Autoritat de Certificació
de la Comunitat Valenciana

ACCV Certification Practice Statement (CPS)

Date: 03/10/2005	**Version:** 2.0
Status: APPROVED	**No. of pages:** 57
OID: 1.3.6.1.4.1.8149.2.2.0	**Classification: PUBLIC**
File: ACCV-CPS-V2.0.doc	
Prepared by: Autoritat de Certificació de la Comunitat Valenciana	

Table of Contents

1. INTRODUCTION

1.1. Presentation

The Autonomous Government of Valencia became a *Certification Services Provider or Certification Authority* by virtue of the stipulations of Decree 87/2002 of 30 May of the Valencian Government, which governs the use of advanced electronic signatures in the Autonomous Government of Valencia.

This document is considered the mandatory *Certification Practice Statement (CPS)* of the Certification Authority of the Community of Valencia.

Pursuant to the above and in compliance with the legal provision contained in Article 19 of Act 59/2003 of 19 December on Electronic Signatures, this Certification Practice Statement (CPS) details the general conditions and regulations of the certification services provided by the Certification Authority of the Community of Valencia, in relation to the management of electronic certificates and signature creation and verification data; conditions applicable to the request, issue, use, suspension and expiry of the validity of certificates; technical and organisational security measures; profiles and means of information on the validity of certificates; and,, where applicable, the existence of coordination procedures with the corresponding public registers which enable immediate exchange of information on the validity of the powers indicated on certificates and which must be recorded in these registers.

This Certification Practice Statement therefore constitutes the general summary of regulations applicable to all certification activity of the Certification Authority of the Community of Valencia in its capacity as Certification Services Provider. However, the various specialities applicable to each of the different types of certificates issued are stipulated in the various Certification Policies which, as supplementary and specific sets of regulations, shall prevail over this Certification Practice Statement, in matters referring to each type of certificate.

It must also be noted that this Certification Practice Statement is drawn up in accordance with the specifications of RFC 3647 *"Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework"* proposed by the *Network Working Group* for this type of document.

1.2. Name of the document and identification

Name of the document	ACCV Certification Practice Statement (CPS)
Document version	2.0
Document status	APPROVED
CPS reference / OID (Object Identifier)	1.3.6.1.4.1.8149.2.2.0
Issue date	December 13th 2009
Expiry date	Not applicable.
Location	This CPS can be viewed at http://www.accv.es/cps

1.3. Group of users of the ACCV services

1.3.1. Certification Authorities

In this Certification Practice Statement, the acronym "ACCV" shall be used to refer to all of the Certification Authorities that make up the ACCV.

The functions of the Certification Authority of the Community of Valencia are attributed to the higher body of the Administration of the Autonomous Government of Valencia which is the competent body for Telecommunications and Information Society matters.

The Certification Authorities that make up the ACCV are as follows:

- "Root CA GVA", as the first level Certification Authority. Its function is to establish the root of the trusted model of the Public Key Infrastructure or PKI. This CA does not issue certificates for end entities. This first level Certification Authority provides its own signature, issuing a certificate the signatory of which is "Root CAGVA", and which contains the public key (or signature verification data) of "Root CAGVA" signed with the signature creation data (private key) of "Root CAGVA". The digital print or fingerprint of the Root Certification Authority of the Autonomous Government of Valencia (Root CA), which establishes the root of the trusted model of the Public Key Infrastructure, expressed in hexadecimal format, is:

  A073 E5C5 BD43 610D 864C 2113 0A85 5857 CC9C EA46

  With this key, the self-signed certificate of the Root Certification Authority is verified, and it is valid from 6 July 2001 until 1 July 2021.

  - "CA GVA", as the subordinate Certification Authority of Root CA GVA. Its function is to issue end-entity certificates for ACCV subscribers. The "CA GVA" certificate is valid from 4 September 2001 until 2 September 2011.
  - ACCV-CA1 as the subordinate Certfication Authority of Root CA GVA. Its function is to issue certificates for legal entities. The "ACCV-CA1" certificate is valid from 4 may 2006 until 1 may 2016.
  - ACCV-CA2 as the subordinate Certification Authority of Root CA GVA. Its function is to issue certificates for ACCV subscribers. The "ACCV-CA2" certificate is valid from 4 may 2006 until 1 may 2016.
  - ACCV-CA3 as the subordinate of Certification Authority Root CA GVA. Its function is to issue certificates for the identification of Windows domain users. The ACCV-CA3 certificate is valid from 17 june 2006 until 14 june 2016.

1.3.2. Registration Authorities

Registration Authorities are those individuals or legal entities to which the ACCV entrusts the identification and verification of the personal circumstances of certificate requesters. For this purpose, Registration Authorities shall be responsible for guaranteeing that the certificate request contains the Requester's truthful and complete information, and that the certificate complies with the requisites stipulated in the corresponding Policy.

Bodies of the Autonomous Government of Valencia as well as other entities can be Registration Authorities provided that the corresponding collaboration agreement has been entered into. These Registration Authorities are referred to as User Registration Points or PRUs in the documentation relating to the Certification Authority of the Community of Valencia, and they are entrusted with confirmation of the requester's identity and delivery of the certificate. The functions of these Registration Authorities, which act on behalf of the ACCV, are as follows:

- To verify the identity and any personal circumstances of certificate requesters, which are relevant for the purpose of the certificates.
- To inform the person requesting the certificate, prior to its issue, of the precise conditions for use of the certificate and its limitations of use.
- To verify that the information contained in the certificate is accurate and that it includes all the information required for a recognised certificate.
- To ensure that the signatory is in possession of the signature creation data corresponding to the verification data recorded on the certificate.

