Autoridad de Certificación de la Abogacía

Consejo General de la Abogacía Española

Reference: **CPS_ACA_012.0**
Date: 01/10/2011
Document status: **Published**

# CPS_ACA_012.0
# CERTIFICATION PRACTICE STATEMENT OF THE SPANISH BAR CERTIFICATION AUTHORITY (*AC ABOGACÍA*)

(CPS_ACA_012.0)

# CPS

## CORPORATES CERTIFICATES

**CERTIFICATION PRACTICE STATEMENT OF THE SPANISH BAR ASSOCIATION CERTIFICATION AUTHORITY *(AC ABOCACÍA)***

## Change control

| Date | Version | Changes |
|---|---|---|
| 27/03/2003 | CPS_ACA_001.0 | Initial version |
| 02/03/2004 | CPS_ACA_001.1 | Corrigenda, Modification to AKI certificate extensions profile. Changes to CA certificate profile and CRL profile. |
| 26/10/2004 | CPS_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. |
| 17/08/2005 | CPS_ACA_002.1 | Updating of new root certificate. |
| 13/03/2006 | CPS_ACA_003.0 | Adaptation new Data Center environment |
| 13/07/2006 | CPS_ACA_004.0 | Inclusion of Legal Entity Certificates |
| 24/10/2006 | CPS_ACA_005.0 | Inclusion of Secure Server Certificates |
| 25/05/2007 | CPS_ACA_006.0 | Inclusion of Software Legal Entity Certificates |
| 02/03/2009 | CPS_ACA_007.0 | Fax number included as a contact<br>Details given of certificate renewal procedure<br>Details given of the process of notifying suspensions and revocations<br>Details given of the suspension procedure<br>Inclusion of Electronic Stamp Certificates |
| 02/09/2009 | CPS_ACA_008.0 | Inclusion of the CA Trusted, which depends on our hierarchy with the pertinent policies |
| 28/02/2010 | CPS_ACA_009.0 | Inclusion of software legal entity certificate policy under the CA Trusted |
| 01/10/2010 | CPS_ACA_010.0 | Inclusion of electronic stamp certificate policy under the CA Trusted |
| 21/12/2010 | CPS_ACA_011.0 | Inclusion of professional association personnel qualified certificate policy |
| 01/10/2011 | CPS_ACA_012.0 | Inclusion of European lawyer qualified certificate policy |

## Abstract of the fundamental rights and obligations contained under this CPS

THIS TEXT IS ONLY AN ABSTRACT OF THE COMPLETE CONTENT OF THE **CPS**. YOU ARE ADVISED TO READ THE ENTIRE TEXT AND THE OTHER RELATED DOCUMENTS TO OBTAIN A CLEAR VIEW OF THE OBJECTIVES, SPECIFICATIONS, STANDARDS, PROCESSES AND RIGHTS AND OBLIGATIONS GOVERNING THE PROVISION OF THE CERTIFICATION SERVICE.

- This CPS and the related documents govern all matters relating to the request, issuance, acceptance, renewal, re-issuance, suspension and revocation of certificates among other many essential aspects in respect of the life of the certificate and the legal relations that are established between the applicants/subscribers, the Certification and Registration Authority and the relying parties as well as third parties.

- Both the CPS and all the other related documents are available to future applicants, subscribers and users at the website http://www.acabogacia.org/doc so that prior to contracting with or trusting *AC Abogacía* they know exactly what the standards and rules applicable to our certification system are.

- *AC Abogacía* issues several types of certificates, consequent on which certificate applicants must understand the terms and conditions set forth under the CPS and the corresponding certification practices in respect of this type of certificate so that they may proceed correctly with the request and use of the certificate.

- Applicants must request the pertinent certificate in accordance with the procedure set forth under the CPS and the related documents.

- The custody of the private keys that subscribers must undertake in respect of their certificates is essential because if they do not take the appropriate measures, the security system we are endeavouring to implement would be futile. In this respect, *AC Abogacía* must be informed immediately when any grounds for certificate revocation/suspension set forth under the CPS arise, thereby proceeding with the suspension of said certificate to prevent its fraudulent use on the part of a non-authorised third party.

- Subscribers shall notify *AC Abogacía* of any modification to or variation in the data provided to acquire the certificate, whether or not they are named in the certificate in question.

- Subscribers must make correct use of the certificate and shall be exclusively liable for certificate usage in a manner other than that set forth under the CPS and the other related documents.

- It is a primordial obligation of users to check the certificate depositary published by *AC Abogacía* to ensure that the certificate they wish to trust and the other certificates in the trust chain are valid and have not expired or been suspended or revoked.

- The liability of *AC Abogacía* and the applicants, subscribers and users is set forth under this CPS and in the related documents as well as the limitation thereof in the event of any ruling on damages.

For further information, please consult our website at http://www.acabogacia.org or contact us at the following e-mail address: info@acabogacia.org

**Contents**

# 1. Introduction

## *1.1. Presentation*

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.

The National Council of Spanish Bar Associations is constituted as Certification Service Provider by virtue of creating its own PKI hierarchy.

### 1.1.1 Overview

This document sets out the Certification Practice Statement of the Certification Authority of the National Council of Spanish Bar Associations, comprising the Bar Association Certification Authority (*AC Abogacía*), governing the issuance of personal certificates, and it is based on the specifications of standard RFC 2527 – *Internet X. 509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework*, of ETSI.

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 for services, organisations and natural persons representing said organisations.

This CPS is consistent with the certificate policies regarding the different certificates issued by *AC Abogacía* that are identified in the sub-component on "Scope of Application and Uses" of this CPS. In the event of a discrepancy between the two documents, the provisions of the particular certification policies in respect of each type of certificate issued shall prevail.

*AC Abogacía*, governed by this CPS and the above-stated policies, hereby establishes the issuance of the following main classes of certificates:

1. BAR MEMBERSHIP QUALIFIED CERTIFICATES: These are certificates of national scope and collegial nature issued to end entities who are natural persons belonging to a Bar Association, that is, issued with the mediation of their Bar Association in its capacity as Registrar having the exclusive jurisdiction to certify a person identified in the certificate as having the status of "Bar member".
2. ADMINISTRATIVE PERSONNEL QUALIFIED CERTIFICATES: These are certificates of a collegial nature issued to end users who are persons bound functionally to Bar Associations, Regional Councils of Bar Associations and the National Council of Spanish Bar Associations, which act as Registrars, or to institutions bound to said Associations and Councils.
3. SECURE SERVER CERTIFICATES: These are certificates that identify and bind a certain URL to a given entity – a Bar Association, a Regional Council of Bar Associations or the National Council of Spanish Bar Associations – as well as any legal entity bound to the professional practice of Lawyer.
4. LEGAL ENTITY QUALIFIED CERTIFICATES: These are certificates of a collegial nature issued to end users that are legal entities having business relations with the Spanish Bar Associations or Bar Institutions.
5. SOFTWARE LEGAL ENTITY QUALIFIED CERTIFICATES: These are certificates of a collegial nature issued to Bar Associations, Regional Councils of Bar Associations and the National Council of Spanish Bar Associations.
6. PENALNET LAWYER CERTIFICATES: These are certificates of European scope and collegial in nature issued to end entities who are natural persons belonging to a

professional association, that is, issued with the mediation of their professional association in its capacity as Registrar, having the exclusive jurisdiction to certify a person indicated in the certificate as having the status of "lawyer" in accordance with Article 2 of Directive 98/5/EC (OJ No L 77 of 14th March 1998).

7. ELECTRONIC STAMP CERTIFICATES: These are certificates of a collegial nature issued to Bar Associations, Regional Councils of Bar Associations and the National Council of Spanish Bar Associations and, in general, to any legal entity that in any manner is bound to or related with the Bar professions.
8. PROFESSIONAL ASSOCIATION PERSONNEL QUALIFIED CERTIFICATES: These are certificates issued to end entities who are natural persons bound functionally to a professional Association or Council, and act as Registrars, or to institutions bound to said associations or councils.
9. EUROPEAN LAWYER QUALIFIED CERTIFICATES:
   These are certificates of European scope and collegial in nature issued to end entities who are natural persons belonging to a Bar Association.

The qualified certificates are such in accordance with the provisions of section 11 of Act 59/2003 governing electronic signatures, passed in Spain on 19th December 2003, while the use of a secure cryptographic device that complies with the definitions set forth in section 24 of Act 59/2003 is mandatory for generating and storing the subscriber's signature-creating data. In this respect signature creation is directly governed by Directive 1999/93/EC of the European Parliament and the Council of 13th December 1999 by virtue of which a Community framework for electronic signatures is laid down, covering any points not addressed by Act 59/2003 of 19th December 2003 governing electronic signatures.

In addition, for internal use only, to support the operations of the management system of the *AC* and the RAs, a series of specific certificates associated with the different roles of administration and operation shall be issued as well as certificates that enable secure communication between the system's different technical components. These certificates simply constitute a technical element required for the correct and secure management of the life cycle of the types of certificates indicated above.

This CPS describes the manner in which *AC Abogacía* meets all of the requirements and security levels exacted by the certification policies.

In respect of the content of this CPS, 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:** | CPS_ACA_012.0 |
| **OID** | 1.3.6.1.4.1.16533.10.1.1 |
| **Description:** | Certification Practice Statement of the Spanish Bar Association Certification Authority (*AC Abogacía*) |
| **Version:** | 012.0 |
| **Issuance date:** | 01/10/2011 |
| **Location:** | www.acabogacia.org/doc |

## *1.3. Community and Applicability*

### 1.3.1 Certification Authority (CA).

The entity responsible for issuing and managing the digital certificates is the National Council of Spanish Bar Associations (CGAE), which constitutes a certification system under the name of Bar Association Certification Authority (hereinafter *AC Abogacía*) with its own PKI hierarchy.

Information on the CA may be found at the website http://www.acabogacia.org

### 1.3.2 Certification Service Provider (CSP)

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

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

For the purpose hereof, the National Council of Spanish Bar Associations is the CSP in respect of issuing and publishing certificates and certificate revocation lists. *AC Abogacía* is the entity that issues end entity certificates and is responsible for certificate life cycle operations, although for certain operations, functions are delegated to the authorised Registration Authorities.

### 1.3.3 Registration Authority (RA)

For the purpose hereof, the entities listed below may act as RAs of the certificates:

a) The National Council of Spanish Bar (CGAE)
b) The Regional Councils of Spanish Bar
c) The Bar Councils (exclusive registrars for Bar Membership certificates)

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

In Spain, only Bar Associations may be Registrars for their members since said Bar Associations have the exclusive certifying capacity in respect of the status of lawyer.

### 1.3.4 Subscriber

This is the natural person or legal entity to whom a certificate is issued and who is identified in the distinguished name (DN) x501 of said certificate. In cases of qualified certificates issued to a natural person, the subscriber is also called "signatory".

In accordance herewith, digital certificates from *AC Abogacía* may be issued to the following natural persons and legal entities:

- In respect of Bar Membership certificates: persons belonging to a Bar Association in the capacity as resident members.

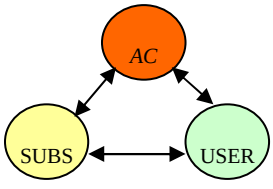
- In respect of Administrative Personnel certificates: persons belonging to a Bar Association or Council of Bar Associations in the capacity as employees or collaborators or bound thereto or to an entity bound to said associations or councils.

