



Certification Practice Statement (CPS)

Drafted following the specifications of RFC 3647 and completed
with points from ETSI TS 101 456 V1.2.1

Date: 27/08/2008 **Version:** 1.4
Status: CURRENT **Nº of pages:** 62
OID: 1.3.6.1.4.1.30051.2.1.1.1 **Classification:** PUBLIC
Archive: ing_ACEDICOM - CertificationPractice.doc
Prepared by: EDICOM - ACEDICOM Certification Authority

| Changes record | | | |
|-----------------------|-------------|--|--|
| Version | Date | Action description | Pages / Sections |
| 1.0 | 07/05/2008 | Initial | |
| 1.1 | 15/05/2008 | Minor changes by audit recommendation of S21SEC | |
| 1.2 | 30/05/2008 | Minor change. HSM Administrator role functions explanation | |
| 1.3 | 27/06/08 | Minor change. Security policies extension | |
| 1.4 | 27/08/08 | Changes according to comments from the Ministry of Industry and Commerce | 1.6.1, 3.1.1, 3.2.3, 4.9.3, 4.9.9, 5.4.3, 6.3.1, 9.6.1.2, 9.11.1 |

Table of Contents

| | |
|---|-----------|
| 1. INTRODUCTION..... | 10 |
| 1.1. PRESENTATION..... | 10 |
| 1.2. DOCUMENT NAME AND IDENTIFICATION..... | 12 |
| 1.3. PKI PARTICIPANTS, COMMUNITY OF CERTIFIED USERS..... | 12 |
| 1.3.1. Certification Authorities..... | 12 |
| 1.3.2. Registration Authorities..... | 14 |
| 1.3.3. End Users..... | 14 |
| 1.4. USE OF CERTIFICATES..... | 15 |
| 1.4.1 Typical uses of certificates..... | 15 |
| 1.4.2. Prohibited uses..... | 16 |
| 1.4.3. Reliability of the electronic signature over time..... | 17 |
| 1.5. ADMINISTRATION OF THE POLICIES..... | 17 |
| 1.5.1. Entity responsible for the CPS..... | 17 |
| 1.5.2. Contact person for CPS..... | 18 |
| 1.5.3. Competence to determine CPS compliance with the different Certification Policies..... | 18 |
| 1.5.4 Approval procedure..... | 18 |
| 1.6. DEFINITIONS AND ACRONYMS..... | 18 |
| 1.6.1. Definitions..... | 18 |
| 1.6.2. Acronyms..... | 21 |
| 2. INFORMATION PUBLICATION AND CERTIFICATE REPOSITORY..... | 23 |
| 2.1. REPOSITORIES..... | 23 |
| 2.2. PUBLICATION..... | 23 |
| 2.3. UPDATE FREQUENCY..... | 23 |
| 2.4. CERTIFICATE REPOSITORY ACCESS CONTROLS..... | 24 |
| 3. CERTIFICATE HOLDER IDENTIFICATION AND AUTHENTICATION..... | 25 |
| 3.1. NAME REGISTRATION..... | 25 |
| 3.1.1. Name types..... | 25 |
| 3.1.2. Meaning of names..... | 26 |
| 3.1.3. Name format interpretation..... | 26 |
| 3.1.2. Uniqueness of names..... | 26 |
| 3.1.5. Resolution of name-related conflicts..... | 26 |

| | |
|--|-----------|
| 3.1.6. Recognition, authentication and function of registered trade names..... | 26 |
| 3.2. INITIAL IDENTITY VALIDATION..... | 26 |
| 3.2.1. Private key possession proof methods..... | 26 |
| 3.2.2. Authentication of identity of an entity..... | 26 |
| 3.2.3. Individual identity authentication..... | 28 |
| 3.3. KEY RENEWAL REQUEST IDENTIFICATION AND AUTHENTICATION..... | 28 |
| 3.3.1. Identification and authentication of routine renewal requests.. | 29 |
| 3.3.2. Key renewal request identification and authentication after a revocation - Key not compromised..... | 29 |
| 3.4. KEY REVOCATION REQUEST IDENTIFICATION AND AUTHENTICATION..... | 29 |
| 4. THE LIFE CYCLE OF CERTIFICATES..... | 30 |
| 4.1. CERTIFICATE APPLICATIONS..... | 30 |
| 4.2. CERTIFICATE REQUEST TRANSACTIONS..... | 30 |
| 4.3. ISSUING CERTIFICATES..... | 30 |
| 4.4. ACCEPTING CERTIFICATES..... | 30 |
| 4.5. USE OF THE PAIR OF KEYS AND THE CERTIFICATE..... | 31 |
| 4.6. CERTIFICATE RENEWAL..... | 31 |
| 4.7. KEY RENEWAL..... | 31 |
| 4.8. CERTIFICATE MODIFICATION..... | 31 |
| 4.9. CERTIFICATE REVOCATION AND SUSPENSION..... | 31 |
| 4.9.1. Circumstances for revocation..... | 31 |
| 4.9.2. Entity that may apply for revocation..... | 32 |
| 4.9.3. Revocation request procedure..... | 32 |
| 4.9.4. Revocation request grace period..... | 33 |
| 4.9.5. Circumstances for suspension..... | 33 |
| 4.9.6. Entity that may apply for suspension..... | 33 |
| 4.9.7. Suspension request procedure..... | 33 |
| 4.9.8. Suspension period limits..... | 33 |
| 4.9.9. Frequency of issue of CRLS..... | 33 |
| 4.9.10. CRL checking requirements..... | 33 |
| 4.9.11. Other revoked certificate notification methods..... | 33 |
| 4.9.12. Special renewal requirements for compromised keys..... | 33 |
| 4.10. CERTIFICATE STATUS CHECKING SERVICES..... | 34 |
| 4.10.1. Operating Features..... | 34 |
| 4.10.2. Service Availability..... | 34 |

4.11. CONCLUSION OF THE SUBSCRIPTION. 34

4.12. KEY DEPOSIT AND RECOVERY. 34

5. PHYSICAL SECURITY, MANAGEMENT AND OPERATIONAL CONTROLS... 36

5.1. PHYSICAL SECURITY CONTROLS. 36

5.1.1. Location and construction. 36

5.1.2. Physical access. 36

5.1.3. Power supply and air conditioning. 36

5.1.4. Exposure to water. 36

5.1.5. Fire protection and prevention. 37

5.1.6. Storage system. 37

5.1.7. Waste disposal. 37

5.1.8. Remote backup. 37

5.2. PROCEDURAL CONTROLS. 37

5.2.1. Trusted roles. 37

5.2.2. Number of people required per task. 38

5.2.3. Identification and authentication for each role. 38

5.3. PERSONNEL SECURITY CONTROLS. 38

5.3.1. Background, qualification, experience, and accreditation requirements. 39

5.3.2. Background vetting procedures. 39

5.3.3. Training requirements. 39

5.3.4. Training update requirements and frequency. 40

5.3.5. Task rotation frequency and sequence. 40

5.3.6. Sanctions for unauthorized actions. 40

5.3.7. Staff hiring requirements. 40

5.3.8. Documentation provided to personnel. 40

5.3.9. Periodic compliance checks. 40

5.3.10. Termination of contracts. 41

5.4. SECURITY PROCEDURE CONTROLS. 41

5.4.1. Event types recorded. 41

5.4.2. Log processing frequency. 41

5.4.3. Audit logs retention period. 42

5.4.4. Audit log protection. 42

5.4.4. Audit log backup procedures. 42

5.4.6. Audit information collection System (internal vs. external). 42

5.4.7. Notification to the subject cause of the event. 42

5.4.8. Vulnerability analysis. 42

5.5. INFORMATION AND RECORDS FILE. 42

5.5.1. Type of information and events recorded. 43

5.5.2. Archive retention term. 43

5.5.3. Archive protection. 43

5.5.4. Archive backup procedures. 43

5.5.5. Record time stamping requirements. 43

5.5.6. Audit information compilation system (internal vs. external)... 44

5.5.7. Procedures to obtain and verify archived information..... 44

5.6. CA KEY CHANGE. 44

5.7. RECOVERY IN CASE OF KEY COMPROMISE OR DISASTER..... 44

5.7.1. Alteration of hardware, software and/or data resources. 44

5.7.2. The public key of an entity is revoked..... 44

5.7.3. The key of an entity is compromised..... 45

5.7.4. Security installation following natural disaster or other types of disaster..... 45

5.8. CESSATION OF A CA..... 45

6. TECHNICAL SECURITY CONTROLS..... 46

6.1. KEY PAIR GENERATION AND INSTALLATION. 46

6.1.1. Key pair generation. 46
 where the generation of the keys is not done by means under control of the end entity, the corresponding Certification Policy will specify the procedure to be used to deliver the private key to the end entities. ... 46

6.1.3. Delivery of public key to certificate issuer..... 46

6.1.4. Delivery of the public key of the CA to the users..... 46

6.1.5. Key size. 46

6.1.6. Public key generation parameters..... 46

6.1.7. Parameter quality check..... 46

6.1.8. Key generation hardware/software..... 47

6.1.9. Key usage purposes..... 47

6.2. PRIVATE KEY PROTECTION..... 47

6.2.1. Standards for the cryptographic modules..... 47

6.2.2. Multi-person private key control..... 47

6.2.3. Private key custody..... 48

6.2.4. Private key security copy..... 48

6.2.5. Private key archive..... 48

6.2.6. Entering the private key in the cryptographic module..... 48

6.2.7. Private key activation method..... 48

6.2.8. Private key deactivation method..... 48

6.2.9. Private key destruction method..... 48

6.2.10 Classification of cryptographic modules..... 48

6.3. OTHER KEY PAIR MANAGEMENT ASPECTS..... 49

6.3.1. Public key archive..... 49

6.3.2. Public and private key usage periods..... 49

6.4. ACTIVATION DATA..... 49

6.4.1. Activation data generation and activation..... 49

6.4.2. Activation data protection..... 49

6.4.3. Other activation data aspects..... 49

| | |
|--|-----------|
| 6.5. IT SECURITY CONTROLS..... | 49 |
| 6.5.1 Specific IT security technical requirements..... | 49 |
| 6.5.2 IT security level assessment..... | 50 |
| 6.6. SERVICE LIFE SECURITY CONTROLS..... | 50 |
| 6.6.1 Systems development controls..... | 50 |
| 6.6.2 Security management controls..... | 50 |
| 6.7. NETWORK SECURITY CONTROLS..... | 51 |
| 6.8. CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS..... | 51 |
| 7. REVOKED CERTIFICATE AND CERTIFICATE LIST PROFILES..... | 52 |
| 7.1. CERTIFICATE PROFILE..... | 52 |
| 7.1.1. Version number..... | 52 |
| 7.1.2. Certificate extensions..... | 52 |
| 7.1.3. Object identifiers (OID) of algorithms..... | 52 |
| 7.1.4. Name formats..... | 52 |
| 3.1.2. Name constraints..... | 53 |
| 7.1.6. Certification Policy Object Identifier (OID)..... | 53 |
| 7.1.7. "Policy Constraints" extension use..... | 53 |
| 7.1.8. Policy qualifier syntax and semantics..... | 53 |
| 7.1.9. Critical "Certificate Policy" extension semantic treatment..... | 53 |
| 7.2. CRL profile..... | 53 |
| 7.2.1. Version number..... | 53 |
| 7.2.2. CRL and extensions..... | 53 |
| 7.3 REVOKED CERTIFICATE LIST..... | 53 |
| 7.3.1 Time limit of certificates in CRLs..... | 53 |
| 7.4.- OCSP PROFILE..... | 53 |
| 7.4.1.- OCSP responder certificate profile..... | 53 |
| 7.4.2.- Version number..... | 54 |
| 7.4.3.- Name formats..... | 54 |
| 7.4.4.- Certification Policy Object Identifier (OID)..... | 54 |
| 7.4.5.- Certificate extensions and fields..... | 54 |
| 7.4.6.- OCSP request format..... | 55 |
| 7.4.7.- Response format..... | 55 |
| 8. CONFORMITY AUDIT..... | 57 |
| 8.1. FREQUENCY OF CONFORMITY CHECKS FOR EACH ENTITY..... | 57 |
| 8.2. AUDITOR IDENTIFICATION/QUALIFICATION..... | 57 |
| 8.3. RELATION BETWEEN AUDITOR AND ENTITY AUDITED..... | 57 |

8.4. TOPICS COVERED BY CONFORMITY AUDIT..... 57

8.5. ACTIONS TO BE TAKEN AS A RESULT OF A DEFICIENCY. 57

8.6. COMMUNICATION OF RESULTS. 58

9. COMMERCIAL AND LEGAL REQUIREMENTS..... 59

9.1. TARIFFS. 59

9.1.1. Certificate issue or renewal fees..... 59

9.1.2. Certificate access fees..... 59

9.1.3. Fees for access to status or revocation information..... 59

9.1.4. Fees for other services such as information on policies..... 59

9.1.5. Refund policy. 59

9.2. FINANCIAL STANDING..... 59

9.2.1. Indemnification to third parties trusting certificates issued by ACEDICOM..... 59

9.2.2. Fiduciary relations. 59

9.2.3. Administrative processes..... 59

9.3. CONFIDENTIALITY POLICY..... 60

9.3.1. Confidential information..... 60

9.3.2. Non-confidential information..... 60

9.3.3. Disclosure of certificate revocation /suspension information... 60

9.4. PERSONAL DATA PROTECTION. 61

9.4.1. Personal Data Protection Plan..... 61

9.4.2. Information deemed private..... 61

9.4.3. Information not deemed private. 62

9.4.4. Responsibilities..... 62

9.4.5. Consent given for personal data use..... 63

9.4.6. Communication of information to administrative and/or judicial authorities..... 63

9.4.7. Other information disclosure situations..... 63

9.5. INTELLECTUAL PROPERTY RIGHTS. 63

9.6. OBLIGATIONS AND CIVIL RESPONSIBILITY. 63

9.6.1. Obligations of the Certification Entity..... 63

9.6.2. Registration Authority Obligations..... 66

9.6.3. Subscriber obligations..... 67

9.6.4. Obligations of third parties trusting certificates issued by ACEDICOM..... 69

9.6.5. Repository obligations..... 69

9.7. GUARANTEE WAIVERS..... 69

9.8. RESPONSIBILITY LIMITATIONS. 69

9.8.1. Guarantees and limitations of guarantees..... 69

| | |
|---|-----------|
| 9.8.2. Definition of responsibilities..... | 69 |
| 9.8.3. Loss limitations..... | 70 |
| 9.9. TERM AND CONCLUSION..... | 70 |
| 9.9.1. Term..... | 70 |
| 9.9.2. Conclusion..... | 70 |
| 9.9.3. Survival..... | 70 |
| 9.10. NOTIFICATIONS..... | 70 |
| 9.11. MODIFICATIONS..... | 71 |
| 9.11.1. Change specification procedures..... | 71 |
| 9.11.2. Publication and notification procedures..... | 72 |
| 9.11.3. Certification Practice Statement approval procedures..... | 72 |
| 9.12. RESOLUTION OF CONFLICTS..... | 72 |
| 9.12.1. Extrajudicial resolution of conflicts..... | 72 |
| 9.12.2. Competent jurisdiction..... | 72 |
| 9.13. APPLICABLE LEGISLATION..... | 72 |
| 9.14. COMPLIANCE WITH APPLICABLE LAW..... | 72 |
| 9.15. DIVERSE CLAUSES..... | 72 |

1. INTRODUCTION.

1.1. PRESENTATION.

EDICOM is constituted as Certification Service Provider or Certification Authority by virtue of the document sent to the Ministry of Industry, Commerce and Tourism in accordance with that set forth in Law 59/2003 of 19th December on electronic signature, in article 30 of the same, transitory provision n° 2: "*Certification Service Providers must communicate to the Ministry of Industry, Tourism and Commerce the beginning of their activity, their identification details, including the fiscal and registry identification, and, where indicated, the data that enable communication to be established with the provider, including the Internet domain name, the customer service details, the features of the services to be provided, the certificates obtained for said services and certificates of the devices used.*"

EDICOM issues ACEDICOM certificates, which are recognized certificates for identification and advanced electronic signature, for the use of physical persons or legal organisations (known collectively as subscribers) that need to engage in relations with the Public Administrations and other institutions or companies in the Electronic Data Interchange area and/or to equip themselves with certified storage systems.

The ACEDICOM certificate is an **acknowledged certificate** in accordance with that laid down in article 11.1 of Law 59/2003, of 19th December, on electronic signature, with the content prescribed by article 11.2, and issued in compliance with the obligations of articles 12, 13, 18 and 20 of said Law.