1.3.3. End users

End Entities or Users are individuals or legal entities that have the capacity to request and obtain an electronic certificate pursuant to the conditions stipulated 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 of the Certification Policies that implement it, the following are End Entities of the ACCV certification system:

- Requesters
- Subscribers
- Relying third parties

1.3.3.1. Requesters

A Requester is the individual who, in his own name or as a representative of a third party, and with prior identification, requests the issue of a *Certificate*.

In the event that the situation involves a Requester of a Certificate the Subscriber of which is a legal entity, the aforementioned individual may only be a legal or voluntary representative or administrator with sufficient authority for these purposes of the legal entity that is to be the certificate subscriber.

1.3.3.2. Subscribers

For the purposes of this CPS, the ACCV certificate subscriber shall correspond to the term signatory contemplated in Article 6 of Act 59/2003 on Electronic Signatures.

The holder of the certificate shall have the status of subscriber. It is the individual or legal entity whose personal identity is linked to the electronically signed signature creation and verification data via a public key certified by the Certification Services Provider.

The signatory assumes the responsibility for safekeeping of the signature creation data, and may not grant use of it to any other person for any reason.

The group of users that may request the issue of ACCV certificates is defined and limited by each Certification Policy.

In general, and without prejudice to the provisions of the Certification Policy that is applicable for each case, it is stipulated that the possible subscribers are all of the citizens of the Community of Valencia.

1.3.3.3. Relying parties

All persons that voluntarily rely on certificates issued by the ACCV shall be considered as relying parties or relying third parties.

The Certification Policies applicable in each case limit the entitlement to rely on certificates issued by the ACCV.

In general, and without prejudice to the provisions of the Certification Policy that is applicable for each case, the employees, systems and applications of the Autonomous Government of Valencia are established as third parties that rely on ACCV certificates.

1.4. Use of certificates

The specific Certification Policies corresponding to each type of certificate issued by the ACCV constitute the documents in which the uses and limitations of each Certificate are determined. The uses and limitations of the different types of certificates issued by the ACCV are therefore not established in this CPS.

1.4.1. Prohibited uses

Certificates issued by the ACCV shall only be used in accordance with the function and purpose stipulated in this Certification Practice Statement and in the corresponding Certification Policies, and in accordance with the regulations in force.

1.5. ACCV Administration Policy

1.5.1. Identification details of the Administrative Organisation

Name	*Autoritat de Certificació de la Comunitat Valenciana*
E-mail address	*accv@accv.es*
Address	*Pl Cánovas del Castillo, 1 46005 Valencia*
Telephone number	*+34·961 923150*
Fax number	*+34·961 923151*

1.5.2. Contact person

Name	*Autoritat de Certificació de la Comunitat Valenciana*
E-mail address	*accv@accv.es*
Address	*Pl Cánovas del Castillo, 1 46005 Valencia*
Telephone number	*+34·961 923150*
Fax number	*+34·961 923151*

1.5.3. Competence for determining the conformity of the CPS to the various Certification Policies.

The Certification Authority of ministry of Justice and Public Administration is the competent body for determining the conformity of this CPS to the various Certification Policies of the Certification Authority of the Community of Valencia, pursuant to the stipulations in Decree 87/2002 of 30 May of the Valencian Government, which governs the use of advanced electronic signatures in the Autonomous Government of Valencia, and in Decree 114/2003 of 11 June, which approves the Organic and Functional Regulations of the Department of Infrastructure and Transport.

1.6. Definitions and Acronyms

1.6.1. Definitions

For the purposes of determining the range of the concepts that are used in this Certification Practice Statement, and in the various Certification Policies, the following shall be understood:

- Certification Authority: individual or legal entity which, in compliance with electronic signature legislation, issues electronic certificates and may also provide other services in relation to electronic signatures. For the purposes of this Certification Practice Statement, all those parties in this CPS defined as such shall constitute a Certification Authority.

- Registration Authority: individual or legal entity appointed by the ACCV to verify the identity of certificate requesters and subscribers, and, where applicable, to verify the validity of representatives' powers and subsistence of the legal status or of the voluntary representation. They are also referred to in the ACCV as PRUs or User Registration Points.

- Certificate chain: list of certificates that contains at least one certificate and the ACCV root certificate.

- Certificate: electronic document signed electronically by a Certification Services Provider which links the subscriber to signature verification data and confirms the subscriber's identity.

In this Certification Practice Statement, any reference to a certificate shall be understood to denote a Certificate issued by the ACCV.

- Root certificate: Certificate, the subscriber of which is ACCV and belongs to the ACCV hierarchy in the capacity of Certification Services Provider. This certificate contains the signature verification data of the aforementioned Authority signed with the signature creation data of the Authority as Certification Services Provider.

- Recognised certificate: Certificate issued by a Certification Services Provider which fulfils the requirements stipulated in Law regarding verification of requesters' identity and other circumstances and the reliability and the guarantees of the certification services provided, pursuant to the provisions of Chapter II of Heading II of Act 59/2003 of 19 December on Electronic Signatures.

- Key: sequence of symbols.

- Signature creation data (Private Key): unique data, such as codes or private cryptographic keys, which the subscriber uses to create Electronic signatures.

- Signature verification data (Public Key): data, such as codes or public cryptographic keys, which are used to verify Electronic signatures.

- Certification Practice Statement: ACCV statement made available to the public in electronic form and free of charge by virtue of the ACCV's status as Certification Services Provider in compliance with the provisions of the Act.