- In respect of legal entities: both Bar Associations and Councils or entities bound to the environment of the Spanish Bar institutions.

- In respect of European certificates: natural persons belonging to Bar Associations or a professional association in the capacity as lawyer in accordance with Article 2 of Directive 98/5/EC (OJ No L 77 of 14th March 1998).

### 1.3.5 User

In accordance herewith User is understood to be a third relying party, the person who voluntarily relies on the certificate from *AC Abogacía* by virtue of his trust in the *AC*. There is therefore a three-way trust circle.




### 1.3.6 Applicant

The applicant is the subject who is in a situation prior to obtaining the certificate and subsequent to the request thereof.

### 1.3.7 Scope of Application and Uses

This CPS implements the certificate policies indicated below, which are to be found at www.acabogacia.org/doc

| |
|---|
| Bar Membership Qualified Certificate Policy<br>(OID 1.3.6.1.4.1.16533.10.2.1) |
| Administrative Personnel Qualified Certificate Policy<br>(OID 1.3.6.1.4.1.16533.10.3.1) |
| Secure Server Certificate Policy<br>(OID 1.3.6.1.4.1.16533.10.4.1) |
| Legal Entity Qualified Certificate Policy<br>(OID 1.3.6.1.4.1.16533.10.5.1) |
| Software Legal Entity Qualified Certificate Policy<br>(OID 1.3.6.1.4.1.16533.20.2.1) |
| Electronic Stamp Qualified Certificate Policy<br>(OID 1.3.6.1.4.1.16533.20.3.1) |
| Penalnet Lawyer Qualified Certificates<br>( OID 1.3.6.1.4.1.16533.20.1.1) |
| Professional Association Personnel Qualified Certificates<br>( OID 1.3.6.1.4.1.16533.20.4.1) |
| European Lawyer Qualified Certificates<br>( OID 1.3.6.1.4.1.16533.10.9.1) |

The certificates from *AC Abogacía* may be used in accordance with the terms set forth under the corresponding certificate policies.

#### 1.3.7.1 Prohibited and Unauthorised Usage

The use of certificates is prohibited in accordance with the provisions of this CPS and the specific certificate policies pertinent hereto.

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 the certificate policies 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.

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

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 encrypted 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 key associated with the certificate.

## *1.4. Contact data*

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 of *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<br>Paseo de Recoletos, 13<br>28004 Madrid |

# 2. General Provisions

## *2.1. Obligations*

### 2.1.1 AC

The *AC* is bound by the provisions of sections 18, 19 and 20 of Act 59/2003 of 19th December 2003 governing electronic signatures, Directive 1999/93/EC of the European Parliament and the Council of 13th December 1999 and any other regulations governing the provision of certification services as well as the provisions of the certificate policies and this CPS. In particular, the *AC* undertakes to:

- Not store or copy the subscriber's signature-creating data when required not to do so by the laws in force.
- Provide the applicant prior to issuing the certificate at least the information indicated below, which shall be transmitted free of charge, in writing or electronically:
    - The signatory's obligations, the manner in which the signature-creating data are to be stored, the procedure for certificate revocation or suspension and the electronic signature creation and verification devices that are compatible with the certificate issued.
    - The mechanisms to guarantee the reliability of the electronic signature on a document over time.
    - The method used by the *AC* to check the signatory's identity and/or other data that are indicated in the certificate.
    - The precise conditions of certificate usage, usage constraints and the manner in which the *AC* guarantees the subscriber's personal liability.
    - The certificates obtained by the *AC*.
    - The procedures applicable for judicial and extrajudicial resolutions.
    - Any other information contained hereunder or under the Certificate Policies.
- Keep an updated certificate directory in which the certificates issued shall be indicated and whether they are valid or their validity has expired or been suspended.
- Implement reasonable security mechanisms to maintain the integrity of the certificate directory.
- Guarantee the availability of a prompt, secure consultation service on certificate validity.
- Suspend and revoke certificates in accordance with this CPS and to publish said revocations in the CRL (Certificate Revocation List).

- Inform subscribers duly and timely of the revocation or suspension of their certificates in accordance with the laws in force in Spain.
- Publish the Certification Policies and Practices on the *AC* website free of charge.
- Inform subscribers, RAs that are bound hereto and users of any amendments to this Certification Practice Statement by publishing the practices in question and the amendments thereto on its website.
- Guarantee that the date and time of the issuance, expiration or suspension of a certificate can be determined.
- Employ personnel with the qualifications, knowledge and experience required to provide the certification services offered by the *AC*.
- Use trustworthy systems to store qualified certificates that enable their authenticity to be checked and unauthorised persons to be prevented from modifying the data therein; that restrict access thereto under the circumstances or by the persons indicated by the signatory, and that detect any change that might adversely affect security conditions.
- Use trustworthy systems and products that are protected against all kinds of modification and that guarantee the technical and, where necessary, the cryptographic security of the certification processes which they support.
- Take measures against the forgery of certificates and guarantee their confidentiality during the generation process and secure delivery thereof to the signatory.
- Have a civil liability insurance policy that must cover at least the amount required by the laws in force.
- Keep the information in respect of the certificate issued for the minimum period required by the laws in force, when applicable.
- Issue certificates in compliance herewith and the standards applicable.
- Protect private keys in a secure manner.
- Issue certificates in accordance with the error-free information obtained from data entry.
- Issue certificates, the content of which is at least that required by the laws in force, where applicable.
- Protect signature-creating data while they are in its custody with due care when required.
- Abide by the provisions of the certification policies and practices.

### 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 Practice Statement for certificate issuance, primarily the following:

- To settle the fees established for the requested certification services.
- To abide by the provisions set forth hereunder.
- To check the identity of certificate subscribers and applicants. .
- To verify the accuracy and authenticity of the information provided by the applicant.
- To archive the documents provided by the subscriber for the period required by the laws in force.
- To abide by the provision of the contracts signed with the *AC*.
- To abide by the provisions of the contracts signed with the subscriber.
- To inform the *AC* of the grounds for revocation if they become aware of same.

### 2.1.3 Applicant

The applicant for a certificate shall be bound to comply with the provisions required by the laws in force and to:

- Provide the RA with the information necessary for correct identification
- Make the endeavours reasonably within his reach to confirm the accuracy and veracity of the information provided.
- Notify any change in the data provided for the creation of the certificate during the validity period thereof.

### 2.1.4 Subscriber

The subscriber of a certificate shall be bound to comply with the provisions required by the laws in force and to:

- Store his private key diligently.
- Use the certificate in accordance with the provisions hereof and the pertinent certificate policies.
- Abide by the documents signed with the RA.
- Inform as promptly as possible of the existence of any grounds for suspension/revocation.
- Notify any change in the data provided for the creation of the certificate during the validity period thereof.
- Not use the private key or the certificate from the moment the suspension or revocation thereof is requested or has come to the attention of the *AC* or the RA or once the term of the certificate has expired.

### 2.1.5 User

Users shall be bound to comply with the provisions required by the laws in force and to:

- Check the validity of the certificates at the time of executing any operation based thereon.
- Understand and abide by the guarantees, limitations and liabilities applicable to the acceptance and use of the certificates they trust.

### 2.1.6 Certificate Register

Any information relating to certificate issuance and status shall be made available to the public as required by the laws in force.

The *AC* shall maintain a secure certificate storage and recovery system as well as a Certificate Register of certificates issued and their status while it may delegate these functions to a third-party entity. Access to the Certificate Register shall be available from the website of *AC Abogacía* (www.acabogacia.org) or over another channel considered to be secure by the *AC*.

## *2.2. Liability*

In the performance of its activity of providing certification services in its capacity as CA, the National Council of Spanish Bar Associations (CGAE) shall be liable for failure to comply with the provisions of the certification policies and practices and, where applicable, by the provisions of Act 59/2003 governing electronic signatures of 19th December 2003, Directive 1999/93/EC of the European Parliament and the Council of 13th December 1999 and/or the regulations transposing same.

Without prejudice to the foregoing, the National Council of Spanish Bar Associations shall not guarantee the algorithms or cryptographic standards used nor shall it be liable for any damage caused by external attacks thereon provided that it has applied the due diligence in consonance with the state of the art at all times and has acted in compliance with the provisions of the certification policies and practices and Act 59/2003, Directive 1999/93/EC of the European Parliament and the Council of 13th December 1999 and the regulations transposing same.

### 2.2.1 Release from liability

The relations between the *AC* and the RA 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 this 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, this CPS or the corresponding certificate policy.
6. The content of the messages or documents signed or encrypted digitally.
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

In the performance of its activity of Certification Service Provider in its capacity as *AC*, the National Council of Spanish Bar Associations (CGAE) shall be liable in accordance with the rules governing liability laid down by Act 59/2003 governing electronic signatures, Directive 1999/93/EC of the European Parliament and the Council of 13th December 1999 and the remaining laws applicable thereto.

The *AC* shall be liable for any damage caused vis-à-vis the subscriber or any person who, in good faith, trusts the certificate provided that on the part of the *AC* itself, there is mens rea, breach or negligence in respect of the following:

1. The accuracy of all of the information contained in the certificate on the date of issue thereof.
2. The guarantee that on delivering the certificate, the subscriber shall have the private key corresponding to the public key designated or identified in the certificate.
3. The guarantee that the public key and the private key function jointly and complementarily.
4. The correspondence between the certificate requested and the certificate delivered.
5. Any liability that is established by the laws currently in force.

## *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 established 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 CPS shall be governed by the laws of Spain currently in force and Directive 1999/93/EC of the European Parliament and the Council of 13th December 1999.

### 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 the status of certificates or revoked certificates free of charge by publishing the CRL. The *AC*, however, reserves the right to 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 Registration and Publication*

### 2.6.1 Publication of information issued by the AC

#### 2.6.1.1 Certification Policies and Practices

This CPS and the different versions hereof are available to the public at 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 at http://www.acabogacia.org/doc

#### 2.6.1.3 Dissemination of certificates

Provided that the subscriber gives his consent for his certificate to be accessible, certificates issued may be accessed at the website http://www.acabogacia.org.

A repository of all the certificates issued shall be kept throughout the term the issuing entity continues to operate.

### 2.6.2 Frequency of publication

Certificate revocation lists shall be published in accordance with the provisions of the corresponding certificate policies.

*AC Abogacía* publishes forthwith any modifications to the certification policies and practices while keeping a record of earlier versions.

### 2.6.3 Access controls

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

The CRLs may be downloaded anonymously by http protocol from the URL addresses contained in the certificates, at the extension "*CRL Distribution Point*".

## *2.7. Compliance Audits*

### 2.7.1 Frequency of compliance audits

Compliance audits are conducted periodically.

### 2.7.2 Identification and qualification of the auditor

The compliance audits are conducted by a top class audit firm in accordance with the criteria of *WebTrust for Certification Authorities*, which may be downloaded from and consulted at *http://www.aicpa.org*, developed by the AICPA (*American Institute of Certified Public Accountants, Inc.*) and the CICA (*Canadian Institute of Chartered Accountants*).

The principles and criteria of WebTrust for CAs are consistent with the standards developed by the American National Standards Institute (ANSI) and the Internet Engineering Task Force (IETF).

### 2.7.3 Relationship between the auditor and the AC

The auditor shall be a well-known company of renowned prestige with departments specialising in system auditing while there shall be no conflict of interest that might distort its action in its relationship with *AC Abogacía*.