Likewise, the certificates comply with the standards on the subject of recognized certificates, specifically:

- ETSI TS 101 862: Qualified Certificate Profile.
- RFC 3739 Internet X.509 Public Key Infrastructure: Qualified Certificates Profile

ACEDICOM also issues server certificates and other types of certificates for purposes other than "electronic signature". They cannot be considered subject to that laid down in Law 59/2003 on Electronic Signature, of 19th December, since they do not come under the concept of "electronic certificate" defined in article 6 of said law, and are not suitable to provide support to the "Electronic Signature" in the same. They are mentioned in this page exclusively because they form part of the catalogue of certificates issued by ACEDICOM, although they are not subject to the criteria and procedures required for recognized certificates, although they do share the whole physical and security infrastructure established for said certificates.

This document is considered as the mandatory *Certification Practice Statement (CPS)* from the EDICOM Certification Authority.

In accordance with the above and in compliance with the specific legislation contained in article 19 of Law 59/2003, of 19th December, on

Electronic Signature, this Certification Practice Statement (CPS) details the rules and general conditions of the certification services provided by the EDICOM Certification Authority, in relation with the management of the data for creation and verification of electronic signature and certificates, the conditions applicable to the requesting, issue, use, suspension and extinction of the validity of certificates, technical and organizational security measures, profiles and the information mechanisms on the use of certificates and, where indicated, the existence of coordination procedures with the corresponding public registries to allow the interchange of information immediately on the validity of the powers indicated in the certificates and which must appear recorded in said registries.

To this end, this Certification Practice Statement constitutes the general compendium of rules applicable to all certifying activities of the EDICOM Certification Authority as Certification Service Provider. However, the different specialities applicable to each of the different types of certificates that are issued are stipulated in the different Certification Policies which, as complementary and specific standards, will prevail over this Certification Practice Statement as regards each type of certificate.

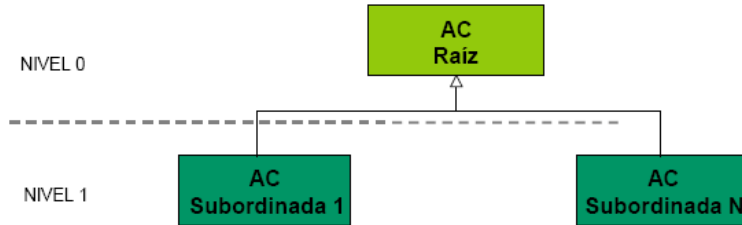
This Certification Practice Statement is drafted in line with the RFC 3647 specifications "*Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*" proposed by *Network Working Group* and completed with aspects stipulated in:

- ETSI TS 101 456: "*Policy Requirements for certification authorities issuing qualified certificates*".
- ETSI TS 101 862: "*Qualified Certificate Profile*".
- ETSI TS 102 042: "*Policy Requirements for certification authorities issuing qualified certificates*".

Likewise, the following are considered as basic standards applicable on the issue:

- Directive 1999/93/EC of the European Parliament and Council, of 13th December 1999, where a community framework for electronic signature is established.
- LAW 59/2003, of 19th December, on Electronic Signature.
- Organic Law 15/1999, of 13th December, on Protection of Data of a Personal Nature.
- Royal Decree 1720/2007, of 21st December, whereby the Regulation of development of Organic Law 15/1999, of 13th December, on protection of personal data, is approved.
- Royal Legislative Decree 1/1996, of 12th April, whereby the Revised Text of the Intellectual Property Law is approved.
- ROYAL DECREE 1553/2005, of 23rd December, regulating the issue of the national identity document and the corresponding electronic signature certificates.

The general architecture of EDICOM PKI at hierarchic level is as follows:



- A first level, in which the root CA that represents the trusted point of the whole system is located and which will allow, as set forth in article 15 of the Law on Electronic Signature, all physical or legal, public or private persons to recognize the effectiveness of EDICOM certificates for electronic signature.
- A second level, consisting of the subordinate CAs of the Root CA that will issue certificates of identity and signature of the subscribers.

1.2. DOCUMENT NAME AND IDENTIFICATION.

| | |
|--------------------------------|---|
| Document name | Certification Practice Statement (CPS). |
| Document version | 1.4 |
| Document status | Valid |
| OID (Object Identifier) | 1.3.6.1.4.1.30051.2.1.1.1 |
| Date of issue | 7th May 2008 |
| Expiry date | Not Applicable |
| Localization | http://acedicom.edicomgroup.com |

1.3. PKI PARTICIPANTS, COMMUNITY OF CERTIFIED USERS.

This certification practice declaration regulates a community of users, who obtain certificates for diverse administrative and private relations, in accordance with Law 59/2003 and the corresponding administrative norm.

1.3.1. Certification Authorities.

The Certification Service Provider is EDICOM.

In this Certification Practice Statement, the acronym "ACEDICOM" is used to designate the set of Certification Authorities that make up ACEDICOM. The functions of the EDICOM Certification Authority are assigned to the EDICOM Systems Department.

The Certification Authorities that make up ACEDICOM are:

."ACEDICOM Root" as first level Certification Authority. Its function is to establish the root of the confidence model of the Public Key Infrastructure or PKI. This CA does not issue certificates for end-user entities. This first level Certification Authority signs for itself. The most relevant data are:

| Field | Contents | I | C | T |
|---------|----------|---|---|---|
| Version | v3 | S | | F |

| | | | |
|----------------------------------|--|---|-----|
| Serial Number | 61 8d c7 86 3b 01 82 05 | S | F |
| Signature Algorithm | SHA1withRSAEncryption | S | F |
| Issuer Distinguished Name | CN=ACEDICOM Root, OU=PKI, O=EDICOM, C=ES | S | F |
| Validity | 7300 days | S | F |
| Subject Public Key Info | Key type: RSA Key length: 4096 bits | S | F |
| Subject DN | | S | D |
| CommonName (CN) | ACEDICOM Root | S | D |
| Organizational Unit (OU) | PKI | O | D |
| Organization (O) | EDICOM | S | D |
| Country (C) | ES | S | D |
| SubjectKeyIdentifier | a6 b3 e1 2b 2b 49 b6 d7 73 a1 aa 94 f5 01 e7 73 65 4c ac 50 | S | D |
| AuthorityKeyIdentifier | KeyId: (Same as the SubjectKeyIdentifier because the certificate is self-signed) | S | F |
| BasicConstraints | | S | X F |
| CA | True | S | X F |
| PathLength | - (No limit) | N | |
| KeyUsage | DigitalSignature, Certificate Sign, CRL Sign | S | X F |
| Certificate Policies | | S | F |
| PolicyIdentifier | 2.5.29.32.0 (anyPolicy) | S | F |
| CPSuri | http://acedicom.edicomgroup.com | S | F |
| CRLDistributionPoints | | S | F |
| DistributionPoint | http://acedicom.edicomgroup.com/crlroot | S | F |
| DIGITAL FINGERPRINT | e0 b4 32 2e b2 f6 a5 68 b6 54 53 84 48 18 4a 50 36 87 43 84 | S | F |

Captions used in the tables:

I = Included. Possible values: S=Always, O=Optionally, C=Conditionally

C = Critical. If the box is ticked, indicates that it is critical.

T = Type. Possible values: D = Dynamic, F = Fixed. Fixed means that the value is the same for all certificates of this type.

- ACEDICOM Root subordinate CAs. Their function is to issue end-user entity certificates for ACEDICOM subscribers. The most relevant data are:

ACEDICOM XX

| Field | Contents | I | C | T |
|--|---|---|---|---|
| Version | v3 | S | | F |
| Serial Number | Generated automatically by the CA | S | | F |
| Signature Algorithm | SHA1withRSAEncryption | S | | F |
| Issuer Distinguished Name | CN=ACEDICOM Root, OU=PKI, O=EDICOM, C=ES | S | | F |
| Validity | 3650 days | S | | F |
| Subject Public Key Info | Key type: RSA Key length: 4096 bits | S | | F |
| Subject DN | | S | | D |
| CommonName (CN) | ACEDICOM XX | S | | D |
| Organizational Unit (OU) | PKI | O | | D |
| Organization (O) | EDICOM | S | | D |
| Country (C) | ES | S | | D |
| Location (L) | Ronda de Auguste y Louis Lumiere 12 Paterna | | | |
| Email (E) | acedicom@edicomgroup.com | | | |
| PostalCode | 46980 | | | |
| Serial Number. | B96490867 | | | |
| SubjectKeyIdentifier | Certificate Public Key Identifier | S | | D |
| KeyId: a6 b3 e1 2b 2b 49 b6 d7 73 a1 aa 94 f5 01 e7 73 65 4c ac 50 | | S | | F |
| AuthorityKeyIdentifier | Belonging to ACEDICOM Root | | | |
| BasicConstraints | | S | X | F |
| CA | True | S | X | F |

| | | | | |
|------------------------------|--|---|---|---|
| PathLength | - (No limit) | N | | |
| KeyUsage | DigitalSignature, Certificate Sign, CRL Sign | S | X | F |
| Certificate Policies | | S | | F |
| PolicyIdentifier | 1.3.6.1.4.1.30051.2.1.1.1 | S | | F |
| CPSuri | http://acedicom.edicomgroup.com | S | | F |
| CRLDistributionPoints | | S | | F |
| DistributionPoint | http://acedicom.edicomgroup.com/crl01 | S | | F |
| Authority Information | | S | | F |
| Access | | S | | F |
| AccessMethod | OCSP | S | | F |
| AccessLocation | http://ocsp.edicomgroup.com | S | | F |

XX It is a two-digit number that refers to the issuing CA.

1.3.2. Registration Authorities.

The Registration Authorities are those physical or legal persons to whom the ACEDICOM entrusts the identification and verification of the personal circumstances of the certificate applicants. To this end, the Registration Authorities will be responsible for guaranteeing that the certificate application contains truthful and complete information on the Applicant, and meets the requirements demanded in the corresponding Policy.

The main company EDICOM and its different subsidiaries, authorized formally by the same, may be Registration Authorities. These Registration Authorities are designated User Registration Points or URPs in the documentation relative to the EDICOM Certification Authority, and are entrusted with the confirmation of the applicant's identity and issuing of the certificate.

The functions of these Registration Authorities, which act on behalf of ACEDICOM, extend to:

- Checking the identity and any personal circumstances of the pertinent certificate applicants for their own purposes.
- Informing the person who applies for the certificate prior to its issue of the precise conditions for the use of the certificate and its limitations of use.
- Verifying that the information contained in the certificate is exact and includes all the information prescribed for a recognized certificate.
- Ensuring that the signer is in possession of the signature creation data corresponding to those verified and recorded in the certificate.

1.3.3. End Users.

End Entities or Users are the physical or legal persons authorized to apply for and obtain an electronic certificate in the conditions laid down in this Certification Practice Statement and in the Certification Policies in force for each type of certificate.

For the purposes of this Certification Practice Statement and the Certification Policies that implement it, the following are End Users of the ACEDICOM certification system:

- Applicants
- Subscribers
- Trusted third parties

1.3.3.1. Applicants.

Applicant is the physical person who, in their own name or on behalf of a third party, and following identification, requests the issue of a *Certificate*. In the case of a Certificate Applicant whose Subscriber is a legal person, said physical person may only be an administrator or legal representative of the legal person who is to be the subscriber of the certificate or, where indicated, a voluntary representative with sufficient power of attorney containing a special clause requesting the Certificate of Legal Personality from ACEDICOM.

1.3.3.2. Subscribers.

For the purposes of this CPS, the *subscriber* of ACEDICOM certificates corresponds to the term signatory/*signer* established in article 6 of Law 59/2003 on Electronic Signature.

The holder of the certificate will have the condition of subscriber. This means the physical or legal person whose personal identity is linked with the signature creation and verification data, signed electronically, through a public key certified by the Certification Service Provider.

The signer assumes the responsibility for safekeeping of the signature creation data, without ceding their use to any other person under any circumstances.

The group of users who can apply for the issue of ACEDICOM certificates is defined and limited by each Certification Policy.

Generically, and notwithstanding that stipulated by the Certification Policy applicable in each case, it is established that the possible subscribers are the set of EDICOM services and applications clients.

1.3.3.3. Trusting parties.

All those who voluntarily trust certificates issued by ACEDICOM will be considered trusting parties or trusting third parties.

The Certification Policies applicable in each case limit the right to trust in certificates issued by ACEDICOM.

Generically, and notwithstanding that stipulated by the Certification Policy applicable in each case, the employees, systems and applications of EDICOM are established as third parties that trust ACEDICOM certificates.

1.4. USE OF CERTIFICATES.

This section lists the applications for which each type of certificate can be used, establishing limitations and prohibiting some applications of the certificates.

1.4.1 Typical uses of certificates.

The Certification Policies corresponding to each specific type of certificate issued by ACEDICOM constitute the documents in which the uses and limitations of each certificate are determined, although in this section, given its special relevance, we describe the main use of ACEDICOM recognized certificates based on secure signature creation devices.

The main purpose of certificates issued by ACEDICOM is to enable the subscriber to sign documents. This certificate (**qualified certificate** according to ETSI, the RFC3739 and the European Directive 99/93/EC and **acknowledged** in accordance with the Law on Electronic Signature) allows substitution of the handwritten signature for electronic in the

subscriber's relations with third parties (LFE 59/2003 artº 3.4). It can also be used to provide security in certain certified storage applications ("substitutive" in other legislations).

The signature certificates issued by ACEDICOM are recognized certificates in accordance with that set forth in article 11.1, with the content prescribed by article 11.2, and issued in compliance with the obligations of article 12, 13, and 17 to 20 of Law 59/2003, of 19th December, on electronic signature, and comply with the technical regulations of the European Telecommunications Standards Institute, identified by reference TS 101 456.

The certificates issued by ACEDICOM are published on secure signature creation device, as indicated in the certificate Certification Policies, in accordance with article 24.3, of Law 59/2003, 19th December. They therefore guarantee the identity of the subscriber holder of the private identification key and signature, and enable generation of the "recognized electronic signature"; i.e., the advanced electronic signature based on a recognized certificate and which has been generated using a secure device, whereby, in accordance with that stipulated in article 3 of Law 59/2003, of 19th December, is compared to the handwritten signature for legal purposes, with no need to fulfil any other additional requirement.

The use of these certificates provides the following guarantees:

- No rejection of origin.

It ensures that the document comes from the subscriber that it purports to. This feature is obtained by means of electronic signature by **Signature Certification**. The receiver of a message signed electronically can verify the certificate used for the signature using the ACEDICOM validation service. In this way they guarantee that the document comes from a certain subscriber.

Since ACEDICOM certificates are on secure signature creation devices and the signature keys remain under the control of the holder subscriber from the moment of their creation, agreement of the same with the signature is guaranteed ("non-rejection" guarantee).

- Integrity

Use of the **Signature Certificate** lets you check that the document has not been modified by any outside of the communication. To guarantee integrity, cryptography provides solutions based on functions of special features called summary functions, which come into play whenever an electronic signature is used. The use of this system lets you check that a signed message has not been altered between sending and reception. To this end, a unique summary of the document is signed with the private key so that any alteration of the message results in an alteration of its summary.

1.4.2. Prohibited uses.

The Certificates issued by ACEDICOM will only be used for the function and purpose that is stipulated in this Certification Practice Statement

and in the corresponding Certification Policies, in accordance with the regulation in force.

The contracting of certificates from ACEDICOM admits only the use of the certificate in the area of activity of the APPLICANT or the organisation to which they are linked, in accordance with the purpose of the type of Certificate requested. Once the Certificate is issued, the APPLICANT may not, except by specific agreement between the parties, make use of the same for commercial purposes. Commercial use of the certificate is understood as any action whereby the APPLICANT offers services to third parties not signatories to the present contract, whether for a consideration or gratuitously, requiring the use of the contracted certificate.

In any case, ACEDICOM certificates have not been designed, nor may be destined or authorized for resale as equipment for control of dangerous situations or for uses that require foolproof actions, such as the operation of nuclear facilities, positioning systems or air services, or armament control systems, where an error could directly entail death, personal injuries or severe environmental damage.

1.4.3. Reliability of the electronic signature over time.

In order to guarantee the reliability of an electronic signature over time, it must be complemented with the information on the status of the associated certificate at the moment at which the same took place and/or non-repudiable information incorporating a time seal, as well as the certificates that make up the chain of confidence.

This means that if we want to have a signature that can be validated over time, the electronic signature that is generated must include evidence of its validity so that it cannot be repudiated. For this type of signature there must be a service that maintains the evidence, and it will be necessary to ask for the signature update before the keys and the associated cryptographic material become vulnerable.