- Secure Signature Creation Device: instrument used to apply signature creation data fulfilling the requirements stipulated by Article 24.3 of Act 59/2003 of 19 December on Electronic Signatures.

- Certificate directory: information repository which complies with the ITU-T X.500 standard.

- Electronic document: set of electronic records which is stored on a medium that can be read by electronic data processing equipment, and which contains information.

- Security document: document required by Organic Law 15/99 on Personal Data Protection, the purposes of which is to establish the security measures set up, for the purposes of this document, by ACCV as Certification Services Provider, in order to protect personal data contained in the certification activity files, which contain personal data (hereinafter referred to as the Files).

- Processor: the individual or legal entity, public authority, service or any other organisation that processes personal data on behalf of the data controller.

- *Recognised* electronic signature: advanced electronic signature based on a recognised certificate and generated by means of a Secure Signature Creation Device.

- Advanced electronic signature: electronic signature enabling the personal identity of the subscriber to be established with respect to the signed data and the integrity of the data to be verified, due to the signature being linked exclusively to the subscriber and the data referred to, and due to having been created via means that it maintains under its exclusive control.

- Electronic signature: set of data in electronic form, recorded next to other data or associated with other data, which can be used as a means of personal identification.

- Hash function: an operation carried out on a set of data of any size, in such a way that the result obtained is another set of data of a fixed size, regardless of the original size, and which has the property of being associated only with the initial data; in other words, it is impossible to find two different messages that generate the same result when the hash function is applied.

- Hash or Digital fingerprint: result of fixed size which is obtained after applying a hash function to a message and which fulfils the property of being associated only with the initial data.

- Public Key Infrastructure (PKI): infrastructure which supports the issue and management of keys and certificates for services of authentication, encryption, integrity and non-repudiation.

- Certificate Revocation Lists: list which only features the inventories of revoked or suspended certificates (not expired certificates).

- Cryptographic Hardware Security Module: hardware module used to carry out cryptographic functions and store keys in a secure manner.

- Certificate Serial Number: integer and unique value that is uniquely associated with a certificate issued by the ACCV.

- OCSP (Online Certificate Status Protocol): IT protocol that permits verification of the status of a certificate at the time that this is used.

- OCSP Responder: IT server which, following the OCSP protocol, responds to OCSP requests with the status of the certificate for which the consultation is made.

- OID (Object Identifier): value, of a hierarchical and comprehensive nature, of a sequence of variable components which are always made up of non-negative integers separated by a point, which can be assigned to recorded objects and which have the feature of being unique among other OIDs.

- OCSP Request: request to an OCSP Responder to consult the status of a certificate, following the OCSP protocol.

- PIN: (Personal Identification Number) specific number known only by the person who has to access a resource that is protected by this mechanism.

- Certification Services Provider: individual or legal entity which, pursuant to electronic signature legislation, issues electronic certificates and may also provide other services in relation to electronic signatures. For the purposes of this Certification Practice Statement, it refers to the Certification Authorities belonging to the ACCV hierarchy.

- Certification Policy: document which supplements the Certification Practice Statement, stipulating the conditions of use and the procedures followed by ACCV to issue Certificates.

- PKCS#10 (Certification Request Syntax Standard): standard developed by RSA Labs, and internationally accepted as a 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, and which is used to unblock access to this resource.

- Data Controller: person who decides on the objective, content and use of the File contents.

- Security Manager: responsible for coordinating and monitoring measures imposed by the security document with regard to files.

- SHA-1: Secure Hash Algorithm. (secure algorithm in summary – 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 that is 160 bits long. The probability of finding two different messages which produce the same summary is practically nil. For this reason, it is used to ensure the integrity of documents during the Electronic Signature process.

- Time-stamping: recording of the date and time on an electronic document using indelible cryptographic procedures, on the basis of the specifications of Request For Comments: 3161 – “Internet X.509 Public Key Infrastructure Time–Stamp Protocol (TSP)”. This process enables the document to be dated in an objective manner.

- Requester: individual who requests the issue of a certificate, after having provided identification.

- Subscriber (or Subject): the holder or signatory of the certificate. The person whose personal identity is linked to the electronically signed data via a public key certified by the Certification Services Provider. The concept of subscriber shall be referred to in the certificates and in the IT applications related to their issue as Subject, due to strict reasons of international standardisation.

- Cryptographic card: card used by the subscriber to store private keys for signature and decoding, in order to generate electronic signatures and decode data messages. It is deemed a Secure Signature Creation Device according to law and enables the generation of recognised electronic signatures.

- Relying third parties or relying parties: parties that put their trust in an ACCV certificate, verifying the validity and legitimacy of the certificate in accordance with what is described in this Certification Practice Statement and in the Certification Policies associated with each type of certificate.

- X.500: standard developed by the ITU which defines the directory recommendations. Corresponds with the standard ISO/IEC 9594-1: 1993. 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 ITU, which defines the basic electronic format for electronic certificates.

1.6.2. Acronyms

ACCV Certification Authority of the Community of Valencia

CA Certification Authority

CP Certificate Policy

CPS Certification Practice Statement

CRL Certificate Revocation List

FIPS

IETF Internet Engineering Task Force

OID Object Identifier

OCSP Online Certificate Status Protocol

OPRU Registration Point Operator

PKI Public Key Infrastructure

PKIGVA PKI of the Autonomous Government of Valencia

PRU User Registration Point

RA Registration Authority

RFC Request For Comment

Sub CA Subordinate Certification Authority

2. Publication of information and certificate repository

2.1. CERTIFICATE REPOSITORY

The certificate repository service shall be available 24 hours a day, 7 days a week, and in the event of interruption due to *force majeure*, the service shall be re-established in the shortest possible time.