### 2.7.4 Fields covered by the audit

The audit shall check the following principles:

- Publication of information: That the *AC* publishes the Business Practices and Certificate Management (Policies and CPS) as well as information on the protection of personal data and that it provides its services in compliance with said affirmations.
- Integrity of service. That the *AC* keeps effective controls to reasonably ensure that:

a. The information provided by the subscriber is authenticated appropriately (for *AC* registration purposes).

b. The keys and certificates processed are integral and protected over all of their life cycle.

- General controls. That the *AC* keeps effective controls to reasonably ensure that:

a. The information on subscribers and users is only disclosed to authorised personnel and protected from uses that are not specified in the *AC* business practices published.

b. The continuity of the operations relating to key and certificate life cycle management is maintained.

c. The tasks of operation, development and maintenance of the *AC*'s systems are appropriately authorised and conducted to maintain the integrity thereof.

### 2.7.5 Audits of the Registration Authorities

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

### 2.7.6 Resolution of incidents

In the event that incidents or non-compliance are detected, the pertinent measures for the resolution thereof in the shortest time possible shall be implemented.

## *2.8. Confidentiality and the Protection of Personal Data*

The *AC* has an appropriate policy in respect of information processing and models of agreement that all the persons who have access to confidential information must sign.

The *AC* complies at all times with the laws in force governing the protection of personal data, particularly with the provision of Organic Law 15/1999 governing the protection of personal data, passed in Spain on 13th December 1999.

Pursuant to section 19.3 of Act 59 /2003 governing electronic signatures, this CPS shall be considered to be the "Security Document" for the purpose set forth in the legislation governing data protection and the laws implementing same.

### 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 released 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 CPS 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:
    a. The certificates issued or in the process of being issued.
    b. The binding of the subscriber to a certificate issued by the Certification Service Provider.
    c. 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.
    d. 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.
    e. The uses and economic restrictions indicated in the certificate.
    f. The validity period of the certificate as well as the date of issuance and the expiry date thereof.
    g. The serial number of the certificate.
    h. 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

The *AC* releases information relating to the suspension or revocation of a certificate by periodic publication in the pertinent CRLs.

There is a CRL and Certificate consulting service at http://www.acabogacia.org.

### 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 this CPS belongs to the CGAE.

*AC Abogacía* shall be the only entity to enjoy the intellectual property rights over the certificates it issues.

*AC Abogacía* grants a non-exclusive licence 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 statement, as defined in component 1, and that it is compliant with the pertinent binding instrument between *AC Abogacía* and the party that produces and/or distributes the certificate.

# 3. Identification and Authentication

## *3.1. Initial registration*

### 3.1.1 Name types

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

The DNs of the *ACA* certificates shall contain the elements stipulated under each Certificate Policy.

### 3.1.2 Pseudonyms

On no account may pseudonyms be used. Neither may pseudonyms be used to identify an organisation.

### 3.1.3 Rules used for interpreting different name formats

*AC Abogacía* always complies with the requirements of standard X.500 referenced in ISO/IEC 9594.

### 3.1.4 Uniqueness of names

The distinguished names indicated in the certificates issued shall be unique to each subscriber. The *AC* reserves the authority to not issue a certificate under the same name as that issued to another subscriber. The e-mail attribute, the association membership number and/or the identity card number shall be used to differentiate between identities when there might be a problem regarding duplicity of names.

### 3.1.5 Name claim dispute resolution procedure

Applicants for certificates 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 *AC* shall not determine that an applicant for certificates has any right over the name that is indicated in a request for a certificate. Neither shall the *AC* act as arbitrator or mediator, nor in any other manner shall it resolve any dispute concerning the ownership of names of individuals and organisations, domain names, trade marks or business names.

The *AC* reserves the right to refuse a request for a certificate due to a conflict of names.

Names shall be designated according to their order of entry.

The *AC* always complies with the provisions of component 2.4.4 of this CPS.

### 3.1.6 Recognition, authentication and role of trademarks

The *AC* does 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 by *AC Abogacía*. The *AC*, however, is not bound to search for evidence of the ownership of registered trademarks prior to certificate issuance.

### 3.1.7 Methods of proving private key ownership

The private key is generated by the subscriber and remains at all times in his exclusive possession. The subscriber creates the private and public key pair, and subsequently sends a request for the issuance of a valid certificate to *AC Abogacía*, which issues the certificate with the subscriber public key that is mathematically associated with the private key that the subscriber holds.

The test method for proving the subscriber's possession of the private key is PKCS#10 or an equivalent cryptographic test or another method approved by *AC Abogacía*.

### 3.1.8 Authentication of a person's identity

For correct verification of the identity of the subscriber of personal certificates, the *AC* requires the subscriber's physical presence.

In cases of legal entity certificates, the representative shall be required to appear in person before the RA and to present the national identity document, Spanish passport or residence card for foreigners to an operator or personnel duly authorised by the Registration Authority.

In cases of secure server certificates, the applicant shall not be required to appear in person before the RA.

In cases of European certificate issuance, the subscriber shall be required to appear in person for identification by any of the means that the State in which the Registration Authority is domiciled considers valid for the process.

In cases where the holder of a certificate requests the registration of any modification to his personal identification data in respect of his identity card, he shall present the pertinent certificate issued by the Register of Civil Status that recorded this variation.

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 Identity Authentication of the Registration Authority's Operators

The *AC* shall verify the aspects indicated below in respect of Registration Authorities that are concerted:

- 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's operators has been correctly checked and validated.
- That the RA's operators have been sufficiently trained to exercise their functions and that they have attended at least one operator training session.
- That the RA has been audited by an external entity designated by the *AC*.
- 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.

For correct identification of the operator, *AC Abogacía* shall require the operator to appear in person before an administrator, or a person authorised by the *AC*, and present the national identity document, residence permit, passport or another document that legally identifies the person. In addition, a document issued by a representative authorised by the Registration authority will have to be provided, accrediting the authorisation of the person to act in the capacity of operator of the Registration Authority.

## *3.2. Certificate renewal*

Certificate renewal consists in issuing a new certificate to the subscriber on the date on which the original certificate expires. Prior to renewing a certificate, the RA must ensure 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 must be duly recorded in accordance with component 3.1.8.

The subscriber shall be notified of the need for renewal sufficiently in advance before his certificate expires so that he may request the renewal thereof.

## *3.3. Re-issuance after a revocation*

The issuance of a new certificate to a subscriber after the certificate has been revoked shall be processed in accordance with component 3.1.8. In any event, the *AC* reserves the right to refuse re-issuance should the grounds for revocation relate to cases where the subscriber private key was compromised.

## *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 component 3.1.8.

- 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 component set forth hereunder shall concur, and the revocation requests shall be submitted and processed in the manner described therein.

# 4. Operational Requirements

## *4.1. Certificate requests*

The issuance of certificates shall be governed by the provisions of each Certificate Policy.

## *4.2. Certificate issuance*

The process to be followed for certificate issuance is established under each Certificate Policy.

## *4.3. Certificate suspension and revocation*

When a certificate is revoked it is no longer valid and this procedure is irreversible.

By contrast, when a certificate is suspended, the loss of validity is temporary and the process is reversible.

Revocations and suspensions take effect from the time they are published in the CRL.

Certificate revocations and suspensions shall be notified to the subscriber by electronic mail sent to the e-mail account that is indicated in the revoked or suspended certificate.

### 4.3.1 Reasons for certificate revocation

A certificate may be revoked for any of the following reasons:

1. Circumstances affecting the information contained in the certificate

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

   This reason for revocation may be requested by the user through the revocation code or the RA operator provided that there are well-grounded doubts about any of the circumstances indicated above.

2. Circumstances affecting the security of the *AC* private key or the certificate

   - Compromise of the *AC* private key or infrastructure or systems when the trustworthiness of the certificates issued after this incident is affected.

- Violation on the part of the *AC* or the RA of the certificate management procedures required by the CPS.

- Compromise or suspected compromise of the security of the subscriber key or certificate.

- Unauthorised access or usage by a third party of the subscriber private key.

- The irregular usage of the certificate by the subscriber.

- Failure to comply on the part of the subscriber with the certificate usage rules stipulated under the Policies, this CPS or the legal instrument binding the *AC*, the RA and the subscriber.

The reasons for revocation grounded on actions that might affect the root or intermediate CA may only be put forward by the *AC* administrators.

The reasons for revocation relating to user certificates may be put forward by the user through the revocation code or the RA operator provided that there are well-grounded doubts about any of the circumstances indicated above.

3. Circumstances affecting the security of the cryptographic device

- Compromise or suspected compromise of the security of the cryptographic device.

- Loss or disablement due to damage to the cryptographic device.

- Unauthorised access by a third party to the private key activation data.

- Failure to comply on the part of the subscriber with the cryptographic device usage rules stipulated under the Policies, this CPS or the legal instrument binding the *AC*, the RA and the subscriber.

The reasons for revocation grounded on actions affecting the cryptographic device in which the root or intermediate CA keys are kept may only be requested by the *AC* administrators.

The reasons for revocation relating to user certificates may be requested by the user through the revocation code or the RA operator provided that there are well-grounded doubts about any of the circumstances indicated above.

4. Circumstances affecting the subscriber

- Express, unequivocal statement by the subscriber or authorised third party.

- Termination of the legal relationship between the *AC*, the RA and the subscriber.

- Modification or termination of the underlying legal relationship or reason giving rise to the issuance of the certificate to the subscriber, including the temporary disqualification of the association member from the exercise of his profession.

- Violation by the applicant of the requirements pre-established for making the certificate request.

- Violation by the subscriber of his obligations, responsibilities and guarantees, as required by the pertinent legal instrument or the *AC*'s CPS.

- Total or partial incapacity suffered.

- Death of the subscriber.

The reasons for revocation relating to user certificates may be requested by the user through the revocation code or the RA operator provided that there are well-grounded doubts about any of the circumstances indicated above.

5. Other circumstances:

- Suspension of the digital certificate for a period exceeding that set forth under this CPS.

- Court or administrative ruling ordering the revocation.

- The concurrence of any other reasons specified under the CPS.

The reasons for revocation consequent on any of these circumstances shall be given by the operators authorised by the RA or the *AC* administrators provided that such reasons are well-grounded.

If the RA or the *AC* to whom the revocation request is addressed does not have all the information required to determine whether or not to revoke a certificate, but has indications that it might be compromised, it may decide to suspend it. When the subscriber is aware of the suspension of his certificate, he shall refrain from using it and contact the RA or the *AC* to have it revoked or to have the suspension lifted, if possible.

The legal instrument binding the *AC* and the RA with the subscriber shall require said subscriber to request the revocation of the certificate in the event that he becomes aware of any of the circumstances indicated above.

### 4.3.2 Who may request revocation?

The revocation of a certificate may be requested by:

- The subscriber himself, in which case, he shall submit the revocation key that was delivered to him with the certificate or identify himself before the RA as required by component 3.1.8.

- Authorised operators of the subscriber's RA provided that they have well-grounded reasons.

- Authorised *AC* administrators provided that they have well-grounded reasons.

### 4.3.3 Revocation request procedure

The revocation or suspension request procedure may be initiated in person or by telephone, or online from the website of *AC Abogacía*.

**In person procedure:**

- Request by the subscriber: The subscriber shall accredit his identity to an operator of his RA and shall state, in writing, his wish to have the certificate revoked or suspended. The operator shall proceed with the revocation or suspension, informing the subscriber of the completion of the process.