The generation of a long lasting signature must include the following elements:

Time stamp: The signature must include a time stamp issue by a Trusted Third Party, TSA (Time Stamping Authority). The time stamp ensures that both the original data of the document and the information on the status of the certificates were generated before a certain date. The time stamp format must comply with the standard defined in RFC3161.

Revocation information: The signature must include an element that ensures that the signature certificate is valid. This element will be generated by a Trusted Third Party, in this case by ACEDICOM.

The signatures must be able to be renewed (re-signed) and the confidence elements (time stamps) updated to make the electronic signatures valid over time, guaranteeing their reliability.

1.5. ADMINISTRATION OF THE POLICIES.

1.5.1. Entity responsible for the CPS.

| | |
|-----------------------|------------------------------------|
| Name: | <i>EDICOM Technical Management</i> |
| E-mail address | <i>acedicom@edicomgroup.com</i> |

| | |
|-------------------------|---|
| Address | <i>C/ Auguste y Louis Lumiere, 12B - Parque Tecnológico, 46980 Paterna (Valencia) SPAIN</i> |
| Telephone number | <i>+34.902 119 229</i> |
| Fax number | <i>+34.96 348 16 88</i> |

1.5.2. Contact person for CPS

| | |
|-------------------------|---|
| Name: | <i>EDICOM Systems Department</i> |
| E-mail address | <i>acedicom@edicomgroup.com</i> |
| Address | <i>C/ Auguste y Louis Lumiere, 12B - Parque Tecnológico, 46980 Paterna (Valencia) SPAIN</i> |
| Telephone number | <i>+34.902 119 229</i> |
| Fax number | <i>+34.96 348 16 88</i> |

1.5.3. Competence to determine CPS compliance with the different Certification Policies.

The EDICOM Technical Management is the competent organ to determine the compliance of this CPS with the different Certification Policies from the EDICOM Certification Authority.

1.5.4 Approval procedure.

The ACEDICOM documentary and organization system guarantees, by the existence and application of the corresponding procedures, the correct maintenance of the Certification Practice Statement and the service specifications related with it.

In this way, the service specification modification procedure and the publication procedure service specifications are anticipated.

The final policy modifications are approved by ACEDICOM after verifying the fulfilment of the requirements established in the corresponding sections of this CPS.

1.6. DEFINITIONS AND ACRONYMS.

1.6.1. Definitions.

In order to determine the scope of the concepts that are used in this Certification Practice Statement, and in the different Certification Policies, the following must be understood:

- **Certification Authority:** The physical or legal person who, in accordance with the legislation on electronic signature, issues electronic certificates, also being able to provide other electronic signature related services. For the purposes of this Certification Practice Statement, all those all that are defined in the same as such are Certification Authorities.
- **Registration Authority:** Physical or legal person appointed by ACEDICOM to verify the identity of certificate applicants and subscribers, and, where indicated, the power of representatives and the subsistence of the legal personality or voluntary representation. In ACEDICOM they are also known as PRUs or User Registration Points.
- **Certification chain:** List of certificates that contains at least one certificate and the root certificate from ACEDICOM.

- *Certificate*: Digital document electronically signed by a Certification Service Provider that links the subscriber with signature verification data and confirms their identity. In this Certification Practice Statement, when certificate is mentioned it is understood to mean a Certificate issued by ACEDICOM.
- *Root certificate*: Certificate whose subscriber is ACEDICOM and which belongs to the ACEDICOM Certification Service Provider hierarchy, and contains the signature verification data of said Authority signed with the signature creation data of the same as Certification Service Provider.
- *Recognized certificate*: Certificate issued by a Certification Service Provider that fulfils the requirements stipulated by Law concerning the verification of the identity and other circumstances of the applicants and the reliability and the guarantees of the certification services rendered, in accordance with that set forth in Chapter II of Law 59/2003, of 19th December, on Electronic Signature.
- *Key*: Sequence of symbols.
- *Signature creation data (Private Key)*: Unique data, such as private codes or cypher keys, which the subscriber uses to create the Electronic Signature.
- *Signature verification data (Public Key)*: The data, such as public codes or cypher keys that are used to verify the Electronic Signature.
- *Certification Practice Statement*. ACEDICOM declaration made available to the public and free of charge as Certification Service Provider in compliance with that stipulated by Law.
- *Secure signature creation device*: Instrument that serves to apply the signature creation data in accordance with the requirements set forth in article 24.3 of Law 59/2003, of 19th December, on Electronic Signature.
- *Certificate Directory*: Repository of information that follows the ITU-T X.500 standard.
- *Electronic document*: Set of logical records stored in support readable by electronic data processing equipment, which contains information.
- *Security document*: Document demanded by Organic Law 15/99 on Protection of Data of a Personal Nature whose purpose is to establish the safety measures implanted, for the purposes of this document, by ACEDICOM as Certification Service Provider, for the protection of the data of personal nature contained in the certification activity Files that contain personal data (hereafter the Files).
- *Responsible for Processing*: The physical or legal person, public authority, service or any other organism that deal with personal data on behalf of the person in charge of processing the files.
- *Recognized electronic signature*: The advanced electronic signature based on a certificate acknowledged and generated by means of a secure signature creation device.
- *Advanced electronic signature* The electronic signature that allows us to establish the personal identity of the subscriber with respect to the signed data and to verify the integrity of the same, being exclusively linked to both the subscriber and the data to which it refers, having been created by means maintained under their exclusive control.

- *Electronic signature*: The data set in electronic form, consigned along with others or associated with them, which can be used as a means of personal identification.
- *Hash function*: n operation carried out on a data set of any size, so that the result obtained is another data set of fixed size, independently of the original size, and which has the property of being associated univocally to the initial data. This means that it is impossible to find two different messages that generate the same result when applying the Hash Function.
- *Hash or digital fingerprint*: Fixed size result that it is obtained after applying a hash function to a message and which fulfils the property of being univocally associated with the initial data.
- *Public Key Infrastructure (PKI)*: Infrastructure that supports the issue and management of keys and certificates for authentication, coding, integrity, or non repudiation services.
- *Certificate Revocation Lists or Revoked Certificate Lists*: List where only the revoked or suspended certificates appear (not those expired).
- *Security Hardware Cryptographic Module*: Hardware module used to carry out cryptographic functions and store keys securely.
- *Certificate serial number*: Whole and unique value that is associated unequivocally with a certificate issued by ACEDICOM.
- *OCSP (Online Certificate Status Protocol)*: IT protocol that enables verification of the state of a certificate at the moment it is used.
- *OCSP Responder*: IT server that responds, following OCSP protocol, to OCSP requests with the status of the certificate being consulted.
- *OID (Object Identifier) Value*, of hierarchic nature and consisting of a variable components sequence although always constituted by non-negative whole numbers separated by a point, which can be assigned to registered objects and have the property of being unique among the rest of the OIDs.
- *OCSP request*: Consultation request on the state of a certificate to the OCSP Responder following OCSP protocol.
- *PIN*: (Personal Identification Number) specific number known only by the person that has to access a resource that is protected by this mechanism.
- *Certification Service Provider*: The physical or legal person who, in accordance with the legislation on electronic signature, issues electronic certificates, also being able to provide other electronic signature related services. In this Certification Practice Statement, it will correspond to the Certification Authorities belonging to the ACEDICOM hierarchy.
- *Certification Policy*: Document that completes the Certification Practice Statement, establishing the conditions of use and the procedures followed by ACEDICOM to issue Certificates.
- *PKCS#10 (Certification Request Syntax Standard)*: Standard developed by RSA Labs, and accepted internationally as standard, which defines the syntax of a certificate request.
- *PUK*: (Personal Unblocking Key) specific number or key known only by the person who has to access a resource, which is used to unblock the access to this resource.
- *Recertification*: Revocation of a user certificate before issuing the user with a new certificate with the same features as the revoked one,

not necessarily signed with the same CA that issued the revoked certificate.

- **File Manager (or File Processing Manager):** Person who decides on the purpose, content and use of the treatment of the Files.
- **Security Manager:** In charge of coordinating and controlling the measures that the security document imposes on the files.
- **SHA-1:** Secure Hash Algorithm (secure summary algorithm - hash-). Developed by NIST and revised in 1994 (SHA-1). The algorithm consists of taking messages of less than 264 bits and generating a summary of 160 bits in length. The probability of finding two different messages that produce the same summary is practically null. This is why it is used to ensure integrity of documents during the electronic signature process.
- **Time stamp:** Establishment of the date and time in an electronic document by means of indelible cryptographic procedures, based on the Request For Comments specifications: 3161 - "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)", which dates the document objectively.
- **Applicant:** Physical person who upon identification, asks for the issue of a certificate.
- **Subscriber (or Subject):** The certificate holder or signer. The person whose personal identity is linked with the signature creation and verification data signed electronically, through a public key certified by the Certification Services Provider. The subscriber concept will be referred in certificates and IT applications related with its issue as Subject, for strict reasons of international standardization.
- **Cryptographic card:** Card used by the subscriber to store private signature and deciphering keys and generate electronic signatures and decipher data messages. It has the consideration of secure signature creation device in accordance with the Law and enables the generation of recognized electronic signature.
- **Trusting third parties or trusting parties:** Those persons who deposit their confidence in an ACEDICOM certificate, verifying the validity and use of the certificate according to that described in this Certification Practice Statement and in the Certification Policies associated with each type of certificate.
- **X.500:** Standard developed by the UIT that defines the directory recommendations. Corresponds with the ISO/IEC 9594-1 standard: 1993. It gives rise to the following series of recommendations: X.501, X.509, X.511, X.518, X.519, X.520, X.521 and X.525.
- **X.509:** Standard developed by the UIT, which defines the basic electronic format for electronic certificates.

1.6.2. Acronyms.

| | |
|-----------------|--|
| ACEDICOM | EDICOM Certification Authority |
| CA | Certification Authority |
| CP | Certificate Policies |
| CPS | Certification Practice Statement |
| CRL | Certificate Revocation List |
| FIPS | Federal Information Processing Standards |
| HSM | Hardware Security Module |

| | |
|------------------|-------------------------------------|
| <i>IETF</i> | Internet Engineering Task Force |
| <i>OID</i> | Object Identifier |
| <i>OCSP</i> | Online Certificate Status Protocol |
| <i>OPRU</i> | Registration Point Operator |
| <i>PKI</i> | Public Key Infrastructure |
| <i>PKIEDICOM</i> | EDICOM PKI |
| <i>PRU</i> | User Registration Point |
| <i>RA</i> | Registration Authority |
| <i>RFC</i> | Request For Comment |
| <i>Sub CA</i> | Subordinate Certification Authority |

2. INFORMATION PUBLICATION AND CERTIFICATE REPOSITORY.

2.1. REPOSITORIES.

The ACEDICOM repository service will be available 24 hours of a day, 7 days a week, and in the event of interruption due to force majeure, the service will be recovered in the shortest possible time.

Understanding by availability the ability to access the service on demand, independently of the speed or rate at which it is provided.

In no case may this availability be less than **99.5%** in prime time (Monday to Saturday from 08:00 to 00:00 hours and from 00:00 to 02:00) and **99%** the rest of the time, measured over a monthly period.

EDICOM reserves up to a maximum of 1 hour daily outside the primary schedule of Monday to Friday and up to 3 Hours on alternate Saturdays and Sundays and at the point of minimum activity to carry out maintenance tasks, system backups, etc.

This time will be excluded from the service level calculations.

If there is a faulty operation of the systems that run the Services, EDICOM will inform the Client as soon as reasonably possible about the problem and the time anticipated for normal provision to resume. EDICOM will provide the Client with user attention centre resources and will do everything possible to rectify the problem in the shortest possible time.

In the event of disasters, a complete disaster recovery plan will be invoked if the interruption of the service is expected to last more than 48 hours. EDICOM will maintain the plan updated in line with the company's best practices.

The ACEDICOM repository does not contain any information of a confidential nature.

ACEDICOM does not use any other repository operated by any entity other than ACEDICOM.

2.2. PUBLICATION.

The CAs belonging to the ACEDICOM trust hierarchy are obliged to publish the information relating to their practices, their certificates and the updated status of these certificates.

This CPS is public and is available on the ACEDICOM website: <http://acedicom.edicomgroup.com>, in PDF format.

ACEDICOM Certification Policies are public and available in PDF format on the ACEDICOM website: <http://acedicom.edicomgroup.com>.

The ACEDICOM CA certificate is public and available in the ACEDICOM repository in X.509 v3 format. It is also available at <http://acedicom.edicomgroup.com>.

The list by ACEDICOM revoked certificate is public and available in CRL v2 format. Also available at <http://acedicom.edicomgroup.com>.

2.3. UPDATE FREQUENCY.

The CPS and the Certification Policies will be published whenever they are modified.

The CA will add certificates revoked to the pertinent CRL within the period of time stipulated in point 4.9.9 *CRL issuing frequency*.

2.4. CERTIFICATE REPOSITORY ACCESS CONTROLS.

Access to reading the information in the ACEDICOM repository and their website is free.

Only ACEDICOM is authorized to modify, replace or delete information from the repository and website. In this sense, ACEDICOM uses suitable means of control to restrict the writing or modification capacity of these elements.

3. CERTIFICATE HOLDER IDENTIFICATION AND AUTHENTICATION.

3.1. NAME REGISTRATION.

This section sets out requirements relating to the identification procedures and authentication that are used during the registration of Linked Certification Entities (if there are any) and subscribers, which must be done prior to the issue and delivery of certificates.

3.1.1. Name types.

The *Subject DN (Distinguished Name)* field contains all the identification information of the entity, or legal, physical person, or any other type, for which the certificate is issued. This information must univocally identify a certificate issued by the same CA, in other words: There must not be certificates issued by the same CA whose *Subject* is identical.

It is very important in the case of recognized certificates (*Qualified Certificates*) to take into account that the *commonName (CN)* content must be a valid name of the certificate subject. Only the name and surnames will be considered as valid. The use of pseudonyms is not allowed.

In addition, it is necessary to consider that many implementations presuppose the presence of the *commonName* attribute, and use its content to show the name of the subject, independently of other attributes such as *givenName*, *surname*, or *pseudonym*.

In addition, recognized certificates (*Qualified Certificates*) must always be issued to physical persons, as indicated in the ETSI TS 101 862 standard (*Qualified Certificate Profile*) and in RFC 3739, section 2.1.

All the following attributes must appear, unless it depends on some factor (indicating "if indicated"). For example, if a person is autonomous instead of representing a company, in this case they would not have to use the attributes O, OU, etc.

| | |
|-----------------------------|--|
| CN | Name and surnames |
| SN (Serial | NIF |
| Number) | |
| GN | First name |
| S | Surnames |
| T | Post held in the organization to which they belong (if indicated) |
| | Distinguished Name Identifier. Obligated by Italian legislation. |
| DN Qualifier | It is an authenticator given by the certificate issuer to identify the subject of the same univocally. The NIF will be used. |
| OU | Department of the company/entity to which they belong (if indicated) |
| O | Company/organization to which they belong (if indicated) |
| C | ISO country code (ES, FR, IT, MX, etc) |
| OID | |
| 1.3.6.1.4.1.30051 | CIF of the entity represented by the subject (if indicated) |
| .3.1.1 | |

3.1.2. Meaning of names.

The rules defined in the previous section guarantee that the distinguishing names (DN) of certificates are sufficiently significant to link the public key with an identity.

3.1.3. Name format interpretation.

The rule used by ACEDICOM to interpret the distinguishing names of certificates it issues are those contained in ISO/IEC 9595 (X.500) Distinguished Name (DN).

3.1.2. Uniqueness of names.

The distinguishing names must be unique and must not give rise to ambiguity.

The DN of certificates cannot be repeated. The use of the CIF number of the company and the NIF of the applicant guarantees the uniqueness of the DN.

The Certification Policies can have the substitution of this uniqueness mechanism.

3.1.5. Resolution of name-related conflicts.

The inclusion of a name in a certificate does not imply the existence of any right over the same, notwithstanding the better right than may be held by third parties.

ACEDICOM does not act as arbitrator or mediator, nor resolve any dispute relating to the ownership of names of persons or organizations, domain names, brand or commercial names, etc.

ACEDICOM reserves the right to refuse a certificate request because of conflict over the name.

3.1.6. Recognition, authentication and function of registered trade names.

Not stipulated.

3.2. INITIAL IDENTITY VALIDATION.

3.2.1. Private key possession proof methods.

It will be necessary to rely on what is established in each case in the Certification Policy applicable for each request.