The ACCV repository consists of a high availability LDAP directory service, accessible at: ldap://ldap.accv.es:389.

The ACCV repository does not contain information of a confidential nature.

The ACCV does not use any other repository operated by any organisation other than the ACCV with the exception of the corporate LDAP directory of the Autonomous Government of Valencia (ldap.gva.es).

2.2. Publication

It is the obligation of the CAs belonging to the ACCV hierarchy of trust to publish the information relating to their practices, their certificates and the updated status of these certificates.

This CPS is public and can be found on the ACCV website: http://www.accv.es/cps, in PDF format.

ACCV Certification Policies are public and can be found on the ACCV website: http://www.accv.es/cps, in PDF format.

The ACCV CA certificate is public and can be found in the ACCV repository, in X.509 v3 format. It can also be found on http://www.accv.es.

Certificates issued by the ACCV are public and can be found in the ACCV repository, in X.509 v3 format.

The ACCV's Certificate Revocation List is public and can be found in CRL v2 format in the ACCV repository.

2.3. Frequency of updates

The CPS and Certification Policies are published each time that they are modified.

Certificates issued by the CA are published immediately after they are issued.

The CA shall add revoked certificates to the relevant CRL within the period of time stipulated in point 4.9.9 *Frequency of issue of CRLs*.

2.4. Certificate repository access controls.

Read access to the information in the ACCV repository and its website is free.

Only ACCV is authorised to modify, replace or delete information from its repository and website.

In this regard, the ACCV uses the appropriate means of control in order to restrict the capacity of write access to or modification of these elements.

3. Identification and Authentication

3.1. Registration of names

3.1.1. Types of names

All certificate subscribers require a distinguished name in accordance with standard X.500.

The distinguished name is included in the Common Name (CN) field and corresponds to the name that appears identified on the National ID Card, Passport or Document that identifies the signatory of the certificate.

3.1.2. Meaning of names

In all cases, distinguished names must have a meaning. If the Certification Policy applicable to the type of certificate does not indicate otherwise, the requester's name and Tax ID Code are used.

ACCV does not permit the use of pseudonyms in the certificates that it issues.

3.1.3. Interpretation of name formats

The rules used by ACCV to interpret the distinguished names of the certificates that it issues are those contained in ISO/IEC 9595 (X.500) Distinguished Name (DN).

3.1.4. Uniqueness of names

Distinguished names must be unique and shall allow for no ambiguity.

For this purpose, the name of the subscriber followed by his/her Tax ID Code, with the format "*name* - NIF *Tax ID Code number*" shall be included as part of the common name of the distinguished name.

The Certification Policies may provide for the replacement of this uniqueness system.

3.1.5. Resolution of disputes relating to names

The inclusion of a name in a certificate does not imply the existence of any right over the name and this shall be without detriment to the paramount right that third parties might hold.

The ACCV shall not act as an arbitrator or mediator, nor shall it resolve any dispute relating to the ownership of names of persons or organisations, domain names, brand names or trade names, etc.

The ACCV reserves the right to refuse a certificate request due to conflict regarding the name.

3.1.6. Recognition, authentication and function of registered trademarks.

The Spanish Patent and Trademark Office of the Ministry of Industry, Tourism and Trade has awarded the following trademarks:

- "Certification Authority of the Community of Valencia", mixed mark no. 2.591.232, awarded on 15 September 2004, published in the Spanish Official Industrial Property Gazette of 16 October 2004.

- "ACCV", trademark no. 2.591.037, awarded on 19 May 2005, published in the Spanish Official Industrial Property Gazette of 16 June 2005.

3.2. Initial Validation of Identity

3.2.1. Methods of proving ownership of the private key.

In the event that the key pair is generated by the end-entity (subscriber), the end-entity must prove ownership of the private key corresponding to the public key requested, which is certified by means of issuing the request for certification in PKCS #10 format.

This rule may be revoked on a case by case basis by the stipulations of the applicable Certification Policy for each request.

3.2.2. Authentication of the identity of an organisation.

In the event that a Certification Policy deems it necessary for an organisation's identity to be authenticated, this policy shall determine the necessary methods for verifying the aforementioned identity.

This CPS explicitly prohibits the use of remote methods of identification of organisations.

3.2.3. Authentication of the identity of an individual.

The process of individual identification is defined by the Certification Policy applicable for each type of certificate.

The process shall not be regarded as having to be less strict than other systems of authentication used by the Autonomous Government of Valencia.

As a general rule, remote methods of identification shall not be used that are different from the digital signature produced with certificates issued by the ACCV itself or by any other recognised Certification Services Provider.

3.3. Identification and authentication of key renewal requests.

3.3.1. Identification and authentication of routine requests for renewal.

Identification and authentication for certificate renewal can be carried out using the techniques for initial authentication and identification or using digitally signed requests via the original certificate intended for renewal, provided that the original certificate has not expired or been revoked There are therefore two alternative methods for renewal:

- Signed web forms in the Personal Certification Services Area, available at www.accv.es.

- Personal attendance at any User Registration Point, with sufficient identification documents (see section 3.2.3. of this CPS).

In addition, and in accordance with the stipulations of Article 13.4 b) of Act 59/2003 of 19 December on Electronic Signatures, certificate renewal via digitally signed requests requires that the period of time elapsed since personal identification must be less than five years.