- Suspension by a third party: In the event that a third party makes the request, the operator will ask said party a series of questions to verify the accusation giving rise to the request, it shall receive the pertinent documentation and if it considers that the required reasons concur, it shall proceed with the suspension, which shall be precautionary until further investigations are made. It shall also send a message to the subscriber, notifying him of the circumstance.

**Online procedure:**

The subscriber of a Bar membership or employee certificate may access a webpage at www.acabogacia.org from which he may request the revocation of his certificate.
To do this, he shall:

- Access http://www.acabogacia.org
- Select: User area → Certificate management → Online revocation
- Key in the Revocation Code provided during the certificate generation process.

The certificate system.- As soon as the certificate has been revoked the subscriber shall be notified thereof while being indicated the time of revocation and the reason for same.

Revocation Management services shall be available 24 hours per day, 7 days per week. In the event of system failure or any other factor that is beyond the control of the *AC*, it shall make best endeavours to ensure that this service is not unavailable for longer than a maximum period of 24 hours.

Revocation status information shall be available 24 hours per day, 7 days per week. In the event of system failure or any other factor that is beyond the control of the *AC*, it shall make best endeavours to ensure that this information service is not unavailable for longer than a maximum period of 24 hours.

### 4.3.4 Revocation period

No stipulation

### 4.3.5 Suspension

Unlike revocation, when a certificate is suspended, the loss of validity is temporary and the process is reversible.

The decision whether or not to revoke a suspended certificate shall be taken by the RA or the *AC* within a maximum period of 30 calendar days. During this time the certificate shall be on hold.

*AC Abogacía* adopts a decision on the certificate status subsequent to the suspension (active, if the request or definitive revocation is not warranted), based on the information obtained hitherto regarding the reasons adduced for the revocation request.

If the RA or the *AC* to whom the revocation request is addressed does not have all the information required to determine whether or not to revoke a certificate, but has indications that it might be compromised, it may decide to suspend it.

The *AC* or the RA may suspend a certificate if a key is suspected to be compromised until this suspicion is confirmed or refuted.

Suspended certificates are published in the CRL giving the reason for revocation: "Certificate Hold (6)" (RFC 3280).

### 4.3.6 Who may request suspension?

The suspension of a certificate may be requested by:

- Authorised operators of the subscriber's RA provided that they have well-grounded reasons and as a precautionary measure.

- Authorised *AC* administrators provided that they have well-grounded reasons and as a precautionary measure.

### 4.3.7 Suspension request procedure

The subscriber shall go to an RA operator and ask for a suspension to be requested as a precautionary measure for a limited time period.

A third party that contacts an operator authorised by the *ACA*, either by telephone or in person, may request the suspension of a certificate, the operator shall ask a number of question to guarantee the legitimacy of the suspension and shall proceed to suspend it while contacting the certificate subscriber so that he may act in consequence.

### 4.3.8 Suspension period limits

The maximum certificate suspension period is 30 calendar days.

### 4.3.9 Frequency of CRL issuance

The root CA of the certification hierarchy of *AC Abogacía* shall issue a CRL each time a CA certificate is revoked. In any event it shall issue a CRL at least once a year.

The CA *ACA Certificados Corporativos* shall issue a new CRL each time it changes the status of a certificate of its hierarchy.

The CA, *ACA Trusted* shall issue a new CRL each time it changes the status of a certificate of its hierarchy.

In particular, a new CRL shall be issued immediately after a certificate status has been changed.

Revoked certificates that expire are removed from the CRL.

The *AC* shall keep a record of all CRLs and ARLs issued.

### 4.3.10 Obligation to check CRLs

Users must, of necessity, check the status of any certificates they are going to trust while, in any event, being bound to check the latest CRL issued, which may be downloaded from the URL addressed indicated in the certificate in question at the extension "CRL Distribution Point".

The CRL is signed by the certification authority that issued the certificate. Users must also check the pertinent CRL(s) in the certificate chain of the hierarchy.

Users shall check that the revocation list is the latest one issued since several valid revocation lists may be found at the same time. The certificates include the information required to access the CRL.

Users shall ensure that the revocation list is signed by the authority that issued the certificate that they wish to validate.

### 4.3.11 Availability of certificate status verification services

The *AC* provides an online revocation verification service, which shall be available 24 hours a day, 7 days a week. The *AC* shall make all endeavours necessary to ensure that this service is never continuously unavailable for over 24 hours.

### 4.3.12 Requirements for verification of certificate status

In order to cheque the status of a certificate, the user must know the subscriber's e-mail address associated with the certificate he wishes to verify.

### 4.3.13 Obligation to consult the certificate status checking service

Users that do not use the CRL to check the validity of a certificate must consult the Certificate Register before trusting said certificate.

### 4.3.14 Other forms of disseminating revocation information available

No stipulation.

### 4.3.15 Checking requirements for other forms of dissemination of revocation information

No stipulation.

### 4.3.16 Special revocation requirements due to compromise of keys

Should the *CA* keys be compromised, this event shall be notified insofar as possible to all the participants in the certification hierarchy.

## *4.4 Security Control Procedures*

### 4.4.1 Type of events recorded

*AC Abogacía* records and save logs of all the events relating to the *AC* security system. These include the following:

- System start-up and shut-down.
- Creation and deletion attempts, password sets or privilege changes.
- Attempts to initialise and end sessions.
- Unauthorised access attempts to the *AC* system over the network.
- Unauthorised access attempts to the *AC* internal network.
- Unauthorised access attempts to the archive system.
- Physical access to logs.
- Changes to the system configuration and maintenance.
- Records of the Certification Authority applications.

- Start-up and shut-down of the *AC* application.
- Changes to details of the *AC* and/or its keys.
- Changes to certificate profile creation.
- Generation of entity keys.
- Certificate life cycle events.
- Events associated with the use of the *AC* cryptographic module.
- Records of the destruction of the media that contain keys and activation data.

In addition, the *AC* keeps, whether manually or electronically, the following information:

- CA key generation ceremonies and key management data bases.
- Physical access records.
- System maintenance and configuration changes.
- Changes in personnel that perform *AC* trusted functions.
- Records of the destruction of material that contains key information, activation data or subscriber personal information, if this information is managed.
- Possession of activation data for transactions with the private CA key.

### 4.4.2 Frequency of processing audit logs

Audit logs shall be inspected each week and whenever there is a system alert caused by an incident, in search of suspicious or unusual activity.

### 4.4.3 Retention period for audit logs

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

### 4.4.4 Audit log protection

System logs are protected from manipulation by signing the files in which they are contained.

They are stored in fireproof devices.

Their availability is protected by storing them in facilities external to those in which the Certification Authority is located.

The devices are only handled by authorised personnel.

### 4.4.5 Audit log backup procedures

The *AC* has an appropriate backup procedure such that in the event of loss or destruction of important archives, the corresponding log backup copies are available within a short time period.

The *AC* has implemented a secure audit log backup procedure, while each week a copy of all the logs is made in an off-site medium. The off-site medium is stored in a fireproof safe under security control that guarantees that only authorised personnel have access thereto. Incremental copies are made daily and complete copies, weekly.

In addition, a copy of the audit logs is kept in an off-site custodial centre.

### 4.4.6 Audit information collection system

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

### 4.4.7 Notification to event-causing subject

No stipulation.

### 4.4.8 Vulnerability assessment

The *AC* revises discrepancies in the log information and suspicious activities in accordance with the internal procedure designed for the purpose thereof in the security policies.
Records archival

### 4.4.9 Type of events recorded

Any events that take place during the life cycle of the certificate are kept, including certificate renewal. The events listed below are stored by the *AC* or by delegation to the RA:

- All the audit data
- All data relating to certificates, including the contracts signed with subscribers and data relating to their identification
- Certificate issuance and revocation requests
- All certificates issued or published
- CRLs issued or certificate status records generated
- The documentation required by the auditors
- Communications between the PKI elements

The *AC* is responsible for the correct archival of all this material and documentation.

### 4.4.10 Retention period for archive

All the system data relating to the certificate life cycle shall be retained over the period required by the laws currently in force if applicable. Certificates shall be kept published in the repository for at least one year after the expiry thereof.

Contracts with subscribers and any information relating to a subscriber's identification and authentication shall be retained for at least 15 years or the period required by the laws currently in force.

### 4.4.11 Protection of archives

The *AC* shall ensure that archives are correctly protected by designating personnel qualified to process said archives and store them in fireproof safes and off-site facilities when required.

The *AC* keeps technical and configuration documents in which details are given of all actions taken to guarantee the protection of archives.

### 4.4.12 Archive backup procedures

The *AC* has an off-site storage facility to guarantee the availability of copies of the electronic file archive. The physical documents are stored in secure locations to which access is restricted exclusively to authorised personnel.

The backup records are signed to guarantee their integrity.

### 4.4.13 Requirements for time-stamping of records

There is a time server based on the NTP protocol to keep the different elements comprising the trustworthy certification systems synchronised.

List of synchronisation servers of the Acabogacia server:

hora.roa.es stratum 1
ntp.dgf.uchile.cl
time.xmission.com
clock.via.net
time.keneli.org

**Synchronisation**

When the ntpd demon is started up, the system reads the configuration files, among others.
The IP addresses or the referenced server names.
The maximum and minimum time interval between two consultations with these servers.

**Internal clock discipline**

Hourly information is requested from all the servers on the server list. In addition to the time, this information gives data relating to the travelling time of the packet in transit over the network, stability and server quality.

At the same time, if the system has run ntpd for a sufficient length of time in a prior session, it reads the latest correction that has to be made to the internal frequency of the clock to keep the time correct within an appropriate margin.

The time server calculates its time by counting the cycles completed by certain oscillators. These are supposed to have a frequency that might not be the correct one. NTP is capable of estimating their error and instructing the kernel to take this correction into account.

As time passes, the corrections made by ntpd are more reliable, the system becomes more stable and the interval between two time server consultations increases. The maximum error permitted of the system clock is 128 milliseconds.

If this limit is exceeded, the system reports itself unsynchronised again and the entire process commences as through from start-up. This does not usually happen; after two hours the time server has an error of around 2 milliseconds.

### 4.4.14 Audit information collection system

No stipulation.

### 4.4.15 Procedures to obtain and verify archive information

During the audit required by this CPS, the auditor checks the integrity of the archive information.

Only authorised personnel have access to archive information.

The *AC* provides the auditor with the information and the means to be able to check the archive information.

## *4.5 Key changeover*

Key changeover for users requires a new issuance process.

## *4.6 Key compromise and disaster recovery*

The *AC* has developed a contingency plan to recover all the systems within a maximum period of five days, though it ensures revocation and publication of information relating to certificate status in less than 24 hours.

Any fault in achieving the goals required by this contingency plan shall be treated as reasonably inevitable unless said fault is due to a failure to comply with the obligations of the *AC* to implement said processes.

### 4.6.1 Entity key is compromised

The *AC*'s contingency plan treats the compromise of the CA private key as a disaster.

Should the CA private key be compromised, the *AC* shall:

- Inform all the subscribers, users and other CAs with whom it has agreements or another type of binding relationship, at least, by publishing a notice on the *AC*'s website.
- Indicate that the certificates and information relating to the revocation status signed using this key are not valid.

### 4.6.2 Security facility after a natural or other type of disaster

The *AC* shall re-establish critical services (revocation and publication of revoked certificates) in accordance herewith within 24 hours of a disaster or unexpected emergency, taking as a base the contingency plan and continuity of existing business.

