificate revocation list
CSR	Certificate Signing request
DES	Data Encryption Standard
DN	Distinguished Name (distinguished name in the digital certificate)
DSA	Digital Signature Algorithm
SSCD	Secure signature-creation device
FIPS	Federal information Processing Standard publication
IETF	Internet Engineering task force
ICA	Spanish Bar Association
ISO	International Organisation for Standardization
ITU	International Telecommunications Union
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
OID	Object identifier
PA	Policy Authority
CP	Certification Policy
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PUK	Personal Unblocking Key
RSA	Rivest-Shimar-Adleman
SHA-1	Secure Hash Algorithm
SSL	Secure Socket Layer (Protocol designed by Netscape and converted into a network standard, whereby encrypted information can be transmitted between an Internet navigator and a server)
TCP/IP	Transmission Control Protocol/Internet Protocol (Protocol system, defined within the framework of the IETF. The TCP Protocol is used for breaking data down into IP packets at source and assembling the packets at destination. The IP Protocol directs the data correctly to its recipient.