3.3.2. Identification and authentication of requests for key renewal following a revocation – Key uncompromised.

The identification and authentication policy for certificate renewal following a revocation without compromise of the key shall be the same as for initial registration. Alternatively, any electronic method

may be used which reliably and unequivocally guarantees the identity of the requester and the authenticity of the request.

3.4. Identification and authentication of key revocation requests

The revocation request process is defined by the Certification Policy applicable for each type of certificate.

The identification policy for revocation requests can be the same as for initial registration. The authentication policy shall permit revocation requests digitally signed by the certificate subscriber.

In all cases, the different Certification Policies may define other identification policies that are less strict.

ACCV or any of the entities that comprise it, may, on their own initiative, request the revocation of a certificate if they are aware or suspect that the subscriber's private key has been compromised, or if they are aware of or suspect any other event that would make taking such action advisable.

The different Certification Policies may define the creation of a revocation password at the time of registration of the certificate.

4. The life cycle of certificates.

The specifications in this section are stated without prejudice to the stipulations provided for in each of the different Certification Policies for the different types of certificates issued by the ACCV.

4.1. Request for certificates

The ACCV Registration Authority that receives the request is responsible for determining that the type of certificate requested is appropriate to the specific characteristics of the requester, in accordance with the contents of the Certification Policy applicable to the aforementioned certificate and, in this way, resolving the submitted request.

Each Certification Policy informs certificate requesters of the specific information that must be supplied beforehand.

4.2. Processing the request for certificates.

The Registration Authority or Entity is responsible for verifying the identity of the requester, as well as the documentation and the record that the requester has signed the document of appearance. Once the request has been completed, the Registration Authority shall send it to the ACCV Certification Authority.

4.3. Issuing certificates

ACCV is not responsible for monitoring, investigating or confirming the accuracy of the information contained in the certificate subsequent to its issue. In the event of receiving information on inaccurate or currently non-applicable information contained on the certificate, the certificate may be revoked.

The certificate shall be issued once ACCV has carried out the necessary verifications to validate the request for certification. This Certification Policy is the system via which it determines the nature and the method of carrying out these verifications.

When the ACCV's CA issues a certificate in accordance with a valid request for certification, it shall send a copy of the certificate to the Registration Authority that issued the request and another to the ACCV's repository.

It is the Registration Authority's responsibility to notify the certificate's subscriber of the issue of the certificate and to provide him/her with a copy, or failing that, to inform the subscriber of how a copy can be obtained.

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

4.4. Acceptance of certificates

Acceptance of certificates by the signatories takes place at the time of signature of the certification contract associated with each Certification Policy. Acceptance of the contract implies that the subscriber is aware of and accepts the associated Certification Policy.

4.5. Use of the key pair and certificate.

Certificates issued by the ACCV are used for communications between citizens and the Valencian Administrations. Certificates can also be used by their holders in any other electronic communications with other entities, organisations, legal entities or individuals that accept certificates.

Certificates can be used as a means of secure identification of the subscriber for the purpose of signing electronic documents, e-mails, etc.

They can also be used to encrypt information in a permanent, electronic form.

4.6. Renewal of certificates.

The period of renewal of certificates begins 70 days before the expiry date of the certificate, when the subscriber receives an e-mail providing notification of the steps to be followed to proceed with renewal of the certificate. These steps involve online access to the Personal Certification Services Area at www.accv.es, identification of the user based on the user's own certificate and the generation of a new certificate or pair of certificates.

4.7. Key renewals

Key renewals require certificate renewal to also be carried out; they cannot be carried out as separate processes.

4.8. Modification of certificates.

Only modification of the fields relating to the subscriber's postal address and telephone number can be permitted during a certificate's life cycle.

4.9. Revocation and suspension of certificates.

4.9.1. Circumstances for revocation

A certificate is revoked when:

- The certificate subscriber or the subscriber's keys or the keys of the subscriber's certificates have been compromised by:
  - The theft, loss, disclosure, modification or other compromise or suspected compromise of the user's private key.
  - Deliberate improper use of keys and certificates, or failure to observe the operational requirements of the subscription agreement, the associated CP or this CPS.
- The following shall render the issue of a certificate defective:
  - An actual prerequisite for issue of the certificate has not been fulfilled.
  - A fundamental factor in the certificate is known to be or is reasonably believed to possibly be false.
  - A data entry error or other processing error.
- The key pair generated by a final user proves to be "weak".
- The information contained in a certificate or used to make a request for a certificate becomes inaccurate, for example when the owner of a certificate changes his/her name.
- A valid revocation request is received from an end-user.

- A valid revocation request is received from an authorised third party, for example a court order.
- The certificate of a higher RA or CA in the certificate's hierarchy of trust is revoked.

4.9.2. Entity that may request the revocation

The revocation of a certificate may be requested by the certificate's subscriber or by the ACCV.

Certificate subscribers can request certificate revocation for any reason and must request revocation in accordance with the conditions specified in the following section.

4.9.3. Revocation request procedure

The request procedure for revocation of each type of certificate is defined in the corresponding Certification Policy.

In general, and without prejudice to the stipulations of the Certification Policies:

- Remote revocation requests shall be accepted if they are digitally signed with an ACCV certificate or a certificate of any other recognised Certification Services Provider, and revocation requests submitted via attendance in person shall be accepted if the user identification requirements established for initial registration are fulfilled.
- In the event of a revocation request being made without possible verification of the requester's identity (by telephone, e-mail without digital signature, etc.), the certificate shall be suspended for a maximum period of 30 calendar days, during which time the veracity of the request shall be verified. In the event of not being able to verify the request within this period, the certificate shall be revoked. It must be noted that the certificate shall not be usable from the time that the request process begins.
- After the certificate has been revoked, the certificate subscriber must destroy the private key that corresponds to the certificate and not use the revoked certificate.