The *AC* has an alternative facility in the event of necessity to bring the certification systems into service.

## *4.7 AC termination*

Prior to the termination of its activity, the *AC* shall implement the following actions:

- Provide the funds necessary (by civil liability insurance) to continue finalising the revocation activities until the definitive termination of its activity, where necessary.
- Inform all the subscribers, applicants, users and other CAs or entities with which it has agreements or another type of relationship of the termination, giving prior notice of at least 2 months, or the period required by the laws in force at the time.
- Revoke all authorisation from entities subcontracted to act on behalf of the *AC* in the procedure of certificate issuance.
- Pursuant to section 21 of Act 59/2003 governing electronic signatures, the *AC* may transfer, with the express consent of the subscribers, the management of the certificates that continue to be valid on the date on which the termination occurs to another Certification Service Provider which will assume said certificates, or otherwise, terminate the validity of same. In the event of transfer to another provider, the *AC* shall inform of the characteristics of the provider to whom the transfer of the certificate management is proposed.

- Inform the competent government department, giving the prior notice indicated above, of the termination of its activity and the destination to be given to the certificates while specifying, as the case may be, whether the management is to be transferred and to whom.
- Prior to the definitive termination of its activity, the *AC* shall provide the competent government department with the information relating to the qualified certificates issued to the public, the validity of which has expired, so that said department takes charge of the custody thereof in accordance with the provisions of section 20.1.f) of Act 59/2003 and Directive 1999/93/EC of the European Parliament and the Council of 13th December 1999 on a Community framework for electronic signatures.

# 5 Physical, Procedural and Personnel Security Controls

## *5.1 Physical security controls*

The *AC* has physical and environmental security controls set up to protect the resources of the facilities in which the systems and equipment used for the operations are located.

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

- ✓ Unauthorised physical access
- ✓ Natural disasters
- ✓ Fire
- ✓ Failure of supporting utilities (electricity, telecommunications, and so forth)
- ✓ Flooding
- ✓ Theft
- ✓ Unauthorised removal of equipment, information, media and software relating to components used for the services pertinent to the Certification Service Provider.

The facilities are equipped with preventive and corrective maintenance systems with assistance 24h-365 days a year and within 24 hours of the request for help.

**Site location and construction**

The facilities are located in an industrial area, in the north of the metropolitan area of Madrid, next to one of the main business zones, 15 minutes from downtown Madrid and 15 minutes from the Madrid airport - Barajas. Access to the motorway and ring road junctions (M-30 and M-40) is some 500 metres from the building.

Given the high value of the communications and clients occupying the building, the data center building is included in the National Civil Emergency Plan of the Spanish Science and Technology Ministry.

### 5.1.1 Physical access

Physical access to the offices of the Certification Service Provider in which certification processes are conducted is restricted and protected by a combination of physical and procedural measures.

It is restricted to expressly authorised personnel with identification and logging on access, including closed circuit television double filming and archive.

The facilities are guarded by private security personnel.

Access to the rooms is controlled by identity card readers and managed by a computer system that keeps an entry and exit log.

### 5.1.2 Power and air conditioning

The centre is equipped with an alternating current feeding system, filtered and push-pull through two UPS in n+1 grade of redundancy, which provides power ranging from 400 to 2,000 W/m2, and a capacity of 7.5 to 25 MW without a single point of failure. In the system racks there are two redundant, separate power points: UPS1 and UPS2, distributed through copper coils that distribute a larger, more efficient electricity capacity to the building. In addition, there are diesel generators in n+1 grade of redundancy with autonomy of 48 hours and the diesel oil distributor is under contract to refill the tanks in less than 4 hours.

The centre is equipped with Heating, Ventilation and Air Conditioning (HVAC) systems. The HVAC system is based on the management of the indoor environment by water cooling, whereby a constant temperature of 21ºC +/- 5ºC is maintained with a relative humidity of 20% to 80%. The pumps and cooling units are located on the upper floor in n+1 grade of redundancy and without a single point of failure. Airflow around the building is also ensured by a redundant ring structure with leak detection sensors. There is an equally redundant air-conditioning and filtering system in each room.

### 5.1.3 Water exposures

The *AC*'s facilities are located in a low flood risk area.

### 5.1.4 Fire prevention and protection

Fire protection: The fire detection system comprises numerous optic sensors located in the ceiling and floor of each of the technical rooms. The system becomes operative as soon as more than two smoke detectors are activated and it is completely addressable for the entire building, enabling cross detection (in ceilings and raised floors). The fire suppression system enables automatic and manual discharge and is based on the total flooding of the office with F-13 gas, which is stored in outhouses separate from the building.

### 5.1.5 Media storage

Each removable storage medium (tapes, cartridges, disks, and so forth), that contains classified information is labelled with the highest classification level of the information it contains and remains exclusively at the hands of authorised personnel.

Information classified as confidential, regardless of the storage device, is kept in fireproof safes or under permanent lock and key, the removal of which requires express authorisation.

### 5.1.6 Waste disposal

When it is no longer of use, sensitive information is destroyed in the manner most appropriate to the medium in which it is contained.

Printed matter and paper: by shredders or waste paper baskets equipped for said purpose to be subsequently destroyed in a controlled environment.

Data storage media: they must be processed prior to being disposed of or reused to erase all data or be physically destroyed or the information contained therein must be made illegible.

### 5.1.7 Off-site backup

The *AC* has a secure off-site storage facility for the custody of documents and magnetic and electronic devices, which is separate from the operations centre.

At least two expressly authorised persons are required for the access, deposit or removal of devices.

## *5.2 Procedural controls*

### 5.2.1 Trusted roles

Trusted roles are those described under the respective Certificate Policies of the hierarchy such that a separation of functions is guaranteed which spreads control and limits internal fraud, while one single person is not permitted to control all the certification functions from beginning to end.

The specifications of standard CEN CWA 14167-1 require at least the following roles:

- **Security Officers:** having overall responsibility for administering the implementation of security policies and practices.
- **System Administrators:** authorised to make changes in the configuration of the system, but do not have access to the data thereof.
- **System Operators:** responsible for the day-to-day management of the system (monitoring, backup, recovery, and so forth).
- **System Auditors:** authorised to view system logs and to check the related procedures followed.
- **CA Officers – Certification Officers:** responsible for activating CA keys in the online environment.

- **Registration Officers**: responsible for approving, issuing, suspending and revoking end-entity certificates.

In particular:

The audit tasks may not be executed at the same time as the certification tasks, nor may the audit role and system role be performed by the same person.

Persons involved in System Administration may not exercise any activity in respect of audit or certification tasks.

### 5.2.2 Number of persons required per task

The *AC* guarantees at least two persons to perform the tasks that require multi-person control, which tasks are detailed below:

The tasks listed below require only one authorised person:

- Log reviews excepting CA logs
- Service restart excepting CA services
- Viewing of the CCTV recordings

The tasks listed below require at least a dual-control of persons in trusted roles:

- The activation of the CA private key for the issuance of CA certificates
- The activation of the CA private key for the change or creation of new certification profiles
- The activation of the root CA private key for ARL issuance
- CA log inspection
- Installation and updating of certification software
- Configuration of certification software

The tasks listed below require the control of at least three or more persons in trusted roles:

- CA key generation
- CA private key backup recovery

- The generation of new Operator Card Sets
- The erasure of Operator Card Sets

### 5.2.3 Identification and authentication for each role

The persons designated for each role are identified by the system auditor who ensures that each person performs the operations for which he is designated.

Each person only controls the assets necessary for his role, thereby ensuring that no person may access non-designated resources.

Resources are accessed depending on the asset by means of login/password, digital certificates, physical access cards and keys.

## *5.3 Personnel security controls*

### 5.3.1 Background, qualifications, experience and clearance requirements

All personnel who perform tasks classed as trustworthy have been working for at least four months in the production facility.

All personnel in trusted roles are qualified and have been trained appropriately to perform the operations designated to them.

The *AC* ensures that the registration personnel are trustworthy, from a Bar Association or from the body delegated to perform registration tasks. For said purpose a statement is required in respect thereof from the entity that assumes RA functions.

The Register's employee will have undergone a preparatory course for the execution of registration and request validation tasks. At the end of said course, an external auditor shall evaluate his/her knowledge of the process.

As a general rule the *AC* will remove an employee from trusted roles when it becomes aware of the existence of the commission of an unlawful act that might affect the performance of said employee's functions.

### 5.3.2 Background check procedures

The *AC* makes the pertinent investigations prior to contracting any person. The *AC* never designates trusted roles to personnel with a seniority of less than four months. The RAs may establish different criteria provided that they so request and that the *AC*, having studied the case, gives its approval.

### 5.3.3 Training requirements

The personnel who are designated trusted roles have been trained in accordance with the terms set forth under the certificate policy of the hierarchy.

### 5.3.4 Requirements and frequency of refresher training

The employees of the *AC* and the RAs undergo the required refresher courses to ensure the correct execution of the certification tasks, particularly when substantial modifications have been made to said tasks and at least once a year.

### 5.3.5 Job rotation frequency and sequence

No stipulation.

### 5.3.6 Sanctions for unauthorised actions

The *AC* and the Certification Service Providers (CSPs) have an internal sanctioning system against personnel who have performed unauthorised actions.

### 5.3.7 Contracting personnel requirements

Employees contracted to perform trusted roles shall sign the confidentiality clauses and the operational requirements used by the *AC* prior to filling said role. Any action that compromises the security of critical processes could give rise to sanctions.

### 5.3.8 Documentation supplied to the personnel

The *AC* shall place at the disposal of all personnel the documentation in which details are given of the functions entrusted, the policies and practices governing said processes and the security documentation.

In addition, it shall supply the personnel with the documentation they require at any time to be able to perform their functions competently.

# 6 Technical Security Controls

## *6.1 Key pair generation and installation*

### 6.1.1 Key pair generation

The CA key is generated in accordance with the documented key ceremony process in the CSP's cryptographic room by personnel in the pertinent trusted roles with, at least, dual control in the presence of witnesses from the organisation holding the CA and the external auditor.

The key of the delegated CAs is generated in a device that complies with the requirements of which details are given in FIPS 140-1 level 3.

The keys are generated using the RSA public-key algorithm.

The minimum CA key length is 2048 bits.

#### 6.1.1.1 Subscriber key pair generation

In the Bar Membership and Administrative Personnel Policies, the 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 and 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 Public key delivery to certificate issuer

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

### 6.1.3 CA public key delivery to users

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

The fingerprint of the CA digital certificate from the Spanish Bar Membership Certification Authority (*AC Abogacía*) which is covered by this CPS is:

For certificates issued prior to 2nd March 2004:

SHA -1: 8AA7 EB2C B5DD 1FB5 74BE 59B6 E66C 044B 6F5C AB72

MD-5: 47:24:B3:70:32:0C:22:8C:74:D5:E6:7A:41:79:FA:94

For certificates issued between 2nd March 2004 and 1st July 2005:

SHA -1: E529 15B5 B211 2B5E 2092 1051 CFE5 93AA 9422 1031

MD-5: 9C:FB:40:3F:25:D0:7C:29:4F:F0:20:37:4C:9B:74:C5

The fingerprint of the Root CA public keys corresponding to the CAs indicated above is:

SHA -1: A962 8F4B 98A9 1B48 35BA D2C1 4632 86BB 6664 6A8C

MD-5: 11:92:79:40:3C:B1:83:40:E5:AB:66:4A:67:92:80:DF

As from 1st July 2005 a new PKI hierarchy is in force.