3.2.2. Authentication of identity of an entity.

Authentication of the identity of an organization or entity will be by means of the presentation to the Registration Point Operator qualified for the issue of this type of certificates on behalf of the applicant for the entity certificate (administrator, legal representative or representing volunteer with sufficient authorization) once its identity is credited as defined in point 3.2.3 of the documentation set forth in

paragraph four of this point, and the extension and use of their faculties of representation over that entity.

The ACEDICOM Registration Point Operator checks the data relating to the constitution and legal personality and the extent and use of the faculties of representation or voluntary representation of the applicant by means of public document that serves to accredit the details cited reliably and their inscription in the corresponding public registry if indispensable. Said verification may also be implemented by means of consultation in the public register where the constitution and empowerment documents are inscribed, being able to use the telematic means provided by said public registers.

If the recognized certificates admit other forms of representation, accreditation of the circumstances on which they are based will be demanded previously, in the same form anticipated previously. When the recognized certificate contains other personal circumstances or attributes of the applicant, such as their condition as holder of a public position, their membership of a professional school or holder of its degree, these will have to be verified by means of the official documents that accredit them, in accordance with their specific regulation.

The documentation that is required to carry out the verifications varies based on the type of body for which the certificate is requested. To this end, and with general character, the following documentation will be provided:

- When applying for an electronic certificate for any trading company or any company of obligatory inscription in the Mercantile Registry (Joint-stock Company, Public Limited Company, Limited Liability Company, Worker-owned Limited Company, Sporting Associations, Partnerships, Limited Partnerships or Cooperatives, Economic Interest Groupings, Joint Ventures, others.), a certificate must be provided from the Mercantile Register relating to the constitution, legal personality, appointment and term of the position of administrator or legal representative, issued during the 10 days prior to the date of presentation of the certificate application in ACEDICOM. If the representation is voluntary, the certificate of appointment and term of the position may be replaced by the sufficient power of attorney, with the special clause authorizing the Legal Person/Body Corporate Certificate application.
- To apply for a certificate for Associations, Foundations, Clubs, Political Parties, Trade Unions or Cooperatives not inscribable in the Mercantile Register, a certificate from the public registry where they are inscribed must be provided, relating to the constitution, legal personality, appointment and term of the position of administrator or legal representative, issued during the 10 days prior to the date of presentation of the certificate application in ACEDICOM. If the representation is voluntary, the certificate of appointment and term of the position may be replaced by the sufficient power of attorney, with the special clause authorizing the Legal Person/Body Corporate Certificate application.

- To apply for an electronic certificate for Private Companies and Communities of Goods, the Constituent Title or Statutes of the Private Company, along with the NIF, the certificate of appointment of the President/Chair or organ of administration and the responsible declaration of the President/Chair (or administrative organ) on the term of their position must be provided, or sufficient power of attorney with special clause authorizing the application for certificate of legal personality, granted by the President/Chair or organ of administration to the voluntary representative.
- In all cases, the applicant must accompany the documentation with the "DIGITAL CERTIFICATION SERVICES SUPPLY CONTRACT" which can be downloaded from the ACEDICOM website: <http://acedicom.edicomgroup.com>

ACEDICOM will keep a copy of the documentation presented by the applicant.

Once all these checks are carried out, a request for issue of the certificate is created in the IT system, sending it securely and electronically to ACEDICOM.

In the event that a Certification Policy deems necessary another authentication procedure for the identity of an entity, the policy will establish the methods needed for the verification of said identity.

Methods based on registration documentation that were submitted by mandatory physical means will be admitted as indirect means of authentication (TS 101 456).

3.2.3. Individual identity authentication.

The individual identification process is defined by the Certification Policy applicable to each type of certificate. As a general rule, either physical appearance to the Operator of the Point of Registry or else remote identification can be used for this purpose.

When the authentication of the identity of the applicant for a certificate is done by means of their appearance before the Registration Point Operator, it will be accredited by presentation of a valid official identity document and in vigour, such as National Identity Document, passport, or the Foreigner Identification Number (NIE) of the applicant and will explicitly verify the date and the place of birth.

When the authentication is done remotely, in general no methods of identification other than the digital signature with certificates issued by ACEDICOM or some other Services of Certification Service Provider that issues recognized certificates will be used.

It is also possible to do without the physical presence if the signature contained in the request for issue of a certificate has been legitimized by notary, and in the cases anticipated by article 13.4 of Law 59/2003, of 19th December.

3.3. KEY RENEWAL REQUEST IDENTIFICATION AND AUTHENTICATION.

3.3.1. Identification and authentication of routine renewal requests.

The identification and authentication for renewal of the certificate can be done using the techniques for authentication and initial identification, or using requests signed digitally by means of the original certificate that is to be renewed, as long as it has not expired or been revoked. There are, therefore, two alternative mechanisms for renewal:

- Signed web forms in the "Certificate Management" Area available at <http://acedicom.edicomgroup.com>.
- Personal appearance at any User Registration Point, with sufficient identification documents (see section 3.2.2 and 3.2.3 of this CPS).

Likewise, and in accordance with that stipulated in art. 13.4 b) of Law 59/2003, of 19th December, on Electronic Signature, the renewal of the certificate by means of digitally signed requests will demand that a period of time of less than five years has passed since the personal identification.

3.3.2. Key renewal request identification and authentication after a revocation – Key not compromised.

The identification and authentication policy for renewal of a certificate after a revocation without compromise of the key will be the same as for initial registration, as described in this document in point 3.2.3., so that the identity of the applicant and the authenticity of the request are guaranteed trustworthily and unequivocally.

3.4. KEY REVOCATION REQUEST IDENTIFICATION AND AUTHENTICATION.

The revocation request process is defined by the Certification Policy applicable to each type of certificate. The identification policy for revocation requests may be the same as for initial registration. The authentication policy will accept digitally signed requests for revocation by the certificate subscriber.

ACEDICOM or any of the entities that compose it may officially request the revocation of a certificate if they have knowledge or suspect that the private key of the subscriber has been compromised, or any other fact that recommends undertaking this action.

The general revocation procedure is described in this Policy in point 4.9.3. In any case, the different Certification Policies may define other, less severe identification policies, and can define the creation of a revocation password at the moment of registration of the certificate.

4. THE LIFE CYCLE OF CERTIFICATES.

The specifications contained in this section are notwithstanding the stipulations anticipated in each of the different Certification Policies for the different types of certificates issued by ACEDICOM.

4.1. CERTIFICATE APPLICATIONS

The ACEDICOM Registration Authority that receives the application is responsible for determining that the type of certificate requested is in line with the specific characteristics of the applicant, in accordance with the content of the Certification Policy applicable to said certificate and, in this way, for resolving the application formulated. In each Certification Policy, the information that must be provided previously to certificate applicants is specified.

4.2. CERTIFICATE REQUEST TRANSACTIONS.

The Registration Authority or Entity is responsible for the verification of the identity of the applicant, verification of the documentation and proof that the applicant has signed the application document in person (DIGITAL CERTIFICATION SERVICES PROVISION CONTRACT). Once it completes the request and carries out the pertinent verifications, the Registration Authority will proceed to make the issue request to the ACEDICOM Certification Authority and save a copy of the request and the associated documentation.

4.3. ISSUING CERTIFICATES.

ACEDICOM is not responsible for the monitoring, investigation or confirmation of the exactitude of the information contained in the certificate after its issue. In the event of receiving information on the inaccuracy or current non-applicability of the information contained in the certificate, it may be revoked.

The certificate will be issued once ACEDICOM has made the verifications necessary to validate the certification request. The mechanism whereby the nature and the way to carry out these verifications is determined is the Certification Policy.

When the ACEDICOM issues a certificate in accordance with a valid certification request, it will notify the Registration Entity that forwarded the application and will keep the same in the ACEDICOM repository.

ACEDICOM:

- a. Uses a certificate generation procedure that securely links the certificate with the registration information, including the certified public key.
- b. Protects the confidentiality and integrity of the registry data.
- c. Takes measures against the falsification of certificates.

It is the task of the Registration Entity to notify the subscriber of a certificate of the issue of the same and provide them with the access data to the same.

Everything specified in this section is subordinate to that stipulated by the different Certification Policies for the issue of each type of certificate.

4.4. ACCEPTING CERTIFICATES.

The acceptance of certificates by the signers takes place at the moment of signature of the "DIGITAL CERTIFICATION SERVICES PROVISION CONTRACT" associated with each Certification Policy. Acceptance of the contract implies the acknowledgement and acceptance by the subscriber of the associated Certification Policy.

4.5. USE OF THE PAIR OF KEYS AND THE CERTIFICATE.

ACEDICOM certificates, as stipulated in the specific policies, are recognized certificates for identification and advanced electronic signature, for the use of physical persons or legal organisations (known collectively as subscribers) that need to engage in relations with the Public Administrations and other institutions or companies in the Electronic Data Interchange area and/or to equip themselves with certified storage systems.

Third Party Acceptors may only deposit their trust in certificates for that established in this CPS and in accordance with that set forth in the 'Key Usage' field of the certificate.

In any case, ACEDICOM certificates have not been designed, nor may be destined or authorized for use or resale as equipment for control of dangerous situations or for uses that require foolproof actions, such as the operation of nuclear facilities, positioning systems or air services, or armament control systems, where an error could directly result in death, personal injuries or severe environmental damage.

4.6. CERTIFICATE RENEWAL.

The certificate renewal period must be initiated 70 days before the expiry date of the certificate. These steps are explained in section 3.3.

4.7. KEY RENEWAL.

Renewing keys necessarily involves renewal of the certificate and they may not be carried out as separate processes.

4.8. CERTIFICATE MODIFICATION.

All circumstances that would make it necessary to carry out modifications in certificates issued to a subscriber by variation of the data contained in the same, would also oblige the changing of the physical support whereby they are processed, as well as renewal of the support by variation of data, the previous sections being applicable.

4.9. CERTIFICATE REVOCATION AND SUSPENSION.

Next, we shall look at aspects to consider for the revocation and suspension of certificates.

4.9.1. Circumstances for revocation.

A certificate is revoked when:

- The certificate subscriber or their keys or the certificate keys have been compromised by:

- Theft, loss, disclosure, modification, or any other compromise or suspicion of compromise of the user's private key.
- The deliberate misuse of keys and certificates, or the lack of observation of the operational requirements in the subscription agreement, the associated CP or this CPS.
- The defective issue of a certificate takes place due to:
 - Failure to satisfy a material prerequisite for the issue of the certificate.
 - A fundamental factor in the certificate is known to be, or there is reasonable suspicion to suppose that it may be false.
 - A data input error or any other processing error.
- The information contained in a certificate or used to apply for it becomes inexact, for example when the owner of a certificate changes their name.
- A valid revocation request being received from an end user.
- A valid revocation request being received from an authorized third party, for example by judicial order.
- Revocation of a certificate from a superior RA or CA in the trust hierarchy of the certificate.
- Cessation of the activity of the certification service provider.

4.9.2. Entity that may apply for revocation.

The revocation of a certificate can be requested both by the subscriber of the same and by ACEDICOM.

The certificate subscribers can request their revocation for any reason and must apply for it under the conditions specified in the following section.

4.9.3. Revocation request procedure.

The revocation request procedure of each type of certificate will be defined in the corresponding Certification Policy.

In general terms, and notwithstanding that defined in the Certification Policies:

- Remote requests for revocation will be accepted if they are digitally signed with a certificate from ACEDICOM or any other recognized Certification Service Provider that issues Qualified Certificates. Applications in person will be accepted if the user identification requirements set out for initial registration are fulfilled.
- After revocation of the certificate, the certificate subscriber must destroy the private key corresponding to the same and not make use of the revoked certificate.

There is a certificate revocation application form available on the ACEDICOM website: <http://acedicom.edicomgroup.com>

A revocation request, whether submitted on paper or electronically, must contain the information described in the revocation request form included in each of the Certification Policies. Nevertheless, ACEDICOM is committed to immediately publish the new status of the certificate by means of OSCP as soon as the reasons for the revocation requested are stated. Likewise, the certificate will be included in CRL lists

published by ACEDICOM in the next CRL renewal cycle, with 24 hour regularity.

Subscribers will be notified of the changes of status in their certificates by e-mail.

4.9.4. Revocation request grace period.

Revocation will take place immediately after the processing of each request verified as valid. No period of grace is therefore associated with this process.

4.9.5. Circumstances for suspension.

Not considered.

4.9.6. Entity that may apply for suspension.

Not considered.

4.9.7. Suspension request procedure.

Not considered.

4.9.8. Suspension period limits.

Not considered.

4.9.9. Frequency of issue of CRLS.

ACEDICOM will publish a new CRL in the repository at 24 hour intervals maximum, even though no modifications have taken place in the same (changes in certificate status) during said period. This period is not affected in the event of certificate revocations, which already obtain immediate response in the publication by OCSP.

The CRLs are generated and signed with the CA key.

4.9.10. CRL checking requirements.

Verification of the revocations is obligatory for each use of public identity certificates. The ordinary procedure for verification of the validity of a certificate will be by query to the ACEDICOM Validation Services, which will indicate the status of the certificate by OCSP protocol.

ACEDICOM also provides for publication of CRLs.

Subscribers will be notified of the changes of status in their certificates by e-mail.

4.9.11. Other revoked certificate notification methods.

ACEDICOM may establish other forms of notification of revocation of certificates in the future.

4.9.12. Special renewal requirements for compromised keys.

There is no variation in the previous clauses when the revocation is due to the private key being compromised.

4.10. CERTIFICATE STATUS CHECKING SERVICES.

4.10.1. Operating Features.

For certificate validation, ACEDICOM has online Validation Services, in addition to the publication of CRLs, which provide information on the status of certificates issued by the ACEDICOM certification hierarchy. This is an online validation service (Validation Authority, VA) that implements the Online Certificate Status Protocol according to RFC 2560. By the use of this protocol, the current status of an electronic certificate is determined without requiring the CRLs. An OCSP client sends a query about the status of the certificate to the VA, which, after consulting its DBs, provides a response on the certificate status via HTTP.

To make use of the online Validation Service it is the responsibility of the Third Party Acceptor to have an OCSP Client in compliance with RFC 2560.

4.10.2. Service Availability.

The CRLs and certificate status online query systems are available 24 hours a day, 7 days a week.

Understanding by availability the ability to access the service on demand, independently of the speed or rate at which it is provided.

In no case may this availability be less than **99.5%** in prime time (Monday to Saturday from 08:00 to 00:00 hours and from 00:00 to 02:00) and **99%** the rest of the time, measured over a monthly period.

EDICOM reserves up to a maximum of 1 hour daily outside the primary schedule of Monday to Friday and up to 3 Hours on alternate Saturdays and Sundays and at the point of minimum activity to carry out maintenance tasks, system backups, etc.

This time will be excluded from the service level calculations.

If there is a faulty operation of the systems that run the Services, EDICOM will inform the Client as soon as reasonably possible about the problem and the time anticipated for normal provision to resume. EDICOM will provide the Client with user attention centre resources and will do everything possible to rectify the problem in the shortest possible time.

In the event of disasters, a complete disaster recovery plan will be invoked if the interruption of the service is expected to last more than 48 hours. EDICOM will maintain the plan updated in line with the company's best practices.

4.11. CONCLUSION OF THE SUBSCRIPTION.

The subscription finalizes with the expiration or revocation of the certificate.

4.12. KEY DEPOSIT AND RECOVERY.

The ACEDICOM can issue two types of recognized certificates on the basis of their support:

On secure device or Software. Only in the former case, the support hardware of the certificates issued by ACEDICOM is certificate CWA14169. The signature creation data (the private keys) are generated within the hardware and cannot be exported in any case. Depositing the private keys is done by ACEDICOM only in the case of centralized SSCD devices, although only the user has access to the same by means of the corresponding activation data which only they know.

The particular details are included in the Certification Policies associated with each type of certificate.

5. PHYSICAL SECURITY, MANAGEMENT AND OPERATIONAL CONTROLS.

5.1. PHYSICAL SECURITY CONTROLS.

ACEDICOM offers its subscribers the highest level of physical security to carry out essential tasks in the generation and management of certificates.

To this end, it has facilities with several security perimeters around the certificate generation services, cryptographic devices and revocation management.

In this way, ACEDICOM controls the physical and environmental security of the facilities and the systems that are in these facilities, with the following measures:

- Physical access controls
- Protection against natural disasters
- Fire protection measures
- Support system failure (electrical energy, telecommunications, etc)
- Flooding
- Anti-theft protection
- Conformity and unauthorized entry
- Disaster recovery
- Unauthorized removal of equipment, information, supports and applications relating to components used for ACEDICOM services.