There is a request form for certificate revocation on the ACCV website at: http://www.accv.es, in the Personal Certification Services Area.

A revocation request, whether it is made on paper or electronically (e.g. e-mail), must contain the information that is described on the revocation request form, referred to in each of the Certification Policies.

4.9.4. Period of grace for the revocation request

Revocation shall occur immediately when each request verified as valid is processed. There is therefore no period of grace associated with this process.

4.9.5. Circumstances for suspension

Suspension entails invalidity of the certificate throughout the time that it is suspended.

Suspension may only be declared on the initiative of the ACCV, when a certificate revocation request has been made without possible immediate verification of the requester's identity (by telephone, via e-mail without digital signature, etc.), or when the ACCV suspects that the private key associated with a user's certificate may have been compromised, or if the ACCV has doubts about the veracity of the data associated with the certificate. The maximum length of time that a certificate can be suspended for any of these causes shall be 30 days.

A certificate shall also be suspended if this is ordered by a judicial or administrative authority, for the length of time that this authority stipulates.
The ACCV does not permit the suspension of certificates as an independent operation on its certificates.

4.9.6. Body that may request the suspension

Both the certificate subscriber and the Certification Authority of the Community of Valencia may request the suspension of a certificate issued by the Certification Authority of the Community of Valencia.

4.9.7. Suspension request procedure

A certificate suspension requested by the subscriber must be carried out by telephone, using the telephone support number of the Certification Authority of the Community of Valencia: 902482481.

4.9.8. Limits of the suspension period

The period of suspension of validity of certificates shall normally be 15 days, except in the event that the legal or administrative decision that orders the suspension imposes a longer or shorter period, in which case the suspension period shall comply with the judicial or administrative decision.

4.9.9. Frequency of issue of CRLs

ACCV shall publish a new CRL in its repository at maximum intervals of 3 hours, even if there have been no modifications to the CRL (changes to the status of certificates) during the aforementioned period.

4.9.10. CRL verification requirements

CRL verification is obligatory for each use of end entity certificates.
Relying third parties must check the validity of the CRL prior to each time that it is used and download the new CRL from the ACCV repository at the end of the period of validity of the previous CRL.

4.9.11. Availability of online verification of revocation and status

ACCV provides an OCSP server for online verification of certificate status at: ocsp.accv.es:80

4.9.12. Requirements for online verification of revocation

The OCSP server is free to access and there is no requisite for its use except those derived from use of the OCSP protocol according to the provisions of RFC 2560.
ACCV also provides web services for consultation of the validity status of issued certificates.

4.9.13. Other available methods of consulting revocation information

Some Certification Policies can support other methods of providing information on revocation status, such as CRL Distribution Points (CDP).

4.9.14. Verification requirements for other methods of consulting revocation information

In the event that the applicable Certification Policy supports other methods of providing revocation information, the requirements for verification of this information shall be specified in the relevant Certification Policy.

4.9.15. Special requirements for the renewal of compromised keys

There shall be no variation in the above clauses in the event that the revocation is due to the compromise of the private key.

4.10. Certificate status verification services.

CRL systems and online certificate status consultation systems shall be available 24 hours a day and 7 days a week.

4.11. End of subscription.

Subscription is completed with the expiry or revocation of the certificate.

4.12. Storage and recovery of keys.

The ACCV may deposit certificates and encryption keys for a certain type of personal certificate, but never those used for identification of the subscriber or electronic signature of documents.
Specific details are included in the Certification Policies associated with each type of certificate.

5. Physical security, management and operations controls

5.1. Physical security controls

5.1.1. Location and structure

The information systems of the ACCV are located in Data Processing Centres with appropriate levels of protection and solidity of structure, and surveillance 24 hours a day, 7 days a week.

5.1.2. Physical access

The ACCV Data Processing Centres have different security perimeters, with different security requirements and authorisations. The equipment that protects the security perimeters includes combination-based physical access control systems, video surveillance and recording, and intrusion detection systems, among other equipment.

In order to access the most protected areas, duality of access and an extensive period of time working for the company is required.

5.1.3. Power supply and air conditioning

The installations are equipped with uninterruptible power supply systems with sufficient power to autonomously power the electrical network during controlled system power cuts and to protect equipment from electrical fluctuations that could damage it.

The equipment shall only be switched off in the event of failure of the autonomous power generation systems.

The air conditioning system consists of various independent pieces of equipment with the capacity to maintain temperature and humidity levels within the systems' optimum margins of operation.

5.1.4. Exposure to water

The ACCV's Data Processing Centres are equipped with flood detectors and alarm systems which are appropriate for the environment.

5.1.5. Fire protection and prevention

The ACCV's Data Processing Centres are equipped with automated systems for detecting and extinguishing fires.

5.1.6. Storage system

Sensitive data media is stored securely in fireproof cabinets and safes in accordance with the type of medium and the classification of the information contained in them.

These cabinets are located in different buildings to remove risks associated with a single location.

Access to these media is restricted to authorised personnel.

5.1.7. Disposal of discarded material

The disposal of magnetic and optical media and information on paper is carried out securely following procedures stipulated for this purpose, using processes of demagnetisation, sterilisation, destruction or shredding, depending on the type of medium to be processed.