The fingerprint of the certificate from the Root CA (Bar Association Certification Authority – *ACA*) in force as from 1st July 2005 is:

SHA-1: 7F8A 7783 6BDC 6D06 8F8B 0737 FCC5 7254 1306 8CA4

The fingerprint of the certificate from the delegated CA (*ACA Certificados Corporativos*) in force as from 1st July 2005 is:

SHA-1: 67B8 6CDB DEFD 4A8D F14A 6C14 46B1 EE04 3807 CB9B

The fingerprint of the certificate from the delegated CA (*ACA Trusted*) in force as from 2nd June 2009 is:

SHA-1: ac cf fc 6a 97 a9 73 df f7 db ee de 58 d6 e9 3c b3 20 53 98

Users may request the re-issuance of an authenticated printed copy of the foregoing data from the contact addresses indicated hereunder.

### 6.1.4 Key size and validity period

#### 6.1.4.1 Issuer key size and validity period

*ACA* uses keys based on the RSA algorithm having a key length of 2048 bits in CA certificates.

The private key usage period of the Root CA is 25 years. The private key usage period of the *AC Abogacía* CA is 12 years. The specific dates may be obtained from the CA certificates themselves.

The Root CA shall stop issuing certificates 12 years prior to the expiry of their validity period, and the *AC Abogacía* CA shall stop issuing certificates 3 years prior to the expiry of their validity period.

#### 6.1.4.2 Subscriber key size and validity period

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

The subscriber public and private key usage period may correspond to the validity time horizon indicated in the certificates, which shall be stipulated in each Certificate Policy, but on no account may it exceed 4 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

As required by the Certificate Policies (CPs). Consult http://www.acabogacia.org/doc.

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

### 6.1.8 Key usage purposes

The root CA and the intermediate CA shall include the following extensions in their certificates:

keyUsage = (critical) keyCertSign, cRLSign
netscapeCertType = SSL_CA, SMIME_CA, ObjectSigning_CA

## *6.2 Private key protection*

**CA private key**

The CA private key can only be accessed by two cryptographic devices protected by an access key, which devices are controlled by 2 of five possible persons. In addition, physical access to the devices requires the presence of a third person.

The CA private signature key is kept and used in a secure cryptographic device that complies with the requirements set forth in FIPS 140-1 level 3.

There is a backup system that recovers the CA keys in the event of destruction or HSM disablement, which may only be operated by authorised personnel in trusted roles, which control shall comprise at least three persons in said roles.

CA private signature key backup copies are stored in a secure manner. Details are given of this procedure in the *AC* security documentation.

**Subscriber private key**

The subscriber private key is controlled and managed by the subscriber, which key is equipped with a protection system against access intents.

## *6.3 Cryptographic module standards*

The cryptographic modules used by the issuing CA to end entities are validated by FIPS-140-1 level 3

### 6.3.1 Multi-person control (n out of m) of the private key

The CA private key can only be accessed by two cryptographic devices protected by an access key, which devices are controlled by 2 of five possible persons. In addition, physical access to the devices requires the presence of a third person.

### 6.3.2 Private key custody

On no account shall the *AC* store either the subscriber private key or that of the CA in the key escrow mode.

### 6.3.3 Private key backup copy

The *AC* has a backup system that reconstructs the CA private key in the event of its loss, making its recovery possible in cases of disaster, loss or deterioration thereof.

### 6.3.4 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 store user private keys.

### 6.3.5 Private key entry into cryptographic module

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

### 6.3.6 Method of activating private key

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

### 6.3.7 Method of deactivating private key

As required by the Certificate Policies.

### 6.3.8 Method of destroying private key

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

## *6.4 Other aspects of key pair management*

### 6.4.1 Public key archival

The *AC* shall retain all public keys over the period required by the laws in force, when applicable, or otherwise while the certification service is active and for at least another 6 months.

### 6.4.2 Usage periods for the public and private key

The usage period for a certificate shall be determined by its lifetime.

A certificate must not be used after its validity period although the relying party may use it to check historical data while bearing in mind that there will not be a valid online checking service for said certificate.

## *6.5 Life cycle of cryptographic devices*

### 6.5.1 Life cycle of cryptographic secure signature-creation devices (SSCDs)

As required by the Certificate Policies (CPs). Consult http://www.acabogacia.org/doc.

## *6.6 Computer security controls*

The *AC* uses trustworthy systems and commercial products to provide its certification services.

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

- Configuration of operating system security
- Configuration of software security
- Correct system dimensioning
- Configuration of users and authorisations
- Event log configuration
- Backup and recovery plan
- Network traffic requirements

The *AC*'s technical and configuration documentation gives details of the architecture of the equipment that provides the certification service in respect of both its physical and logic security.

### 6.6.1 Specific computer security technical requirements

Each of the *AC* servers includes the following functionalities:

- ✓ *AC* service access control and privilege management
- ✓ Enforcement of task separation for privilege management
- ✓ Identification and authentication of roles associated with identities
- ✓ Archival of subscriber and CA history and audit data
- ✓ Security-related events audit
- ✓ Security self-diagnostics in respect of *AC* services

- ✓ CA key and system recovery mechanisms

The functionalities indicated above operate by virtue of a combination of operating system, PKI software, physical protection and procedures.

### 6.6.2 Computer security rating

The security level of the equipment is reflected by an initial risk analysis such that the security measures implemented respond to the likelihood and impact produced when a group of defined threats could take advantage of security breaches.

Physical security is guaranteed by the installations defined further above and personnel management.

## *6.7 Security life cycle controls*

### 6.7.1 System development controls

The *AC* follows a change control procedure for operating system and application versions that improves their security functions while correcting any vulnerability detected.

### 6.7.2 Security management controls

#### 6.7.2.1 Security management

The *AC* develops specific activities for employee training and awareness-building in respect of security. The materials used for training and the documents describing the processes are updated after they have been approved by a security management forum.

The *AC* requires by contract equivalent security measures of any external provider involved in certification tasks.

#### 6.7.2.2 Asset and information classification and management

The *AC* keeps an inventory of assets and documentation and implements a procedure for managing this material to guarantee its correct usage.

The *AC*'s security policy gives details of the information management procedures to be followed, into which said information is classified according to its level of confidentiality.

Documents are classified at three levels: PUBLIC, INTERNAL USE and CONFIDENTIAL.

#### 6.7.2.3 Management operations

The *AC* follows an appropriate incident management and response procedure by implementing an alert system and periodic reporting. The *AC* security document gives a detailed account of the incident management process.

The *AC* has fireproof safes for storing physical media.

The *AC* follows the entire procedure relating to the functions and responsibilities of the personnel involved in the control and handling of elements comprising the certification process documented.

**Media handling and security**

All media shall be handled securely in accordance with requirements of the information classification procedure. Media containing sensitive data are securely disposed of when they are not going to be required again.

**System planning**

The *AC*'s technical department keeps a record of equipment capacities.

In combination with implementing resource control for each system, a possible re-dimensioning may be considered.

**Incident reporting and response**

The *AC* follows a procedure for monitoring incidents and their resolution by virtue of which the pertinent response is recorded as well as the cost of resolving the incident.

**Operational procedures and responsibilities**

The *AC* defines activities designated to persons in trusted roles that are different from those of persons in charge of performing everyday operations that are not confidential in nature.

#### 6.7.2.4 System access management

The *AC* makes every endeavour reasonably within its reach to verify that system access is restricted to authorised persons. In particular:

**AC General**

a) There are high availability firewall- based controls.

b) Sensitive data are protected by cryptographic techniques or access controls requiring strict identification.

c) The *AC* has a documented procedure to be followed for user account management and access policy, details of which are given in its security policy.

d) The *AC* follows a procedure to ensure that the operations are undertaken in accordance with the trusted role policy.

e) Each individual is associated with his identifier before undertaking certification operations according to his trusted role.

f) The *AC* personnel shall be accountable for their activities, for example, by keeping event logs.

**Certificate generation**

The *AC* facilities are equipped with continuous surveillance and alarm systems to be able to detect, record and react immediately upon any unauthorised and/or irregular attempts to access its resources.

The authentication required to undertake the certificate issuance process is done by an m of n operator control system to activate the *AC* private key.

**Revocation management**

The *AC* facilities are equipped with continuous surveillance and alarm systems to be able to detect, record and react immediately upon any unauthorised and/or irregular attempts to access its revocation system.

Revocation refers to the permanent loss of effectiveness of a digital certificate. The log systems shall generate the tests that guarantee the non-repudiation of the action undertaken by the CA operator.

**Revocation status**

Revocation status application enforces access control based on certificate authentication to prevent attempts to modify revocation status information.

#### 6.7.2.5 Cryptographic hardware life cycle management

The *AC* ensures that the cryptographic hardware used for certificate signing is not manipulated during transport.

The cryptographic hardware is constructed on supports prepared to prevent any kind of manipulation.

The *AC* records all the pertinent information on the device to add to the provider's catalogue of assets.

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

The *AC* conducts periodic testing to ensure that the device is functioning correctly.

The cryptographic device is only handled by personnel in trusted roles.

The AC private signature key stored in the cryptographic hardware shall be eliminated once the device has been withdrawn.

The configuration of the *AC* system and its modifications and updating are documented and controlled.

The *AC* has a device service contract for the correct maintenance of the device. All changes or updates are authorised by the security officer and are recorded in the corresponding work minutes. These configurations are executed by at least two persons in trusted roles.

### 6.7.3 Life cycle security rating

No stipulation.

## *6.8 Network security controls*

The *AC* protects physical access to the network management devices and it has an architecture that orders the traffic generated based on its security characteristics while creating clearly defined network sections. This division is made by firewall usage.

Confidential information transferred over unsecure networks is encrypted.

## *6.9 Cryptographic module engineering controls*

### 6.9.1 *AC* cryptographic modules

**Cryptographic device storage:**

For the purpose of preventing unauthorised manipulation of the cryptographic module, it is stored in a secure location with the following characteristics:

- There is an inventory that controls device handling, entry and removal
- Access to the device is limited to personnel in trusted roles.
- Failed access attempts are recorded in a system log that manages the device.
- There is an incident and unusual event management procedure in respect of device usage, giving rise to a subsequent investigation and the pertinent incident reporting.
- Correct hardware functioning is checked by manufacturer test procedures at least once a week.

- The cryptographic device is handled in the presence of at least two employees in trusted roles.
- The cryptographic device is protected with handling detection mechanisms.

**Cryptographic device installation:**

The cryptographic device is installed in the presence of at least two employees in trusted roles.

**Cryptographic device repair:**

The cryptographic device shall be repaired in accordance with the terms stipulated under the service contracts in force with the original device provider. The initial test and functioning control procedures shall be executed once the device has been recovered.

A device in a test environment shall never be used in a production environment unless it is initialised such that it is in the identically same condition as it would be in if it were received new.

**Cryptographic device withdrawal:**

The cryptographic device shall be withdrawn in the presence of at least two employees in trusted roles.

In cases of permanent withdrawal the handling control mechanisms shall be destroyed. The device shall be stored in a protected location until it is destroyed.

**Cryptographic device re-usage:**

A cryptographic device may be reused provided that it is initialised such that it is in the identically same condition as it would be in if it were received new.

# 7 Certificate and CRL profiles

## *7.1 Certificate profile*

### 7.1.1 Preamble

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[1] 3039 (replaced) and 3739 "*Qualified Certificates Profile*". The provisions of standard TS 101 862 shall prevail in cases of contradiction.