5.1.1. Location and construction.

The ACEDICOM information systems are located in Data Processing Centres with suitable levels of protection and solidity of construction and with monitoring 24 hours a day, 7 days a week.

5.1.2. Physical access.

ACEDICOM Data Processing Centres have several security perimeters, with different security requirements and authorizations. Among the equipment protected by the security perimeters are physical access control systems by combination and biometrics, video surveillance and recording systems, and intruder detection, among others.

5.1.3. Power supply and air conditioning.

The facilities have uninterrupted power supply systems with sufficient energy to maintain the electrical network independently during controlled system switch-off periods and to protect the equipment against electrical fluctuations that might damage them.

The switch-off of the equipment will only take place in the event of failure of the independent power generation systems.

The environmental conditioning system consists of several stand-alone equipment sets with capacity to maintain temperature levels within the optimal margins for operation of the systems.

5.1.4. Exposure to water.

The present location and design of the ACEDICOM IT room guarantee the non-existence of flood danger, although the necessary procedures have been designed to be able to detect the presence of water in the room.

5.1.5. Fire protection and prevention.

The ACEDICOM Data Processing Centres have automated systems for fire detection and extinguishing.

5.1.6. Storage system.

The sensitive information supports are stored securely in non-flammable closets and strongboxes, according to the type of support and the classification of the information contained in them.

These closets are in different premises to eliminate risks associated with a single location. Access to these supports is restricted to authorized personnel.

5.1.7. Waste disposal.

The disposal of magnetic and optical supports and information on paper is carried out safely following established procedures for this purpose, adopting formatting processes, permanent erasure, destruction or shredding based on the type of supports to be treated.

5.1.8. Remote backup.

Remote backup copies are made on a daily basis, being stored in premises near to the backup Data Processing Centre, where ACEDICOM operations would continue in the event of a serious incident or failure of the main Data Processing Centre.

5.2. PROCEDURAL CONTROLS.

The information systems and services of ACEDICOM operate securely, following pre-established procedures.

For security reasons, information on procedural controls is deemed a confidential matter and is only explained in summarized form.

5.2.1. Trusted roles.

The people who are to occupy these positions are formally designated by EDICOM the executive management.

The trustworthy functions include:

Registry Operator

They check the applicant's identity and create the "End Entity" in the CA by means of a web form. Authentication in the form will be by means of smartcard exclusively on the equipment authorized to this end.

This "End Entity" creation operation will be left "pending" and must be approved by a Registry Operator other than that which created the application.

Systems administrator

They will not have access to the CA keys.

They will not have access to the CA logs. It will be avoided by means of the CA software user properties.

They will be authenticated by smartcard with the CA software, which will not allow any other alternative method of authentication.

HSM Administrator

They will be responsible for generating the physical keys of the CA in the HSM and will have access to said keys in the HSM. They will not have access to copies of said keys. They will also take part in the CA activation process and recovery of keys in the HSM in the event of contingencies.

Systems operator

Their functions will be backup and operation in general. This role is not incompatible with that of systems administrator.

System auditor

Authorized to view the CA logs and audit them. The logs may be viewed through the web interface provided by the CA. Authentication by smartcard.

Only this Role will have access to the logs.

The Auditor must take charge of:

- .Checking the follow-up of incidents and events
- .Checking the protection of the systems (exploitation of vulnerabilities, access logs, users, etc.).
- .Checking alarms and physical security elements

Security Manager

Responsible for the definition and verification of all the physical and IT security procedures.

They must take care of:

- .Recording the entry of all the documentation required and enumerated.
- .Checking the coherence of the documentation with the procedures, assets inventoried, etc.

5.2.2. Number of people required per task.

At least two persons are required to activate the keys of the cryptographic hardware devices for key generation and storage. Modification of the CA configuration parameters involves authorized authentication by two people with sufficient privileges.

5.2.3. Identification and authentication for each role.

All the users authorized by ACEDICOM identify themselves by user name and password based access techniques that can be replaced by identification cards.

The authentication is complemented with the corresponding authorizations to access certain ACEDICOM information assets or systems.

Secret shared techniques are used as far as possible for access to critical resources.

5.3. PERSONNEL SECURITY CONTROLS.

ACEDICOM considers, in terms of staff controls, the following aspects:

- The information is kept confidential, providing the necessary means and maintaining an appropriate attitude when carrying out its

functions and, outside the labour scope, in everything referring to infrastructure security.

- It shall be diligent and responsible in the treatment, maintenance and safeguarding of the infrastructure assets identified in the policy, the security plans or this document.
- No non-public information is revealed outside the scope of the infrastructure, nor are any information supports removed at lower security levels.
- Any incident that is considered to affect the security of the infrastructure, or to limit the service quality, is reported to Security Manager, as soon as possible.
- The infrastructure assets are used for the purposes to which they have been assigned.
- User guides or manuals are required for the systems used, enabling them to carry out their function correctly.
- Written documentation setting out its functions and the security measures to which it is subject is required.
- The security manager makes sure that the previous point is executed, providing the area managers with all the necessary information.
- No software or hardware that is not specifically authorized in writing by systems manager shall be installed in any of the infrastructure systems.
- No information may be accessed voluntarily, or deleted or altered, unless specifically destined to the person or professional profile.

5.3.1. Background, qualification, experience, and accreditation requirements.

The Certification Authority requires that all the personnel who carry out tasks in its facilities must have sufficient qualification and experience in similar situations.

All personnel must meet the security requirements of the entity and must have:

- Knowledge and training in digital certification frameworks.
- Basic training on security in information systems.
- Specific training for their post.
- Academic qualification or equivalent experience in the industry
- Trusted roles must be free from conflicts of interests.

Qualifications and experience may be replaced by the appropriate education and training.

5.3.2. Background vetting procedures.

By checking the Curricula Vitae of the personnel. The police record will be requested from those persons that are to occupy a management or trusted position to ensure that they do not have a serious criminal record in the case of new personnel incorporations.

5.3.3. Training requirements.

Certification Authority personnel are subject to a specific training plan to carry out their function within the organization.

This training plan includes the following aspects:

1. Training in the basic legal aspects related with certification services provision.
2. Training in security of information systems.
3. Services provided by the Certification Authority.
4. Basic PKI concepts.
5. Certification Practice Statement and the pertinent Certification Policies.
6. Incident Management.

5.3.4. Training update requirements and frequency.

In view of technological changes in the area, introduction of new tools or modification of operative procedures, appropriate training will be provided for the personnel affected.

Training sessions will be held to deal with changes in the Certification Practice Statement, Certification Policies or other relevant documents.

5.3.5. Task rotation frequency and sequence.

No rotation plan has been defined for the allocation of tasks to the Certification Authority personnel.

5.3.6. Sanctions for unauthorized actions.

In the event of commission of any unauthorized action regarding the operation of the Certification Authority, disciplinary measures will be taken. Actions such as those that negligently or wilfully contravene the Certification Practice Statement or the pertinent Certification Policies will be considered unauthorized.

If any infraction takes place, the Certification Authority will suspend the access of the person/s involved to the whole Certification Authority information system immediately as soon as the fact is reported.

Additionally, based on the gravity of the infractions, disciplinary actions will be applied that include the suspension and dismissal of the person responsible for the harmful action.

5.3.7. Staff hiring requirements.

All Certification Authority personnel are subject to secrecy by signature of the confidentiality agreement subscribed when appointed to their post. In this agreement, in addition, they undertake to carry out their tasks in accordance with this Certification Practice Declaration, the ACEDICOM Information Security Policy and the procedures approved by ACEDICOM.

5.3.8. Documentation provided to personnel.

The ACEDICOM provides the documentation strictly required by its personnel at all times, so that they shall be sufficiently competent in accordance with that set forth in the corresponding section of this policy.

5.3.9. Periodic compliance checks.

Checking that the personnel have the necessary knowledge takes place when finalizing the training sessions and under the discretion of the educational staff in charge of giving these courses.

Annually, the Security Manager will carry out a review of the suitability of the authorizations given to the privileges currently granted to the employees.

5.3.10. Termination of contracts.

In the event of conclusion of the working relation with personnel carrying out their functions in ACEDICOM, the Security Manager will carry out the actions or checks detailed in the following points, or directly give instructions to this end to the appropriate staff.

5.3.10.1. Access to entity premises

Access privileges of the individual to the facilities of the entity whose access is restricted must be suppressed.

5.3.10.2. Access to Information Systems

The access privileges of the individual to the IS of the entity must be suppressed, with special attention to administration and remote access privileges.

5.3.10.3. Access to documentation

Suppression of access to all information, with the exception of information deemed PUBLIC.

5.3.10.4. Informing the rest of the organization

The rest of the entity must be informed of the individual leaving and the loss of their privileges. In this way, the intention is to reduce the possibility of "social engineering" attacks by the same.

5.4. SECURITY PROCEDURE CONTROLS.

5.4.1. Event types recorded.

ACEDICOM records all the events related with:

- .Successful or failed attempts to change the operating system security parameters.
- .Starting up and shutting down applications.
- .Successful or failed session start or finish attempts.
- .Successful or failed attempts to create, modify or deleted accounts from the system.
- .Successful or failed attempts to create, modify or deleted authorized system users.
- .Successful or failed attempts to request, generate, sign, issue or revoke keys and certificates.
- Successful or failed attempts to reactivate or renew certificates.
- .Successful or failed attempts to generate, sign or issue a CRL.
- .Successful or failed attempts to create, modify or delete information on certificate holders.
- .Successful or failed attempts to access the facilities by authorized staff.
- .Backup, archive and restoration.
- .Changes in the system configuration.
- .Software and hardware updates.
- .System maintenance.
- .Personnel changes

5.4.2. Log processing frequency.

The audit records are examined at least once a week for suspicious or unusual activity. Processing of the audit records consists of a revision of the records which includes the verification that they have not been manipulated, a brief inspection of all the registry entries of and a more in-depth investigation of any alert or irregularity in the records. The actions taken on the basis of the audit review must also be documented.

5.4.3. Audit logs retention period.

ACEDICOM will retain all the audit records generated by the system for a minimum period as of the date of their creation of four (4) weeks for daily audits, (1) one year for monthly and fifteen (15) years for annual audits.

It must be emphasized that the annual audit records contain all the records generated at least during the last year, without exception, since the copies of the records are always made complete, never incrementally, and the consolidation procedure assures that at any time a year of records is available in the systems.

5.4.4. Audit log protection.

The registry files, both manual and electronic, are protected from reading, modification, erasure or any other type of unauthorized manipulation using logical and physical access controls.

5.4.4. Audit log backup procedures.

Complete backup audit record copies are generated daily, cryptographically protected to prevent their manipulation.

5.4.6. Audit information collection System (internal vs. external).

The audit compilation system of the ACEDICOM information systems is a combination of automatic and manual processes executed by the operating systems, the ACEDICOM applications, and the personnel who run them.

5.4.7. Notification to the subject cause of the event.

Not stipulated.

5.4.8. Vulnerability analysis.

At least one monthly analysis of vulnerabilities and perimeter security is carried out. It is the responsibility of the analysis team coordinators to notify ACEDICOM, through the Security Manager, of any problem preventing the audits, or the delivery of the resulting documentation. It is ACEDICOM's responsibility to inform the audit teams of suspension of the analyses.

The security analyses involve the start of the tasks needed to correct the vulnerabilities detected and the issue of a counter-report by ACEDICOM.

5.5. INFORMATION AND RECORDS FILE.

ACEDICOM guarantees that all the information relating to certificates is kept for fifteen (15) years as of the beginning of the registration procedure.

5.5.1. Type of information and events recorded.

The information and events record are:

- The audit records specified in point 5.4 of this Certification Practices Statement
- The backup support of the servers that make up the ACEDICOM infrastructure.
- Documentation relative to the service life of the certificates, among which are included:
 - .Certification contract
 - .Copy of the identification documentation provided by the certificate applicant.
 - .Location of the User Registration Point -PRU- where the certificate was issued.
 - .Identity of the PRU operator where the certificate was issued
 - .Date of the last face-to-face identification of the subscriber
- Confidentiality agreements
- Agreements signed by ACEDICOM.
- Authorized access to the Information Systems (Registration Point operator authorization, among others).

5.5.2. Archive retention term.

All the information and documentation relating to the service life of certificates issued by ACEDICOM are kept for a period of fifteen (15) years.

5.5.3. Archive protection.

Access to the file archive is restricted to authorized personnel.

Likewise, the events relating to certificates issued by ACEDICOM are cryptographically protected to prevent manipulations of the contents.

5.5.4. Archive backup procedures.

Two daily copies are made of the files that make up the archives to be retained.

One copy is made locally and stored in a flame-proof strongbox in the ACEDICOM main Data Processing Centre.

The second copy of the data is made encrypted and remotely and stored in the continuity or backup Data Processing Centre located in a building apart from the ACEDICOM main Data Processing Centre.

5.5.5. Record time stamping requirements.

The ACEDICOM systems record the instant in time when they are made. The timing of the systems comes from a reliable time source. All ACEDICOM systems synchronize their timings from this source. The time sources used, based on NTP (Network Time Protocol) are autocalibrated in different ways, using as reference among others that of the Royal Institute and Observatory of the Navy.

5.5.6. Audit information compilation system (internal vs. external).

The information gathering system is internal to the ACEDICOM entity.

5.5.7. Procedures to obtain and verify archived information.

Only authorized personnel have access to the physical archives of supports and computerized archives, to carry out integrity or other checks.

Integrity checks of the electronic archives (backups) take place automatically, at the time of their generation and after copying to the backup support. An incident [report] is created in the event of errors or unexpected behaviour.

5.6. CA KEY CHANGE.

The procedures to provide the new CA public key to the holders and third party acceptors of the certificates of the same in the event of a CA key change are the same used to provide the current public key. Consequently, the new key will be published in the website: <http://acedicom.edicomgroup.com>.

The procedures to provide a new public key to the users of said CA correspond to the renewal procedures described in this document.

5.7. RECOVERY IN CASE OF KEY COMPROMISE OR DISASTER.

Should the facilities of the Certification Authority become unavailable for a period longer than six hours, the ACEDICOM Disaster Recovery Plan will be activated.

The Disaster Recovery Plan guarantees that the services identified as critical due to their availability requirement are available in the continuity DPC in less than 12 hours as of activation of the Plan.

5.7.1. Alteration of hardware, software and/or data resources.

If the hardware, software, and/or data resources are altered or are suspected to have been altered, the ACEDICOM services will cease operations until the reestablishment of a secure framework with the incorporation of new components of demonstrable efficiency. In parallel, an audit will be carried out to identify the cause of the alteration and to ensure the non-reproduction of the same.

In the event of issued certificate being affected, the subscribers will be notified of the fact and recertification implemented.

5.7.2. The public key of an entity is revoked.

In the event of revocation of the certificate of an ACEDICOM entity, the corresponding CRL will be generated and published, the operation of the entity will cease and the generation, certification and start-up of a new entity with the same designation as the one eliminated and with a new pair of keys will take place.

In the event that the affected entity is a CA, the revoked certificate of the entity will remain accessible in the ACEDICOM repository in order to continue to allow the verification of the certificates issued during its period of operation.

The component bodies of ACEDICOM dependent on the renewed entity will be informed of the change and invited to request their recertification by the new member of the organization.

5.7.3. The key of an entity is compromised.

If the key of an entity is compromised, it will be immediately revoked in accordance with that set forth in the previous point and the rest of the entities that make up ACEDICOM, dependent or not on the affected entity, will be notified.

The certificates signed by entities dependent on the key compromised in the period between the compromising of the key and revocation of the corresponding certificate will also be revoked once their subscribers have been informed and recertified.

5.7.4. Security installation following natural disaster or other types of disaster.

In the event of a natural disaster affecting the facilities of the ACEDICOM main Data Processing Centre and, therefore, the services provided, the Disaster Recovery Plan will be activated, guaranteeing that the services identified as critical owing to their availability requirement are available in the continuity DPC in less than 12 hours after activation of the Plan, and the rest of the essential services within reasonable terms and according to their level of need and criticality.