5.1.8. Remote backup

Encrypted remote backup copies are made on a daily basis and are stored in premises located close to the back-up Data Processing Centre, where the ACCV operations would continue in the event of a serious incident or collapse of the main Data Processing Centre.

5.2. Procedure controls

The ACCV's information systems and services are operated in a secure manner, following pre-established procedures.

For security reasons, information relating to procedure controls is considered to be confidential in nature and is only explained in summarised form.

5.2.1. Positions of trust

The roles identified for the control and management of services are as follows:
a. Systems Administrator
b. User Registration Point (PRU) Administrator
c. Certification Authority Operator
d. PRU Operator
e. Training, Support and Communications Manager
f. Security Manager
g. Auditor
h. Legal Expert
i. Documentation Manager
j. Deployment Support Manager
k. Certification Authority Coordinator

5.2.1.1. Systems Administrator

Is responsible for the installation and configuration of operating systems and software products, and maintaining and updating the products and programs installed.

Is entrusted with the establishment and documentation of the monitoring procedures of the systems and services provided, as well as the monitoring of the tasks carried out by the Certification Authority Operators.

Must ensure that services are provided with the appropriate level of quality and reliability, in accordance with the critical level of these services.

Is responsible for the correct implementation of the Copies Policy, and in particular, for maintaining sufficient information which permits the effective restoration of any of the systems. Along with the Certification Authority Operator and, in exceptional cases, the PRU Administrator, is responsible for making the local backup copies.

Must maintain the inventory of servers and equipment making up the ACCV certification platform group.

Must not have access to aspects relating to the security of systems, or of the network, etc. (registrations/removals of users, management of firewall rules, management and maintenance of intrusion detection systems, etc.).

Must collaborate with the Auditors in relation to everything that is required of him/her.

5.2.1.2. PRU Administrator

This profile is similar to that of Systems Administrator but dedicated to the tasks related to installation, maintenance and control of the systems that make up the User Registration Points.

Is responsible for administrative tasks relating to PRU Operators' authorisations, confidentiality agreements, etc.

Must maintain the inventory of PRUs and equipment used for PRU operations.

In exceptional cases, may work with the Systems Administrator and Certification Authority Operator to carry out local backups of the PKI systems.

In the same way as for Systems Administrators, must not have access to aspects relating to the security of systems, or of the network, etc. (registrations/removals of users, management of firewall rules, management and maintenance of intrusion detection systems, etc.).

Must collaborate with the Auditors in relation to everything that is required of him/her.

5.2.1.3. Certification Authority Operator

Assists the Systems Administrators and PRU Administrators in technical or administrative matters that do not require access to the DPC.

Must assist the Training, Support and Communications Manager in any tasks instructed.

Must collaborate in accordance with the requests of PRU Administrators, with regard to inventory roles, assistance in the installation of systems making up the PRUs, documentation preparation, collaboration in the training and support of PRU Operators, etc.

Works with the Documentation Manager to monitor existing documents, to monitor the documentation file (hard copy) and to revise certificates and contracts.

Works with the Security Manager on administrative tasks, inventory tasks and, in general, technical or administrative tasks.

Along with the Systems Administrator and, in exceptional cases, the PRU Administrator, is responsible for making the local backup copies. This is the only task that the Certification Authority Operator carries out within the DPC.

Must collaborate with the Auditors in relation to everything that is required of him/her.

5.2.1.4. User Registration Point Operator

Is solely and exclusively responsible for functions relating to the identification of certificate requesters, the processing of digital certificates, the revocation of digital certificates and the unblocking of cryptographic cards, all while exclusively using the tools and applications provided by the PRU Administrators, and strictly following the approved procedures.

Within this job profile, there is a subgroup called "CallCentre Suspension Operators" which only have privileges to suspend certificates after receiving the certificate's holder revocation request by telephone.

Must collaborate with the Auditors in relation to everything that is required of him/her.

5.2.1.5. Training, Support and Communications Manager

Is responsible for the maintenance of content of the website of the Certification Authority of the Community of Valencia.

Is entrusted with communication and updating duties in relation to the ACCV's website.

Is responsible for defining the training plan for end users, Call Centre agents and personnel involved directly in the operation and administration of the ACCV's certification platform. In addition, works with the PRU Administrator in preparing training for PRU Operators.

The Training, Support and Communications Manager is responsible for preparation of the contents of the courses taught on the e-learning corporate platform.

Must revise the Call Centre incident and response files on a monthly basis, and revise the Call Centre agents' scripts.

Must coordinate the actions of microcomputing personnel and provide the tools and necessary material for them to carry out their duties correctly.

The Training, Support and Communications Manager may receive the collaboration of the Certification Authority Operators for those tasks that he/she deems appropriate.

5.2.1.6. Security Manager

Must comply with and ensure compliance with the ACCV's security policies, and must be responsible for any matter relating to the security of the ACCV: physical security, security of applications, of the network, etc.

Is the individual responsible for managing the perimeter protection systems and specifically managing firewall rules.

Is responsible for installation, configuration and management of the intrusion detection systems (IDS) and the tools associated with these.

Is responsible for resolving or ensuring the resolution of security incidents that have occurred, eliminating vulnerabilities detected, etc.

Is responsible for management and control of the DPC physical security systems, the access control systems, the air conditioning and power supply systems.

Is responsible for explaining the security systems to personnel that must know about them, ensuring the awareness of all ACCV personnel and ensuring compliance with security regulations and policies.

Must establish schedules for carrying out the analysis of vulnerabilities, trials and tests of service continuity plans and information systems audits.