All of the collegial certificates defined 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).

**Clarifications on the "x509v3 KeyUsage" extension:**

RFC 3280 that defines the profiles of X509 certificates replaces RFC 2459 due to obsolescence. An important change is that the key usage "digital signature", as defined in RFC 3280, is not asserted as usage suited to digital signatures for security services other than "non-repudiation", as expressed in the corresponding clause of RFC 2459.

In coherence with the earlier RFC 2459, RFC 3039 required that if the usage asserted as "non-repudiation" was present, it should be set exclusively and not combined with any other key usage. The change indicated above generated a request to the ITU to correct the error and harmonise 3039 with the new RFC 3280.

RFC 3739 "Qualified Certificates Profile" (March 2004, replacing RFC 3039) does not give an opinion in the section corresponding to the key usage "non-repudiation", but refers to the CSP policies or specific legal requirements governing the scope of issuance while considering the possible risks of combining the key usage "non-repudiation" with other key usage.

Moreover, the functionality of non-repudiation is achieved by applying the digital signature mechanism to the data the object of signature, and by the existence of a non-repudiation service or application. This service shall require the existence of the key usage "non-repudiation" in the signatory's certificate as well as the application of

[1] Idem

additional mechanisms (such as time stamps issued by a Time-Stamping Authority, OCSP validation, and so forth), according to the pertinent technical standards.

### 7.1.2 Profile description

All certificates shall have the content and fields described in this section including, at least, the following:

| **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<br>OU = Bar Association Certification Authority<br>O = National Council of Spanish Bar Associations, tax number:Q-2863006I<br>E = ac@acabogacia.org<br>L = Madrid<br>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**) |

### 7.1.3 Version number

The *AC* issues X.509 Version 3 certificates.

### 7.1.4 Certificate extensions

Those set forth under the pertinent PC shall be applied.

### 7.1.5 Object identifiers (OIDs) of the algorithms

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

The public key algorithm object identifier is:
1.2.840.113549.1.1.1 rsaEncryption

### 7.1.6 Name constraints

No stipulation.

## *7.2 CRL profile*

The CRL profile is that proposed in the pertinent certificate policies according to standard X.509 version 3 of RFC 3280 "*Internet X.509 Public Key Infrastructure Certificate and CRL Profile*". The CRLs are signed by the certification authority that issued the certificates.

### 7.2.1 Version number

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

### 7.2.2 CRL and extensions

Those stipulated under each CP shall be applied.

# 8 SPECIFICATION ADMINISTRATION

## *8.1 Policies authority*

The Operations Department of *AC Abogacía* is responsible for administering the CPS. Please contact:

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

| | |
|---|---|
| **Email:** | info@acabogacia.org |
| **Telephone:** | 902 41 11 41 |
| **Address:** | Consejo General de la Abogacía Española<br>Paseo de Recoletos, 13<br>28004 Madrid |

## *8.2 Specification change procedures*

### 8.2.1 Elements that may be changed without required notification

The only changes that may be made to this policy without requiring notification are typographic or editing corrections or changes in contact details.

### 8.2.2 Changes requiring notification

#### 8.2.2.1 List of elements

Any elements of this CPS may be changed unilaterally by *AC Abogacía* without prior notice. Any amendments hereto must be justified from a legal, technical and/or commercial viewpoint.

#### 8.2.2.2 Notification mechanism

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.

#### 8.2.2.3 Notification period for comments

Affected users may submit their comments to the policies administration organisation within 45 days of receiving the notification.

#### 8.2.2.4 Mechanism to receive, review and incorporate the comments

Any action taken consequent on comments is at the discretion of the policy authority (PA).

## *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 may be withdrawn from online consultation, but can be requested by interested parties at *AC Abogacía*.

Users may request a printed copy of the CPS at the contact address of *AC Abogacía*.

## *8.4 CPS approval procedures*

The publication of any revisions of this CPS shall be approved by *AC Abogacía*, after complying with the prerequisites required by the National Council of Spanish Bar Associations.

# Annex 1: Security Document (Organic Law governing the protection of personal data - "LOPD")

**PREAMBLE**

The National Council of Spanish Bar Associations shall protect the files containing personal data required to undertake the activity of providing digital certificate services pursuant to Organic Law 15/1999 governing the protection of personal data (LOPD), passed in Spain on 13th December 1999, the regulation governing security measures, approved by Spanish Royal Decree 994/1999 (RD 994/1999) of 6th June 1999, and any other laws applicable thereto. Said files shall be owned privately and the creation, modification or erasure thereof shall be notified to the Spanish Agency for the Protection of Personal Data by the mechanisms authorised for said purpose.

For the effective provision of said certificate service, subscribers are required to facilitate with truthful information all the data necessary for certificate issuance. Said data are collected for this purpose and the applicant, future subscriber, gives his consent to the processing thereof for the usage and purposes established. In accordance with the provisions of said law, the personal data contained in the files correspond to the basic level.

To undertake the CSP activity itself and for the correct functioning of the service, different external entities must have access to the data, particularly the Registration Authorities as well as the different providers that collaborate in providing the service. The National Council of Spanish Bar Associations shall, in any event, be the file manager, while the other entities shall be processing managers, exclusively for the purposes set forth hereunder and they undertake to process said data in accordance with the instructions of the National Council of Spanish Bar Associations, to not disclose them to third parties and to destroy or return them once their relationship with the National Council of Spanish Bar Associations has terminated, excepting the data that must be kept in accordance with the laws currently in force in Spain governing electronic signatures.

Users (third relying parties) may consult the data contained in the certificates and the validity status in the certificate directory, of public access, pursuant to the provisions of Act 59/2003 governing electronic signatures. Users may only use the information to check the validity of the certificate or the signatures generated in accordance with the laws in force, this CPS and the Certificate Policies. We make the general warning that any processing, recording or usage for purposes other than those indicated above requires, of necessity, the prior consent of the data owners. The LOPD sanctions with fines of up to SIX HUNDRED THOUSAND EUROS (€ 600,000) each of the violations or failures to comply with said law, without prejudice to the institution of criminal proceedings in accordance with the Spanish Criminal Code as well as civil actions brought by damaged parties.

The data owners may exercise their rights of access, rectification, erasure or opposition before the National Council of Spanish Bar Associations at the email address indicated at http://www.cgae.es while referencing the notification as "PERSONAL DATA", without prejudice to the obligations of keeping certain data as required by Act 59/2003 governing electronic signatures.

## A. SCOPE OF APPLICATION OF THE SECURITY DOCUMENT

The purpose of this document, an inseparable part of the CPS of *AC Abogacía*, is to establish the technical and organisational measures required to guarantee the security that the computer files must have as well as the premises, equipment, systems and the persons that are involved in the computer processing of personal data.

Details are given in the CPS of the measures, procedures, rules and standards directed at guaranteeing the level of security required by the aforementioned laws for the purpose of guaranteeing the security of personal data, for which this institution is responsible.

In addition, general security measures applicable to any other information system in use at the National Council of Spanish Bar Associations are established even though said system is not included among the systems that directly support the provision of the certification services.

Compliance with the CPS, of which this Security Document forms part, is required of all the personnel of this institution. All of the personnel of this institution have been informed of the internal rules set forth hereunder so that there is due compliance with the requirement of section 9.2 of Royal Decree 994/1999, passed in Spain on 11th June 1999.

## B. FUNCTIONS AND OBLIGATIONS OF THE PERSONNEL

In respect of the use and processing of personal data, the National Council of Spanish Bar Associations establishes two differentiated functions:

**File Manager**. The file manager, who may delegate some of the tasks to the security officer, has the following functions:

1. To notify the Data Protection Agency of the personal data files kept in the National Council of Spanish Bar Associations.
2. To ensure compliance with all the requirements of Organic Law 15/1999 of 13th December 1999 governing the protection of personal data and Royal Decree 994/1999 of 11th June 1999 approving the Regulation governing security measures in respect of automated files that contain personal data and compliance with the security standards set forth in the security document.
3. To draw up, enforce and check the application of and compliance with the security document.
4. To establish the criteria to be followed by the security officer when performing the function of granting, changing or annulling authorised access to data and resources.

5. To establish the mechanisms necessary to prevent users from accessing data or resources with rights other than those authorised.
6. To keep the incident record updated.
7. To authorise the removal of media that contain personal data.
8. To appoint one or several security officers, in charge of coordinating and controlling the measures described in the security document. On no account does this appointment involve a delegation of the responsibility corresponding to the file manager.
9. To adopt the appropriate corrective measures in accordance with the analysis of the audit reports issued by the security officer.

**Security Officer**. The security officer is entrusted with the following functions:

1. To ensure compliance with the security standards set forth in the security document.
2. To compile and describe the security measures, procedures, rules and standards adopted by the National Council of Spanish Bar Associations.
3. To determine and describe the computer resources to which the security document shall be applied.
4. To establish and check the incident notification, processing and recording procedure application.
5. To establish and check data backup and recovery procedure application.
6. To check compliance with the frequency established for making backup copies.
7. To compile and keep updated the list of users that have authorised access to the computer system of the National Council of Spanish Bar Associations, specifying the access level that each user has.
8. To establish and check user identification and authentication procedure application.
9. To establish and check password designation, distribution and storage procedure application.
10. To check, insofar as possible, the maintenance of the confidentiality of user passwords.
11. To establish and check the application of the procedure for periodically changing user passwords.
12. To establish and check a procedure application that guarantees the storage of valid passwords in an unreadable form.
13. To establish and check a system application that restricts the access of users exclusively to the data and resources that they require to exercise their functions.
14. To establish and check the mechanisms that facilitate the access to users to data and/or resources for which they are authorised.

15. To grant, change or annul authorised access to data and resources in accordance with the criteria established by the file manager.
16. To establish and check the application of a system that identifies, makes inventory of and stores the computer storage media containing personal data in a secure location.
17. To ensure compliance with the security standards while notifying the file manager of any violations committed that could be sanctioned depending on the labour laws applicable thereto.
18. To establish and check periodic control application to verify compliance with the provisions of the security document.
19. To establish and check the application of the security measures to be adopted when a data storage medium is to be disposed of or reused.
20. To coordinate and control the measures set forth in the security document.
21. To coordinate and control the execution of a system and external audit of the information systems and installations in which personal data are processed that verifies compliance with the security regulations and the procedures and instructions in force in respect of data security.
22. To establish and check the application of measures to control physical access to the premises in which the information systems containing personal data are located.
23. To establish and check the application of a record of data storage media that, directly or indirectly, informs of the type of medium, the date and time of creation, the sender, the number of media, the type of information they contain, the manner in which they are sent and the person responsible for receiving them, who must be duly authorised.
24. To establish and check an outgoing computer media record application that, directly or indirectly, informs of the type of medium, the date and time of creation, the recipient, the number of media, the type of information they contain, the manner in which they are sent and the person responsible for the delivery, who must be duly authorised.
25. To establish and check the application of necessary measures to prevent the subsequent recovery of information stored in the computer media that are to be disposed of or reused.
26. To establish and check the application of necessary measures to prevent the wrongful recovery of information stored in computer media that are to be removed from the premises in which the files are located.
27. To monitor the recording of incidents and to extend same to leave record of the procedures implemented in order to recover the data, indicating the person who executed the process, the data recovered and, as the case may be, which data required manual recording in the recovery process.
28. To authorise in writing the execution of the data recovery procedures.
29. To check that during the information system testing phase, the tests are not

conducted using real personal data.