5.8. CESSATION OF A CA.

The causes that may give rise to cessation of the activity of the Certification Authority are:

- The CA private key being compromised
- Policy decision by EDICOM

In the event of cessation of their activity as Certification Service Provider, ACEDICOM will take, at least two months in advance, the following actions:

- Inform all the subscribers of its certificates and cancel the use of the same, revoking them.
- Inform all the third parties with which it has signed a certification agreement.
- Notify the competent Ministry in the area of Information Society and electronic signature of the cessation of its activity and what is to happen to the certificates, as well as any other relevant circumstances related to the cessation of activity.
- Send to the competent Ministry in the area of Information Society and electronic signature all the information relating to the revoked electronic certificates as well as information on events and logs so that they may take charge of their safekeeping during the rest of the compromised period.
- Revoke the authorizations to run the certificate issuing process to every outsourcer acting on behalf of or for the CA.
- - Destruction of the CA private keys.
- ACEDICOM does not contemplate the transfer of the management of the certificates that may still be effective at the moment of cessation of the CA, so will cancel all certificates in the terms stipulated in Law 59/2003.

6. TECHNICAL SECURITY CONTROLS.

ACEDICOM uses reliable systems and products, protected against all alteration and which guarantee the technical and cryptographic security of the certification processes to which they serve as support.

6.1. KEY PAIR GENERATION AND INSTALLATION.

6.1.1. Key pair generation.

The pairs of keys for the internal components of ACEDICOM PKI, specifically root CA and Subordinate CAs, are generated in cryptographic hardware modules that meet the requirements set out in a standardized certification authority electronic signature secure device protection profile, in accordance with ITSEC, Common Criteria or FIPS 140-2 Level 3 or higher security level.

The pairs of keys for end entities are generated on the basis of that stipulated in the Certification Policy applicable.

where the generation of the keys is not done by means under control of the end entity, the corresponding Certification Policy will specify the procedure to be used to deliver the private key to the end entities.

6.1.3. Delivery of public key to certificate issuer.

The public keys generated by means under the control of the end entities are sent digitally to ACEDICOM as part of a certification request in PKCS#10 format, signed with the private key corresponding to the public key that is to be certified.

6.1.4. Delivery of the public key of the CA to the users.

The public keys of all the CA belonging to the ACEDICOM trust hierarchy can be downloaded from the ACEDICOM website: <http://acedicom.edicomgroup.com>
Additional measures are in place to trust the self-signed certificate, such as verification of the digital fingerprint of the certificate.

6.1.5. Key size.

The ACEDICOM Root keys and ACEDICOM Root keys are RSA keys 4096 bits in length.

The size of the keys for each type of certificate issued by ACEDICOM is set forth in the Certification Policy applicable. In any case, the size will never be less than 1,024 bits.

6.1.6. Public key generation parameters.

The ACEDICOM Root and ACEDICOM keys are created with the RSA algorithm. The key generation parameters for each type of certificate issued by ACEDICOM are defined by the Certification Policy applicable. In both cases, the public keys are codified according to RFC 3280 and PKCS#1.

6.1.7. Parameter quality check.

The procedures and means of verification of the quality of the key generation parameters for each type of certificate issued by ACEDICOM are defined by the Certification Policy applicable and specifically in accordance with ETSI special report MR. 001 276, indicating the quality of electronic signature algorithms.

The signature algorithms and parameters used by the ACEDICOM Certification Authorities to sign electronic certificates and lists of revoked certificates are as follows:

Signature algorithm Signature algorithm parameters

Rsa MinModLen=1020

Key generation algorithm

rsagen1

Padding method Cryptographic

emsa-pkcs1-v1_5

Hash function

sha1

6.1.8. Key generation hardware/software.

The pairs of keys for the Certification Entities are generated using cryptographic hardware modules that meet the requirements set out in a standardized certification authority electronic signature secure device protection profile, in accordance with ITSEC, Common Criteria or FIPS 140-2 Level 3 or higher security level.

The hardware or software devices to be used in the generation of keys for each type of certificate issued by ACEDICOM are defined by the Certification Policy applicable.

6.1.9. Key usage purposes.

The usage aims for each type of certificate issued by ACEDICOM are defined by the Certification Policy applicable.

All the certificates issued by ACEDICOM contain the extensions *KEY USAGE* and *EXTENDED KEY USAGE* defined by the X.509 v3 standard for the definition and limitation of said aims.

It must be taken into account that the effectiveness of constraints based on extensions of certificates sometimes depends on the operativity of IT applications that have not been made or controlled by ACEDICOM.

6.2. PRIVATE KEY PROTECTION.

6.2.1. Standards for the cryptographic modules.

The modules used for the creation of keys by ACEDICOM root CA and Subordinate CAs meet the requirements set out in a standardized certification authority electronic signature secure device protection profile, in accordance with ITSEC, Common Criteria or FIPS 140-2 Level 3 or higher security level.

6.2.2. Multi-person private key control.

The private keys, both of the Root CA and *Subordinate CAs* are under multi-person control. This is activated by means of the CA software boot

through a combination of CA operators, HSM administrators and Operating System users.

This is the only activation method for this private key.

Multi-person control: control by more than one person, normally by a subgroup 'k' of a total of 'n' persons. In this way, it is guaranteed that nobody has individual control of the critical actions while facilitating the availability of the necessary people.

6.2.3. Private key custody.

Private signature keys of the subscribers are safeguarded. These keys and the private keys of the Certification Authorities and Registration Authorities that make up ACEDICOM are housed in cryptographic hardware devices with level 3 FIPS 140-2 security certification meeting the requirements laid down in a standardized certification authority electronic signature secure device protection profile.

6.2.4. Private key security copy.

Backup copies of the ACEDICOM private key components are stored encrypted in secure non-flammable archives. The CA private key may only be exported once in multiple fragments in the custody of different persons.

6.2.5. Private key archive.

Backup copies of some of the ACEDICOM private key components will be safeguarded encrypted in secure non-flammable archives.

6.2.6. Entering the private key in the cryptographic module.

The private keys are created in the cryptographic module at the moment of creation of each of the ACEDICOM entities that make use of these modules.

6.2.7. Private key activation method.

The private key both of ACEDICOM Root and ACEDICOM is activated by booting the CA software and the cryptographic hardware that contains the keys.

6.2.8. Private key deactivation method.

An Administrator can deactivate the key of the ACEDICOM Certification Authorities by detaining the CA software.

6.2.9. Private key destruction method.

The private keys are destroyed in a form that prevents their theft, modification, unauthorized divulgation or use.

The destruction of HSM is not considered, due to its high cost. Instead, the start-up tasks of the same are carried out. During the step from "operational" to "start-up" the keys contained in it are deleted securely.

There is an operational procedure for destruction of the CA keys.

In general terms, the destruction always must be preceded by a revocation of the certificate associated with the key, if this were still effective.

6.2.10 Classification of cryptographic modules.

The modules used for the creation of keys by ACEDICOM root CA and Subordinate CAs meet the requirements set out in a standardized certification authority electronic signature secure device protection

profile, in accordance with ITSEC, Common Criteria or FIPS 140-2 Level 3 or higher security level. The hardware and software systems used are in compliance with CWA 14167-1 and CWA 14167-2 standards.

6.3. OTHER KEY PAIR MANAGEMENT ASPECTS.

6.3.1. Public key archive.

The ACEDICOM Public Key Infrastructure, in compliance with that set forth in article 20 f) of LFE59/2003 and in its commitment to permanence will maintain its archives for a minimum term of fifteen years (15).

6.3.2. Public and private key usage periods.

The ACEDICOM Root certificate is valid for (20) years. The ACEDICOM certificate is valid for (10) years.

The validity period of certificates of end entities will be stipulated by the Certification Policy applicable in each case, and in no case will it exceed four (4) years of maximum validity.

Expiry will automatically cause the invalidation of Certificates, originating the permanent cessation of its operativity according to its usage and, consequently, of the certification service provision.

6.4. ACTIVATION DATA.

6.4.1. Activation data generation and activation.

For the restoration of a Certification Authority of the ACEDICOM domain, cryptographic cards must be created, which will be used for operation and recovery activities. The CA operates with several types of role, each one with their corresponding cryptographic cards where the activation data are stored.

6.4.2. Activation data protection.

Only authorized personnel know the PINs and passwords to access the activation data.

6.4.3. Other activation data aspects.

Not stipulated.

6.5. IT SECURITY CONTROLS.

6.5.1 Specific IT security technical requirements.

It is guaranteed that the access to the systems is limited to properly authorized individuals. In particular:

- ACEDICOM guarantees an effective administration of the access level of the users (operators, administrators, as well as of any user with direct access to the system) to maintain system security, including the management of user accounts, audit and modifications or appropriate access refusals.

- ACEDICOM guarantees that access to the application and the Information System is restricted in accordance with that set forth in the access control policy, as well as that the systems provide sufficient security controls to implement the segregation of functions identified in the Entity practices, including the separation of system management functions from security and the operators. Specifically, the use of system utility programs is restricted and closely monitored.
- The Entity personnel are identified and recognized before using critical applications related with the service life of the certificate.
- The Entity personnel are responsible and must be able to justify their activities, for example by means of an events file.
- The possibility of disclosure of sensitive data by means of the reutilization of storage objects (for example deleted files) that are accessible to unauthorized users must be avoided.
- The security and monitoring systems allow swift detection, recording and action against irregular unauthorized attempts to access their resources (for example, by means of an intruder detection system, monitoring and alarm).
- Access to the ACEDICOM public information deposits (for example, certificates or information on revocation status) has access control for data modifications or deletion.

6.5.2 IT security level assessment

The CA applications are reliable, in accordance with technical specification CEN CWA 14167-1, evaluating the degree of compliance by means of a suitable protection profile, in accordance with ISO 15408 or equivalent norm.

6.6. SERVICE LIFE SECURITY CONTROLS.

6.6.1 Systems development controls.

An analysis of security requirements is performed during the design and specification phases for requirements of any component used in the applications of the (technical) Certification Authority and the (technical) Registration Authority, to guarantee that the systems are safe.

Change control procedures are used for the new versions, updates and emergency patches of these components.

6.6.2 Security management controls.

ACEDICOM maintains an inventory of all the IT assets and will make a classification of the same in line with their protection needs, coherent with the risk analysis carried out.

The configuration of the systems is audited periodically, in accordance with that set out in the corresponding section of this document.

ACEDICOM systems are protected against virus and unauthorized and malicious software.

The capacity needs are monitored, and procedures will be planned to guarantee sufficient electronic and storage availability for the information assets.

6.7. NETWORK SECURITY CONTROLS.

It is guaranteed that access to the different ACEDICOM networks is limited to duly authorized individuals. In particular:

- Controls are implemented (for example firewalls) to protect the internal network from external domains accessible by third parties. The firewalls are configured to prevent accesses and protocols that are not necessary for ACEDICOM operations.
- Sensitive data are protected when they are interchanged through non-secure networks (including subscriber registration data).
- It is guaranteed that the local network components (such as routers) are located in safe surroundings, as well as the periodic audit of their configurations.

6.8. CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS.

ACEDICOM uses cryptographic hardware and software modules available commercially developed by third parties.

ACEDICOM uses only cryptographic modules with FIPS 140-2 or ITSEC E3 certification or higher.

7. REVOKED CERTIFICATE AND CERTIFICATE LIST PROFILES.

7.1. CERTIFICATE PROFILE.

The certificates issued by the ACEDICOM system will comply with the following norms:

- RFC 3280: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile, April 2002
- ITU-T Recommendation X.509 (2005): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework
- ETSI TS 101 862 V1.3.1 (2004-03): Qualified Certificate Profile, 2004
- RFC 3739: Internet X.509 Public Key Infrastructure - Qualified Certificate Profile, March 2004 (TS 101 862 prevailing in the event of conflict).

7.1.1. Version number.

ACEDICOM supports and uses X.509 certificates version 3 (X.509 v3). X.509 is a standard developed by the International Telecommunication Union (international entity of the United Nations for coordination of telecommunications network services between governments and companies) for Public Key Infrastructures and Digital Certificates.

7.1.2. Certificate extensions.

The extensions used in certificates are:

- *KeyUsage*. Qualified as critical.
- *BasicConstraint*. Qualified as critical.
- *CertificatePolicies*. Qualified as non-critical.
- *Subject Directory Attributes*. Qualified as non-critical.
- *CRLDistributionPoints*. Qualified as non-critical.
- *Authority Information Access*. Qualified as non-critical.
- *Qcstatements*. Qualified as non-critical.

ACEDICOM has defined an allocation policy for OIDs within their private numeration range whereby the OID of all the ACEDICOM proprietary Certificate Extensions begins with the prefix 1.3.6.1.4.1.30051.3.1

ACEDICOM has the following proprietary extensions defined:

| OID | Concept Description |
|-------------------------|-------------------------------|
| 1.3.6.1.4.1.30051.3.1.1 | CIF of the entity represented |

The profile of each certificate is detailed in each of the corresponding policies.

7.1.3. Object identifiers (OID) of algorithms

Object Identifier (OID) of the Cryptographic algorithms:

- SHA1withRSAEncryption (1.2.840.113549.1.1.5)

7.1.4. Name formats.

Certificates issued by ACEDICOM contain the *distinguished name* X.500 of the certificate issuer and subscriber in the *issuer name* and *subject name* fields, respectively.

The *cn* field of the *subject name* must be filled in with capital letters, without accents and replacing the letter "Ñ" by the letter "N" and the letter "Ç" by the letter "C". This feature only occurs in the *CommonName* attribute.

3.1.2. Name constraints.

Names contained in the certificates are restricted to distinguished names X.500, unique and non-ambiguous.

7.1.6. Certification Policy Object Identifier (OID).

The object identifier defined by ACEDICOM to identify the current certification practice is as follows: 1.3.6.1.4.1.30051.2.1.1.1

7.1.7. "Policy Constraints" extension use.

Not stipulated.

7.1.8. Policy qualifier syntax and semantics.

Not stipulated.

7.1.9. Critical "Certificate Policy" extension semantic treatment.

The "Certificate Policy" extension identifies the policy defining the practices that ACEDICOM explicitly associates with the certificate. Additionally, the extension may contain a policy qualifier.

7.2. CRL profile.

7.2.1. Version number.

The format of the CRLs used in this policy is specified in version 2 (X509 v2).

7.2.2. CRL and extensions.

This Certification Practice Statement supports and uses CRLs in compliance with standard X.509:

7.3 REVOKED CERTIFICATE LIST.

7.3.1 Time limit of certificates in CRLs

The serial numbers of revoked certificates will appear in the CRL until they reach their expiry date.

7.4.- OCSP PROFILE.

7.4.1.- OCSP responder certificate profile.

OCSP responder certificates Will be issued by the corresponding subordinate CA of the ACEDICOM certification domain and will comply with the following norms:

- RFC 3280: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile, April 2002
- ITU-T Recommendation X.509 (2005): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework
- IETF RFC 2560 Online Certificate Status Protocol - **OCSP**

The validity period of the same will be no more than 2 years. As anticipated in RFC 2560, the issuing CA will include the "*idpkix-ocsp-nocheck*" extension in the OCSP responder certificate to indicate that OCSP clients must trust the validation services provider for the lifetime of the associated. However, the CA does not count out the possibility in the future of including information on additional mechanisms to confirm the validity of these certificates in the AIA extension of OCSP responder certificates.

7.4.2.- Version number.

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

7.4.3.- Name formats.

The OCSP Responder certificates issued by a CA in the ACEDICOM domain will contain the distinguished name X.500 of the certificate issuer and subscriber in the issuer name and subject name fields, respectively.

Names contained in the certificates are restricted to 'Distinguished Names' X.500, which are unique and non-ambiguous.

The DN for the certificates will be composed of the following elements:

CN, OU, O, C

The "C" attribute (countryName) will be encrypted in compliance with "ISO 3166-1-alpha-2 code elements", in PrintableString, while the rest of the attributes will be encoded in UTF8:

CN=OCSPSignerCertificate

CN=ACEDICOM XX

OU=PKI

O=EDICOM

L=Ronda de Auguste y Louis Lumiere 12 Paterna

ST=Valencia,

C=ES

serialNumber=B96490867

postalCode=46980

emailAddress=acedicom@edicomgroup.com

where XX is the code of each of the subordinate CAs (01,02, etc.)

7.4.4.- Certification Policy Object Identifier (OID).

Not stipulated.

7.4.5.- Certificate extensions and fields.

The profile of the OCSP responder certificate that issues the ACEDICOM PKI is:

| FIELD | CONTENTS | CRITICAL for extensions |
|------------------------------|--|-------------------------|
| X509v1 fields | | |
| 1. Version | V3 | |
| 2. Serial Number | Unique number assigned by CA | |
| 3. Signature Algorithm | SHA1withRSAEncryption | |
| 4. Issuer Distinguished Name | CN=ACEDICOM XX OU=PKI O=EDICOM L=Ronda de Auguste y Louis Lumiere 12 Paterna ST=Valencia, C=ES serialNumber=B96490867 postalCode=46980 emailAddress=acedicom@edicomgroup.com | |
| 5. Validity | 2 years | |
| 6. Subject | CN=OCSPSignerCertificate CN=ACEDICOM XX OU=PKI O=EDICOM L=Ronda de Auguste y Louis Lumiere 12 Paterna ST=Valencia, C=ES serialNumber=B96490867 postalCode=46980 emailAddress=acedicom@edicomgroup.com | |
| 7. Subject Public Key Info | Algorithm: RSA Encryption Key length: 2048 bits | |
| X509v3 extensions | | |
| 1. Subject Key Identifier | Derived from using the SHA-1 hash function on the subject's public key. | NO |
| 2. Authority Key Identifier | Derived from using the SHA-1 hash function on the issuing CA's public key. | NO |
| 3. KeyUsage | DigitalSignature | YES |
| 4. extKeyUsage | OCSPSigning | |
| 14. OCSPNoCheck | NULLvalue as anticipated in the norm. | NO |

7.4.6.- OCSP request format.

The Nonce extension (id-pkix-ocsp-nonce) is supported as contemplated in the norm to prevent "replay attacks".

7.4.7.- Response format.

The OCSP responder of the validation service is able, at least, to generate id-pkix-ocsp-basic type responses.

Regarding the state of certificates, it must respond as:

- "Revoked", for those certificates issued by the CA of the ACEDICOM certification domain and which are recorded in the CRLs.
- "Good", for those certificates issued by the CA of the ACEDICOM certification domain and which are not recorded in the CRLs. The "good" status is simple a "positive" response to the OCSP request, indicating that the certificate is not revoked, but it does not necessarily mean that the certificate was issued at any time or that it is within the validity period.
- "Unknown" if the request corresponds to an unknown issuer CA.

As for the semantics of the fields thisUpdate, nextupdate and producedAt.

- "producedAt" must contain the moment of time in which the OCSP responder generates and signs the response.
- "thisUpdate" must to indicate the moment at which it is known that the status indicated in the response is correct. In the case of revoked

certificates, they must contain the "this Update" field of the CRL that was used. In all other cases, the local date will be used.

- "nextUpdate" must indicate the moment in time in which new revocation information will be available. In the case of revoked certificates, it must contain the "nextUpdate" field of the CRL that was used, except when the "nextUpdate" date is prior to the local date. In the rest of cases, the nextUpdate field will not be set, which is equivalent according to rfc2560 to indicating that it is possible to obtain new revocation information at any time, so it is the responsibility of the client to consult it again when they consider it convenient.

8. CONFORMITY AUDIT.

8.1. FREQUENCY OF CONFORMITY CHECKS FOR EACH ENTITY.

An audit will be carried out on ACEDICOM at least once a year, to guarantee the suitability of its function and operativity with the stipulations included in this CPS.

Other technical and security audits will be carried out, among which an audit of compliance with the legislation on protection of data of a personal nature is included.

8.2. AUDITOR IDENTIFICATION/QUALIFICATION.

The auditor will be selected at the time of each audit.

If the ACEDICOM has an internal audit department, they may carry out the conformity audit.

If they do not have such a department, the ACEDICOM may use an independent external auditor, who must demonstrate experience in IT security, security of information systems and/or audits of conformity of Certification Authorities and their related elements.

8.3. RELATION BETWEEN AUDITOR AND ENTITY AUDITED.

Apart from the audit function, the auditor and the audited party (ACEDICOM) must not have any relation, present or planned, financial, legal, or of any other kind that might derive in a conflict of interests. In accordance with that set forth in the current regulation in our ordinance on personal data protection, and taking into account that for compliance by the auditor with the services regulated in the contract, it will be necessary to access the personal data of the files held by ACEDICOM, the auditor will have the consideration of Treatment Manager, by virtue of that anticipated in article 12 of Organic Law 15/1999, of 13th December.

8.4. TOPICS COVERED BY CONFORMITY AUDIT.

The audit will determine the compliance of the ACEDICOM services with this CPS and the applicable CPs. Likewise, it will determine the risks of non-fulfilment of suitability of the operativity defined by these documents.

The aspects covered by an audit will include, but are not limited to:

- Security policy.
- Physical Security.
- Technological evaluation.
- Administration of CA services.
- Current CPS and CPs.

8.5. ACTIONS TO BE TAKEN AS A RESULT OF A DEFICIENCY.

Once the report of the conformity audit carried out has been received, the ACEDICOM discusses any deficiencies found with the entity that has executed the audit, and develops and executes a corrective plan to resolve said deficiencies.

If the ACEDICOM audited is unable to develop and/or to execute this plan or if the deficiencies found suppose an immediate threat for the security or integrity of the system, one of the following actions must be taken:

- Revoke the ACEDICOM key, as described in the corresponding sections of this policy.
- Finalize the ACEDICOM service provision, as described in the corresponding section of this policy.

8.6. COMMUNICATION OF RESULTS.

The auditor will communicate the results of the audit to the EDICOM Technical Director, the Head of ACEDICOM and the ACEDICOM Security Manager, as well as the people in charge of the different areas in which non-compliance is detected.

9. COMMERCIAL AND LEGAL REQUIREMENTS.

9.1. TARIFFS.

9.1.1. Certificate issue or renewal fees.

The fees for issue and revocation of each certificate are specified in the ACEDICOM public repository: <http://acedicom.edicomgroup.com>

9.1.2. Certificate access fees.

The access to certificates issued, given its public nature, is free of charge and so no fee is applied to the same.

9.1.3. Fees for access to status or revocation information.

Access to the status or revocation information on certificates based on CRLs is free of charge, so no fee is applied. Access to the OCSP responder service may be charged according to ACEDICOM criteria. In this case, the service rates will be published in the ACEDICOM public repository: <http://acedicom.edicomgroup.com>

9.1.4. Fees for other services such as information on policies.

No charge will be applied for the information service on this CPS or the certification policies administered by ACEDICOM or for any other additional service other than the "Electronic Signature Services" known at the time of drafting this document.

This stipulation may be modified by the Certification Policy applicable in each case.

9.1.5. Refund policy.

No additional stipulation.

9.2. FINANCIAL STANDING.

9.2.1. Indemnification to third parties trusting certificates issued by ACEDICOM.

ACEDICOM, in its activity as Certification Service Provider, has sufficient economic resources to assume the risk of responsibility for damages to the users of its services and to third parties. Its responsibility in the exercise of activity as CSP, as defined in current Spanish legislation in article 20.2 of Law 59/2003, of 19th December (on electronic signature), is guaranteed by means of a Professional Civil Responsibility Insurance Policy with a cover of Three Million Euros (3.000.000 €).

9.2.2. Fiduciary relations.

ACEDICOM does not operate as representing fiduciary agent of subscribers in any way, or of third parties who trust the certificates issued by ACEDICOM.

9.2.3. Administrative processes.

ACEDICOM guarantees the realization of audits of the processes and procedures established at regular intervals. These audits will be carried out both internally and externally.

9.3. CONFIDENTIALITY POLICY.

9.3.1. Confidential information.

The following items are declared specifically as confidential information, which may not be disclosed to third parties, except in those suppositions legally anticipated:

- The private keys of the entities that make up ACEDICOM.
- The private keys of subscribers which ACEDICOM maintains in safekeeping.
- All information relative to the operations carried out by ACEDICOM.
- All information relative to the parameters of security, control and audit procedures.
- All information of a personal nature provided to ACEDICOM during the registration process of certificate subscribers, with the reservation specified by the Certification Policy applicable and the certification contract.
- The business information provided by its suppliers and other persons with which the ACEDICOM must keep secret established legally or conventionally.
- Business continuity and emergency plans.
- Transaction records, including the complete registries and audit registries of the transactions.
- All information classified "CONFIDENTIAL" or "STRICTLY CONFIDENTIAL"

9.3.2. Non-confidential information.

ACEDICOM considers public access information:

- The contents of the Certification Practice Statement approved by ACEDICOM.
- The contents of the different Certification Policies approved by ACEDICOM.
- The certificates issued as well as the information contained in them.
- The Certificate Revocation List (CRL)
- All information qualified "PUBLIC".

The ACEDICOM CPS and CPs will not include information described as confidential in point 9.3.1 of this document.

Access is allowed to the information not considered confidential, notwithstanding the pertinent security controls established by ACEDICOM in order to protect the authenticity and integrity of the documents that contain the public access information and to prevent unauthorized persons adding, modifying or suppressing contents.

9.3.3. Disclosure of certificate revocation /suspension information.

Information relating to the revocation or suspension of certificates is provided via CRL.

9.4. PERSONAL DATA PROTECTION.

ACEDICOM has a Privacy Policy, published on the ACEDICOM website, in compliance with the dispositions set forth in the legislation on protection of data of a personal nature, and in which information is provided on the protection policy for personal data in ACEDICOM.

9.4.1. Personal Data Protection Plan.

ACEDICOM implements a privacy policy, in accordance with Organic Law 15/99, of 13th December, on Personal Data Protection.

The Certification Entity does not disclose or transfer personal data, except in the anticipated cases, as in section 5.8, in the event of conclusion of the Certification Entity.

ACEDICOM has the procedures in this document, which it applies in the provision of its services, whereby, in compliance with the requirements stipulated by the certificate policies managed by the same, and in accordance with article 19 of Law 59/2003, of 19th December, on electronic signature, the requirements and obligations in relation with the obtaining and management of personal data that it obtains are detailed, fulfilling to this end the dispositions of Organic Law 15/1999 of 13th December, on Protection of Personal Data, and Royal Decree 1720/2007, of 21st December, whereby the Regulation on the development of Organic Law 15/1999, of 13th December, on protection of data of a personal nature, is approved.

Specifically, the following sections of the Security Measures Regulation are fulfilled with the controls in the following sections of this document:

- a. Scope of application of the security document with detailed specification of the resources protected - section 9.4.
- b. Measures, norms, procedures, rules and standards that guarantee the security level demanded by the Regulation - section 9.4, and, in general, all the technical controls in sections 5 and 6.
- c. Staff functions and obligations - section 5.3.
- d. Structure of the files with personal data and description of the information systems that process the same - 9.4.2 section and section 1.3.1 respectively.
- e. Procedure for notification, management and response to incidents - section 9.4.4.
- f. Backup and data retrieval procedures - section 5.5.

9.4.2. Information deemed private.

In accordance with that set forth in article 3 of Organic Law 15/1999, 13th December, on Protection of Data of Personal Nature, any information relating to identified or identifiable physical persons is considered personal data.

Both the personal information that does not have to be included in certificates and the certificate status verification mechanism, are deemed personal information of private nature.

In any case, the following data are considered private information:

- Certificate applications, approved or denied, as well as all other personal information obtained for the issue and maintenance of certificates.
- Private keys generated and/or stored by ACEDICOM.
- All other information identified as "private Information".

Likewise, the data gathered by the Certification Service Provider have the legal consideration of basic level data.

In accordance with Organic Law 15/99, the confidential information is protected against loss, destruction, damage, falsification and illicit or unauthorized processing, pursuant to the stipulations set forth in Royal Decree 994/99, of 11th June, whereby the Regulation of Safety Measures for the automated files containing data of a personal nature is approved.

In no case does ACEDICOM include, in the electronic certificates that it issues, the data referred to in article 7 of Organic Law 15/1999, of 13th December, on Protection of Data of a Personal Nature.

9.4.3. Information not deemed private.

This information makes reference to the personal information that is included in certificates and the aforementioned certificate status checking mechanism, in accordance with section 3.1 of this document.

This information, provided in the certificate request in the terms anticipated in article 17.2 of Law 59/2003, of 19th December, electronic signature, is included in the certificates and the certificate status verification mechanism.

The information is not of private nature, by legal imperative ("public data"), but is only published in the deposit with the subscriber's consent.

In any case, the following information is considered non-confidential:

- a. Certificates issued or in issuing process.
- b. The subjection of the subscriber to a certificate issued by ACEDICOM.
- c. The name and the surnames of the certificate subscriber, as well as any other circumstances or personal data of the holder, in the event that they are significant in terms of the purpose of the certificate, pursuant to with this document.
- d. The electronic address of the certificate subscriber.
- e. The uses and economic limits described in the certificate.
- f. The validity period of the certificate, as well as the date of issue and expiry date of the certificate.
- g. The certificate serial number.
- h. The different states or situations of the certificate and the initial date of each of them, specifically: pending generation and/or delivery, valid, revoked, suspended or expired and the reason that caused the change of status.
- i. Certificate revocation lists (CRLs), as well as the rest of the revocation status information.
- j. The information contained in the ACEDICOM Deposit.

9.4.4. Responsibilities.

ACEDICOM guarantees compliance of their legal obligations as Certification Service Provider, in accordance with Law 59/2003, of 19th December, and by virtue of this, and pursuant to article 22 of this Law, will be held responsible for the damages that may be caused in the exercise of said activity by the breach of the prescriptions contained in article 17 of Law 59/2003, relating to the protection of personal data.

ACEDICOM includes in this document their notification, management and response procedure for incidents related with personal data.

This procedure contains a registry in which the type of incident, the time it has taken place, the person responsible for notification, the person notified and the effects derived from the same are recorded.

ACEDICOM implants identification and authentication measures, as well as the necessary control of staff access to the personal data, as described in sections 4 and 5 of this document.

The management procedures for the personal data supports and backups defined in sections 5.5 of this document meet the requirements of articles 13 and 14 of Royal Decree 994/99.

9.4.5. Consent given for personal data use.

In order to supply the service, ACEDICOM must obtain the consent of the holders of the data necessary for provision of the certification services. Consent will be taken as granted upon signature of the certification contract by the user.

9.4.6. Communication of information to administrative and/or judicial authorities.

ACEDICOM may only communicate information described as confidential or containing data of a personal nature in those cases in which it is so required of the same by the competent public authority and in the legally anticipated suppositions.

Specifically, ACEDICOM is obliged to reveal the identity of the signers when so required by the judicial organs in the exercise of the functions attributed to the same, and in the rest of the circumstances anticipated in article 11.2 of the LOPD where it is required.

9.4.7. Other information disclosure situations.

ACEDICOM includes, in the privacy policy anticipated at the beginning of section 9.4, prescriptions to allow the divulgation of the information of the key holder directly to the same or to third parties.

9.5. INTELLECTUAL PROPERTY RIGHTS.

All intellectual property rights including those referring to certificates and CRLs issued by ACEDICOM, OIDs, this CPS, the Certification Policies applicable to the same, and any other document, electronic or of any other type, the property of ACEDICOM, belong to ACEDICOM.

The private and public keys are the property of the user, independently of the physical means used for their storage.

The subscriber retains any right that they may hold over the product trademark or brand name contained in the certificate.

9.6. OBLIGATIONS AND CIVIL RESPONSIBILITY.

9.6.1. Obligations of the Certification Entity.

9.6.1.1 Obligations and other commitments

ACEDICOM is committed to fulfil the following:

- a. ACEDICOM guarantees, under full responsibility, that it meets all the requirements established in this document.
- b. ACEDICOM is the only entity responsible for the compliance of the procedures described in this document, including when a part or the totality of the operations are subcontracted externally.
- c. ACEDICOM provides certification services in accordance with this document, in which at least the contents anticipated in article 19 of Law 59/2003 are detailed.
- d. Prior to the issue and delivery of the certificate to the subscriber, the ACEDICOM informs the same of the aspects anticipated in article 18.b) of Law 59/2003, and the following aspects:
 - a) Indication of the policy applicable, with indication of whether the certificates are issued to the public and of the need, where indicated, for the use of secure signature creation device.
 - b) The way in which the patrimonial responsibility of ACEDICOM is guaranteed.
 - c) Whether ACEDICOM is declared in accordance with the certification policy and, where indicated, in accordance with which system. Specifically, the certification of the Certification Service Provider and the certification of the electronic signature products used.
- e. This requirement is met by making the ACEDICOM Certification Practices Statement document available, as well the Certification Policy document applicable to the type of certificate issued.
- f. ACEDICOM obliges the subscribers and the verifiers by means of appropriate legal instruments in each situation.
- g. These legal instruments may be transmitted electronically, are in written and comprehensible language, and have the following minimum contents:
 - a) Prescriptions to execute that stipulated in this certification policy.
 - b) Indication of the policy applicable, with indication of whether the certificates are issued to the public and of the need, where indicated, for the use of secure signature creation device.
 - c) Affirmation that the information contained in the certificate is correct, except in the event of notification to the contrary by the subscriber.
 - d) Consent for publication of the certificate in the deposit and access by third parties to the same.
 - e) Consent for storage of the data used for the registration of the subscriber, the provision of the secure signature creation device and for the cession of this information to third parties, in the event of conclusion of operations of ACEDICOM without valid certificate revocation.
 - f) Limits on use of the certificate, including those set forth in section 4.5 of this document.
 - g) Information on how to validate a certificate, including the requirement to verify the state of the certificate, and the conditions in which the certificate may reasonably be trusted, which are applicable when the subscriber acts as checker.
 - h) Limitations of responsibility applicable, including the uses whereby ACEDICOM accepts or denies responsibility.
 - i) Procedures applicable for resolution of disputes.