30. To publish internal rules.

31. To check the knowledge of the internal rules on the part of the company's personnel.

32. To ensure compliance with the internal rules of the National Council of Spanish Bar Associations.

In respect of the management and operation of the activity of Certification Service Provider, other roles and functions are required in accordance with the standards of CEN CWA 14167-1, details of which are given in component 5.2.1.

## C. STRUCTURE OF FILES AND DESCRIPTION OF SYSTEMS BY WHICH THEY ARE PROCESSED

The personal data constituting the files subject to processing are the following:

Identification data:

- Name, surnames and identity card

Contact data:

- Electronic mail address
- Alternative electronic mail address for contact

Professional data:

- Association or Institution
- Membership / Associate no. (where applicable)
- Status in respect of the corporation / entity (where applicable)
- Responsibility, title or specialist area (where applicable)
- Department to which he belongs (where applicable)

Data of digital certificate (public key certificate):

- Certificate serial number
- Validity commencement and termination date
- Public key associated with the private key held by the user
- Request and certificate status (Pending approval, Approved, Valid, Suspended or Revoked).

Description of the processing system

- The system that supports the provision of certificate services is based on centralised servers located in a top security data center. The system has local access over controlled work stations located in a secure area of the data center and over the Internet.

- Certificate public system consultation operations are appropriately protected as described in component 2.6 hereof.
- Registration, data modification and de-registration operations on the part of remote operators of the Registration Authorities are protected by access with digital certificate managed by an operator card.
- Certificate request transmission operations on the part of applicants are protected by an access password prior to the transmission.
- The process is described in chapter 4 of this document.

## D. MEASURES TO GUARANTEE THE SECURITY LEVEL

The measures implemented to guarantee the security levels required by the law governing the protection of personal data, at its basic level, are extensively supported by other legal requirements and good practices to be implemented in order to be authorised to provide certification services. The specific measures required for the certification system, according to which the files containing personal data are processed, are described in chapters 4, 5 and 6 hereof.

**System control and audit**

The periodic controls required to verify compliance with the provisions of the security document shall be implemented on an on-going basis and at least once a year.

The periodic controls shall be conducted in the following areas:

- Control of security plan application
- Control of the identification and authentication system
- Control of the access screening system
- Control of compliance with the regulations governing confidentiality and secrecy
- Control of compliance with internal rules and functions of personnel in trusted roles
- Antivirus control
- Control of compliance with the regulations governing intellectual property

The data included in the files are basic level data, consequent on which the execution of specific external audits is not required. The security procedures and measures are, however, audited within the voluntary external audit framework of the activity of providing certification services, as set forth in component 2.7.

In addition, the National Council of Spanish Bar Associations provides the General Security Measures listed below, which are applicable to all systems, equipment, users and procedures although they might not be directly involved in the processing of personal data.

# General Security Measures

## D.1 Identification and authentication

1. There is an up-to-date list of users that have authorised access to the information systems.
2. The security officer shall store and update the list of all the network users that have authorised access to the information systems. The security officer is responsible for ensuring that the attribution and designation of passwords and the custody of the user list is executed such that their confidentiality and integrity are guaranteed.
3. There is an identification and authentication system for users that wish to access the system. The users are identified in the system by their user number and access key or by the pertinent digital certificate. There is also a procedure for designating, distributing and storing passwords that guarantees their confidentiality and integrity.
4. The identification numbers and access keys designated to each user of the corporate network of the National Council of Spanish Bar Associations are personal and non-transferrable while the user is the only party responsible for the consequences that might ensue from the misuse, disclosure or loss of same.
5. The passwords of authorised users shall have a minimum length of four characters. While they are valid, passwords shall be stored in an unreadable form.
6. The security officer shall provide a mechanism that unequivocally identifies, in a personalised manner, any user that tries to access the information system and verifies that said user is authorised.

## D.2 Access control and confidentiality of information

1. All information stored in the corporate network of the National Council of Spanish Bar Associations or its providers, either statically or circulating in the form of electronic mail messages, is the property of the National Council of Spanish Bar Associations and is confidential in respect of third parties external to the National Council of Spanish Bar Associations.
2. Industrial or commercial secrets of the company shall be considered as especially reserved information, which shall embrace, without limitation, the procedures, methodologies, source code, algorithms, personal information databases (data of clients, providers, and so forth), marketing plans and any other material that comprises the industrial or commercial strategy of the National Council of Spanish Bar Associations.
3. Users shall only have authorised access to the data and resources they require to perform their functions. In particular, the certification system shall define the separation of roles and privileges according to the provisions of the pertinent component hereof.
4. To access the premises in which the certification system of the National Council of Spanish Bar Associations is located, a physical access control system is required, which prevents the access of unauthorised personnel.

5. Testing prior to the implementation or modification of the information systems that process files containing personal data are not conducted with real data unless the security level corresponding to the file processed is ensured.

### D.3 Electronic mail usage

2. The computer system, the corporate network and the terminals used by each user are the property of the National Council of Spanish Bar Associations or its providers, in cases where the service has been organised in this manner.
3. No electronic mail message shall be considered to be private. Electronic mail shall be considered to be both internal mail, between the corporate network terminals, and the external mail, sent to or coming from other public or private networks, particularly the Internet.
4. The National Council of Spanish Bar Associations reserves the right to inspect, either itself or through the provision of third-party services, without prior notice, any electronic mail messages of users of the corporate network and the mail server log archives for the purpose of verifying compliance with these rules and preventing activities that might have repercussions on the National Council of Spanish Bar Associations in respect of subsidiary civil liability.
5. Any file introduced into the corporate network or the user terminal over electronic mail messages coming from external networks must comply with the requirements set forth in these rules, particularly those relating to intellectual and industrial property as well as virus control.

### D.4 Internet access

1. Use of the data information system of the National Council of Spanish Bar Associations to access public networks, such as the Internet, shall be limited to matters directly relating to the activity of the National Council of Spanish Bar Associations and user work station functions.
2. Access to real time debates (Chat / IRC) is particularly dangerous since it facilitates the installation of utilities that permit unauthorised access to the system, consequent on which its use is strictly prohibited. All the foregoing is applicable unless express authorisation is obtained from the security officer.
3. Access to websites (WWW), news groups (Newsgroups) and other information sources, such as FTP, and so forth, is restricted to those that contain information relating to the activity of the National Council of Spanish Bar Associations or to user work station functions.
4. The National Council of Spanish Bar Associations reserves the right to monitor and verify, either itself or through the provision of third-party services, on a random basis and without prior notice, any Internet access session initiated by the user.
5. Any file introduced into the corporate network or the user terminal from the Internet must comply with the requirements set forth in these rules, particularly those relating to intellectual and industrial property as well as virus control.

### D.5 Intellectual and industrial property

Usage of software applications without the pertinent licence and the use, reproduction, assignment, conversion or public disclosure of any type of work or invention protected by intellectual or industrial property rights is strictly prohibited.

## E. INCIDENT REPORTING, MANAGEMENT AND RESPONSE PROCEDURE

### 1. Reporting

Any staff member of the National Council of Spanish Bar Associations or any person who is temporarily providing his services in said Council shall report to the security officer forthwith any anomaly detected that affects or might affect data security.

Any delay in reporting incidents shall constitute a breach of contractual good faith, sanctioned in accordance with the labour laws applicable thereto.

Incidents shall be reported over the security officer's electronic mail and/or by telephone.

### 2. Management

The security officer shall receive the incident report and record same while notifying the internal or external engineers in charge of system security.

### 3. Response

The security officer shall ensure that the technical department immediately responds to the incident detected and shall supervise the work performed to correct the anomaly in question. Once the correction has been made, said manager shall send a report to the file manager providing all the data required for recording the incident.

### 4. Incident record

In accordance with section 10 of Royal Decree 994/1999, the file manager has created an electronic record in which is indicated the following information relating to incidents:

- Type of incident
- The time the incident occurred
- Person reporting the incident
- Effects deriving from said incident report.

The file manager is required to keep the incident record up to date.

Likewise, the security officer is required to handle any incidents that might arise as promptly as possible while guaranteeing, insofar as possible, that the security of personal data is not modified at any time.

The data recovery procedures implemented shall also be recorded in the incident record, indicating the person who executed the process, the data recovered and, if applicable, which data required manual recording in the recovery process.

Authorisation from the file manager shall be required to execute the recovery procedures.

## F. DATA BACKUP AND RECOVERY PROCEDURE

### F.1 Frequency of making backup copies

Making backup copies periodically enables the National Council of Spanish Bar Associations to have at its disposal the information copied in the event of destruction of the equipment or errors produced in the data and/or software applications.

There is a specific backup policy for each environment that indicates the frequency with which backup copies are to be made depending on the information they contain. These policies are documented.

### F.2 Backup copy storage

The risk of data loss in the event of a contingency is minimised by making two backup copies, one of which is stored in the data center premises and the other, in an off-site facility.

The backup copies are stored securely in the data center and in a bank safe deposit box.

### F.3 Backup copy protection

Appropriate backup copy protection means that said copies are correctly conserved and that access to stored data is controlled effectively.

The backup copies are kept in the security area of the data center in safes under lock and key, to which only authorised personnel have access, or in fireproof safes, depending on criticality. Access to the bank safe deposit box is also restricted to authorised personnel.

### F.4 Backup system automation

The automation of the backup procedure reduces the possibility of erroneous or omitted cycles.

### F.5 Description of backup copy content

The documentation on the content of the backup copies facilitates their identification.

The content of said copies is reflected on the tape labels. This same information is saved in a data base. An electronic record is also kept of the backup copy execution confirmation emails received by systems when said copies are made.

### F.6 Storage control

A record of backup copy content makes information on the backup copies stored available, which facilitates an efficient control of tape library management.

The Systems Department keeps a manual inventory of the content of backup copies stored in the library, which is updated each time there is a new entry or removal. The copies kept in the offices are identified with labels, thereby informing of the tape content.

### F.7 Control of backup copy entry and removal

The existence of a system that records entries and removals of backup copies ensures that the inventory is trustworthy.

The inventory reflects all entries and removals of backup copies. In the event that the removal of a copy is requested, this will also be recorded as well as the person making the request and the reasons.

To remove information from the data center for the purpose of depositing it in the off-site storage facility, express authorisation is required from the security officer. The request to remove devices shall be sent to the security officer's mail account, indicating the following:

- Date of removal
- Reason for removal
- Type of medium
- Medium code
- Type of information contained

The security officer will either authorise of refuse the removal.

### F.8 Transport of backup copies

Backup copies must be transported in an appropriately secure environment to ensure that the data contained therein are not modified, stolen or destroyed in transit.

### F.9 Backup and recovery testing

Recovery testing performed on backup copies verifies that the backup copy recovery procedure is functioning correctly, thereby guaranteeing the integrity of the data contained therein.

### F.10 Period for existence of backup copies and their eventual destruction

The establishment of a period for existence of backup copies in accordance with the laws currently in force and this company's policy contributes to their storage and ensures the efficient use of the physical space available for storage.

The period for existence of the backup copies is defined according to the time period indicated in their Backup Policy. The lifetime of the storage devices according to their use is estimated and said devices are destroyed at the end of their useful lives upon prior authorisation from the security officer.

# 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 for assembling the packets at destination. The IP Protocol directs the data correctly to its recipient. |