- j) Law applicable and competent jurisdiction.
- k) ACEDICOM must identify the certificate subscriber, in accordance with articles 12 and 13 of Law 59/2003 and this document and, specifically:
 - a) ACEDICOM verifies for itself, or by means of a Registration Entity, the identity and any other personal circumstances of the applicants for certificates, in accordance with that set forth in article 13 of Law 59/2003.
 - b) ACEDICOM complies with the rest of the obligations contained in article 12 of Law 59/2003.

ACEDICOM directly assumes other obligations incorporated to the certificate or incorporated by reference.

Note: Incorporation by reference is obtained by including in the certificate an object identifier or another form of connection to a document, which is considered wholly included in said document.

In addition to that stipulated in the corresponding section, the legal instrument binding ACEDICOM and the subscriber is in written and comprehensible language, and has the following minimum contents:

- a. Indication that the certificates are issued to the public and of the need, where indicated, for the use of a secure signature creation device, as is indicated in section 6.2.8 of this document.
- b. Certification of ACEDICOM services.
- c. The way in which the patrimonial responsibility of ACEDICOM is guaranteed.

9.6.1.2 Guarantees offered to subscribers and authenticators

ACEDICOM, as minimum, guarantees the subscriber:

- a. The fulfilment of its legal obligations as certification service provider, pursuant to Law 59/2003, of 19th December.
- b. That there are no factual errors in the information contained in the certificates, known or committed by ACEDICOM and, where indicated, by the Registration Entity.
- c. That there are no factual errors in the information contained in the certificates, due to lack of diligence in the management of the certificate application or the creation of the same.
- d. That the certificates fulfil all the material requirements stipulated in the CPS.
- e. The responsibility of ACEDICOM, with the limits set out.
- f. That the services of revocation and the use of the Deposit fulfil all the material requirements stipulated in the CPS.

ACEDICOM, as minimum, guarantees the subscriber:

- a. That, in the event of generating the private keys of the subscriber or, where indicated, the key holder, confidentiality is maintained during the process.
- b. The fulfilment of its legal obligations as certification service provider, pursuant to Law 59/2003, of 19th December.
- c. That the information contained or incorporated by reference in the certificate is correct.
- d. In the case of certificates published in the Deposit, that the certificate has been issued to the subscriber identified in the same

and that the certificate has been accepted, in accordance with the corresponding section of the present document.

- e. That in the approval of the certificate application and in the issue of the certificate all the material requirements established in this document have been fulfilled.
- f. Speed and security in provision of the services, especially of the services of revocation and Deposit.

Additionally, the Certification Entity guarantees the subscriber and the authenticator:

- a. That the certificate contains the information that a recognized certificate must contain, in accordance with article 11.2 of Law 59/2003, of 19th December.

9.6.2. Registration Authority Obligations.

- The persons who operate in the RAs integrated in the ACEDICOM hierarchy - User Registration Point operators - are obliged to:
- Carry out their operations in accordance with this CPS.
- Carry out their operations in accordance with the Certification Policy applicable for the type of certificate applied for on each occasion.
- Exhaustively check the identity of the persons to whom the digital certificate transacted by them is granted to the same, to which end they will require the physical presence of the applicant and a valid national identity document, original and in force. Foreign users must show the Residence Card / NIE (or analogous and official identity document).
- Not to store or copy the signature creation data of the person to whom the services have been provided.
- To notify the person requesting the services, before the issue of a certificate, of the obligations they assume, the way to keep the signature creation data, the procedure to be followed to communicate the loss or illegal use of the signature data or creation and verification devices, the price, the precise conditions for the use of the certificate, its limitations of use and the method whereby their possible patrimonial responsibility is guaranteed, and the website where they can consult any information of ACEDICOM, the current and previous CPS and CP, the applicable legislation and any conflicts that might arise from the exercise of the activity.
- Validate and send securely to the CA to which the RA is subordinated a certification application properly filled in with the information provided by the subscriber, and to receive the data associated with the certificates issued pursuant to said request.
- Store securely, and until the moment of its remission to the Certification Authority, both the documentation provided by the subscriber and that generated by the RA, during the registration or revocation process.
- Formalize the Certification Contract with the subscriber in accordance with that established by the Certification Policy applicable.
- Request the revocation of a certificate when they have knowledge or suspicion that a private key has been compromised.

- Authenticate the requests from end users for the renewal or revocation of their certificates, to generate renovation or revocation requests signed digitally and send them to their superior CA.
- In the case of approval of a certification request, notify the subscriber of the issue of their certificates and the way to obtain them.
- In the event of the rejection of a certification request, notify the applicant of said refusal and the reason for the same.
- Maintain the digital certificate transaction tools under strict control and notify the EDICOM Certification Authority of any malfunction or any other eventuality other than the anticipated normal behaviour.
- Send a signed copy of the certification contract and revocation requests to the EDICOM Certification Authority.
- Receive and transact the revocation requests received made in person immediately, after having carried out a reliable identification based on the DNI of the applicant, or the NIE in the case of foreigners.
- Collaborate in whichever aspects of the operation, audit or control of the User Registration Point are required of them by the Certification Authority.
- The most general and ample obligation of confidentiality, during and after provision of the service as Registration Authority, regarding the information received by ACEDICOM and the information and documentation specified in the service. In the same sense, not to transmit this information to third parties for any purpose without express written and previous authorization from ACEDICOM, in which case the identical obligation of confidentiality will be transferred to said third parties.

9.6.3. Subscriber obligations.

9.6.3.1 Obligations and other commitments

ACEDICOM obliges the subscriber to:

- a. Provide ACEDICOM with complete and appropriate information, especially regarding the registration procedure.
- b. Express their prior consent to the issue of a certificate.
- c. Fulfil the obligations set forth for the subscriber in this document and article 23.1 of Law 59/2003, of 19th December, on electronic signature.
- d. Use the certificate in accordance with that stipulated in the corresponding section.
- e. Notify the ACEDICOM CA, without unjustifiable delay, of the loss, alteration, unauthorized use, theft or compromise of their secure signature creation device, if applicable.
- f. Notify ACEDICOM and any person who the subscriber believes may trust the certificate, without unjustifiable delays, of:
 - a) The loss, theft or potential compromise of their private key.
 - b) The loss of control of their private key, due to the compromising of the activation data (for example, the PIN code of the secure signature creation device) or any other causes.

- c) Any inaccuracies or changes in the content of the certificate that are known, or could be known, to the subscriber.
- g. Stop using the private key once the period indicated in the corresponding section has elapsed.
- h. Refrain from monitoring, manipulating or performing acts of reverse engineering on the technical implantation of the ACEDICOM Hierarchy, without prior permission in writing.
- i. Abstain from intentionally compromising the security of the ACEDICOM Hierarchy.
- j. Use the pair of keys exclusively for electronic signatures and in accordance with any other limitations that are notified to them.
- k. Acknowledge that these electronic signatures are electronic signatures equivalent to handwritten signatures pursuant to article 3.4 of Law 59/2003, of 19th December.
- l. Be especially diligent in the safekeeping of their private key and secure signature creation device (if applicable), in order to prevent unauthorized use.
- m. In the cases in which the subscribers generate their own keys, they undertake to:
 - 1. Generate their subscriber keys using an algorithm acknowledged as acceptable for the recognized electronic signature.
 - 2. Create the keys in the secure signature creation device.
 - 3. Use key lengths and algorithms acknowledged as acceptable for the recognized electronic signature.
- n. Notify ACEDICOM, without unjustifiable delays, of the loss, alteration, unauthorized use, theft or compromise of their secure signature creation device, if applicable.

9.6.3.2 Guarantees provided by the subscriber

ACEDICOM obliges the subscriber, by means of the corresponding legal instrument, to guarantee:

- a. That all the affirmations made in the application are correct.
- b. That all the information provided by the subscriber that is contained in the certificate is correct.
- c. That the certificate is used exclusively for legal and authorized purposes, in accordance with the ACEDICOM Data Centre.
- d. That each digital signature created with the private key corresponding to the public key listed in the certificate is the digital signature of the subscriber and that the certificate has been accepted and is operative (has not expired or been revoked) at the moment of creation of the signature.
- e. That the subscriber is an end entity and not a Certification Authority, and does not use the private key corresponding to the public key listed in the certificate to sign any certificate (or any other certified public key format), or CRL.
- f. That no unauthorized person has ever had access to the subscriber's private key.

9.6.3.3 Private key protection

ACEDICOM obliges the subscriber, by means of the corresponding legal instrument, to guarantee that the subscriber is the only person

responsible for any damages incurred by their breach of the duty to protect the private key.

9.6.4. Obligations of third parties trusting certificates issued by ACEDICOM.

The following obligations correspond to the parties that trust certificates issued by ACEDICOM:

- To limit the reliability of the certificates to the permitted uses of the same, as expressed in the extensions of the certificate and the pertinent Certification Policy.
- To check the validity of certificates when carrying out or verifying any operation based on the same.
- To assume their responsibility in the correct verification of digital signatures.
- To assume their responsibility in the verification of the validity, revocation or suspension of the certificates in which they trust.
- To be fully aware of the guarantees and responsibilities applicable in the acceptance and use of the trusted certificates, and to agree to abide by the same.

9.6.5. Repository obligations.

- To maintain the set of certificates issued by ACEDICOM accessible for the end entities.
- To maintain the information of the certificates that have been revoked accessible for the end entities, in CRL format.

9.7. GUARANTEE WAIVERS.

ACEDICOM may reject all service guarantees that are not bound to obligations stipulated by Law 59/2003, of 19th December, on Electronic Signature, especially those guarantees of adaptation for a particular purpose or guarantee of mercantile use of the certificate.

9.8. RESPONSIBILITY LIMITATIONS.

9.8.1. Guarantees and limitations of guarantees.

ACEDICOM limits its responsibility, restricting the service to the issue and management of certificates and, where indicated, of pairs of subscriber keys and cryptographic deposits (of signature and verification of signature, as well as encryption or decryption) provided by the Certification Entity.

ACEDICOM may limit its responsibility by means of the inclusion of usage constraints on the certificate, and value limits for the transactions for which the certificate can be used.

9.8.2. Definition of responsibilities.

ACEDICOM Registration Entities do not assume any responsibility in the event of loss or damage:

- Of the services rendered, in the event of war, natural disasters or any other case of force majeure.
- Caused by the use of certificates that exceeds the limits set by the same, the pertinent Certification Policy and this CPS.
- Arising from the improper or fraudulent use of certificates or CRLs issued by ACEDICOM.
- Caused to the signer or third parties in good faith if the addressee of documents signed electronically does not check or take into account the restrictions that appear in the certificate regarding its possible uses, or when they fail to take into account the suspension or loss of use of the certificate published in the CRL, or when they do not verify the electronic signature.

9.8.3. Loss limitations.

With the exception of that stipulated by the requirements of this CPS, ACEDICOM does not assume any other commitment and offers no other guarantee, nor assumes any other responsibility to subscribers or trusting parties.

9.9. TERM AND CONCLUSION.

9.9.1. Term.

ACEDICOM stipulates, in its legal instruments with the subscribers and authenticators, a clause that determines the validity period of the legal relation by virtue of which they provide certificates to the subscribers.

9.9.2. Conclusion.

ACEDICOM stipulates, in its legal instruments with the subscribers and authenticators, a clause that determines the validity period of the legal relation by virtue of which they provide certificates to the subscribers. Once the CA activity is finalized, the steps indicated in section 5.8 will be taken.

9.9.3. Survival.

ACEDICOM sets forth, in its legal instruments with the subscribers and authenticators, survival clauses, by virtue of which certain rules remain effective after the conclusion of the legal relation regulating the service between the parties.

To this end, ACEDICOM ensures that, at least the requirements contained in the Obligations, Civil Responsibility, Conformity Audit and Confidentiality sections, remain effective after the conclusion of the certification policy and the legal instruments binding ACEDICOM with subscribers and authenticators.

9.10. NOTIFICATIONS.

All notifications, demands, requests or any other communication required under the practices described in this CPS will be made digitally by means of document or electronic message signed in accordance with the same or by means of certified mail in writing addressed to any of the addresses contained in point 1.5 *Contact details*. The electronic communications

will become effective once received by the addressee to whom they are remitted.

Once the CA activity is finalized, the steps indicated in section 5.8 will be taken.

9.11. MODIFICATIONS.

ACEDICOM may modify this document unilaterally, adhering to the following procedure:

- The modification must be justified from the technical and legal point of view.
- The modification proposed by ACEDICOM may not violate the stipulations contained in the certification policies set out by ACEDICOM.
- A control of modifications is established, to guarantee, in any case, that the resulting specifications meet the requirements that are to be fulfilled and that gave rise to the change.
- The implications that the change of specifications has on the user are set forth, and the need to notify them of these modifications is anticipated.

9.11.1. Change specification procedures.

The entity empowered to make and approve changes to the ACEDICOM CPS and CPs is the EDICOM Technical management, whose contact details are in section 1.5.1. of this CPS.

In those situations in which the EDICOM Technical Management considers that the modification of the CPS does not materially reduce the confidence that a Certification Policy or its implementation provides, or alter the acceptability of the certificates that supports the policy for the purposes for which they have been used, the upgrade of the lower number document version and the last Object Identifier number (OID) that represents it will go ahead, maintaining the document version number, as well as the rest of its associated OID. It is not considered necessary to communicate this type of modifications to the subscribers of certificates corresponding to the CP or CPS modified.

In the event that the Technical Direction of EDICOM judges that the changes to the current specification affect the acceptability of certificates for specific intentions, they will proceed with the increase of the highest number version of the document and setting to zero of the lowest number of the same. The two last numbers of the Object Identifier that it represents will also be modified (OID). This type of modifications will be communicated to the subscribers of certificates corresponding to the CP or CPS modified by sending a notification to the electronic mail address provided by the user when issuing the certificate, at least 30 days in advance of publication.

The user can accept the modifications or reject them:

- If rejecting them, their certificate, issued under the instructions of the previous CPS, will be valid for the purposes included in the same, but not for the specific aims that are included in the new modified CPS or CP. If 15 days as of notification to the user no response has been received from the same, it will be considered that the user has not accepted the modification, although they may accept it at any later date.

- If accepting them, a recertification procedure will take place in which the new certificate will only be different from the revoked one in the OID of the policy that applies to it, to reflect the changes.

9.11.2. Publication and notification procedures.

All modifications to this Certification Practices Statement or the Certification Policy Documents will be published on the ACEDICOM website.

9.11.3. Certification Practice Statement approval procedures.

The EDICOM Technical Management is the competent entity to decide the approval of this Certification Practices Statement, as well as the Certification Policies associated with each type of certificate.

Likewise, the EDICOM Technical Management is responsible for the approval and authorization of any modifications to these documents.

9.12. RESOLUTION OF CONFLICTS.

9.12.1. Extrajudicial resolution of conflicts.

The ACEDICOM may establish, through the legal instruments whereby it articulates the relation with subscribers and authenticators, the procedures for mediation, arbitration and resolution of conflicts that are deemed appropriate, all notwithstanding the administrative procedure legislation.

9.12.2. Competent jurisdiction.

The ACEDICOM stipulates in their legal instruments with subscribers and authenticators, the procedures applicable for mediation and resolution of conflicts.

9.13. APPLICABLE LEGISLATION.

The operation and operations of ACEDICOM, as well as this CPS, is governed by the community and state legislation in force at all times.

The following norms are explicitly assumed to be applicable:

- Law 59/2003, of 19th December, on Electronic Signature.
- .The Order of 21st February 2000 whereby the regulation of accreditation of certification service providers and certification of certain products electronically is approved.
- Directive 11999/93/EC of the European Parliament and Council, of 13th of December 1999, whereby a community framework for electronic signature is established.

9.14. COMPLIANCE WITH APPLICABLE LAW.

The ACEDICOM hereby declares that the present CPS meets the requirements contained in Law 59/2003, of 19th December, on Electronic Signature.

9.15. DIVERSE CLAUSES.

No additional stipulation.