Must collaborate with the Auditors in relation to everything that is required of him/her.

5.2.1.7. Auditor

The auditor profile corresponds to an internal position, without prejudice to the personnel responsible for external audits.

The Auditor is responsible for:

- Verifying the existence of all the required and listed documentation
- Verifying the consistency of the documentation with procedures, inventoried assets, etc.
- Verifying the monitoring of incidents and events
- Verifying the protection of systems (exploitation of vulnerabilities, access logs, users, etc.).
- Verifying alarms and physical security elements
- Verifying compliance with regulations and legislation
- Verifying knowledge of procedures among the personnel involved

In short, must verify all aspects mentioned in the security policy, copies policies, certification practices, Certification Policies, etc. in the group of ACCV systems and within the ACCV personnel, as well as in the PRUs.

5.2.1.8. Legal expert

Is responsible for the legal aspects of the provision of certification services and the formalisation of the provision of these services to other entities, with which a certification agreement has to be set up.

Is entrusted with processing the approval and publication of Certification Policies, modifications to the Certification Practice Statement document and, in general, to any government regulations which affect the Certification Authority's certification platform and services.

Ensures compliance with the electronic signature legislation currently in force, analysing the existing Certification Policies and Certification Practice Statement and those which are subject to approval, and notifying the inconsistencies or problems that he/she detects.

Must collaborate with the Auditors in relation to everything that is required of him/her.

5.2.1.9. Documentation Manager

Is responsible for maintaining the ACCV's electronic documentation repository and hard-copy documentation files.

Checks that documents are updated when required and by the persons that the Documentation Manager appoints, and may even exceed specified requirements for documents to be updated or maintained.

Is responsible for keeping the document index file up to date and is the only individual authorised to store, delete or modify documents in the ACCV's documentation repository.

May receive the collaboration of the Certification Authority Operators in carrying out documentary control or inventory tasks.

Must guarantee that any certificate issued is associated with a certification contract drawn up in hard copy.

Must collaborate with the Auditors in relation to everything that is required of him/her.

5.2.1.10. Deployment Support Manager

Is responsible for maintaining contact with development teams of IT applications of user organisations and entities of the ACCV's services, in order to provide the necessary support and assistance for the development and deployment of data transmission applications and services which use digital certification and electronic signatures.

Is responsible for redirecting technical IT or legal queries that he/she cannot resolve to the appropriate personnel.

Must gather sufficient information (projects information template) in order to be able to provide an optimum level of assistance and advice.

Must provide guidance on development possibilities, techniques and tools, taking into account the corporate information systems, security policy, applicable legislation, etc.

The Deployment Support Manager must provide guidance on existing technical and administrative regulations, the role of creation of PRUs by organisations and entities that offer electronic transmission services, the operating method of these, etc. Must collaborate with ministries or entities with which a certification agreement has been set up, in order to analyse methods of distribution of certificates, creation of PRUs, etc.

Must collaborate with the Auditors in relation to everything that is required of him/her.

5.2.1.11. Certification Authority Coordinator

Is responsible for monitoring and control of performance of the roles attributed to each job profile described above, and for the distribution of new tasks among the profiles.

Is responsible for constituting a means of communication between the personnel appointed to each of the profiles and the Certification Authority management body. In the same way, is responsible for serving as a link with other departments of the Autonomous Government of Valencia.

Is responsible for presenting strategic decisions to the Certification Authority management body and for approving tactical decisions.

Advises ACCV personnel on training to be taken, retraining courses, etc. and facilitates the implementation of these courses and training plans.

Must collaborate with the Auditors in relation to everything that is required of him/her.

5.2.2. Number of persons required per task

Two persons are required for activation of the keys of cryptographic hardware devices for key generation and storage. Modification of the configuration parameters of cryptographic hardware requires authentication by two authorised persons with sufficient privileges.

5.2.3. Identification and authentication for each role

All authorised ACCV users are identified by means of digital certificates issued by the ACCV itself and gain authentication by means of cryptographic smart-cards and/or biometric devices.

Authentication is supplemented with the corresponding authorisations for accessing certain information assets or ACCV systems.

5.3. Personnel security controls

This section is taken from the ACCV *Personnel Security Controls* document.

5.3.1. Background, qualifications, experience and accreditation requirements

The Certification Authority requires all personnel who carry out duties in its installations to have sufficient qualifications and experience in environments relating to the provision of certification services.

All personnel must comply with the organisation's security requirements and must possess:

- Knowledge and training in digital certification environments.
- Basic training in information systems security.
- Specific training for their post.
- Academic qualification or experience in the equivalent industry

5.3.2. Background verification procedures

Not stipulated. By means of verification of CVs of personnel.

5.3.3. Training requirements

The personnel of the Certification Authority are subject to a specific training plan for carrying out their role within the organisation.

This training plan includes the following aspects:

1. Training in the basic legal aspects relating to the provision of certification services.

2. Training in information systems security.

3. Services provided by the Certification Authority.

4. Basic concepts of PKI.

5. Certification Practice Statement and the relevant Certification Policies.

6. Incident management.

5.3.4. Requirements and frequency of training updates

Prior to technological changes in the environment, the introduction of new tools or the modification of operating procedures, the appropriate training will be carried out for the personnel affected.

Training sessions will be carried out prior to changes in the Certification Practice Statement, Certification Policies or other relevant documents.

5.3.5. Frequency and order of task rotation

No rotation plan has been defined for the personnel of the Certification Authority in the assignment of its tasks.

5.3.6. Penalties for unauthorised actions

In the event that an action is carried out which is unauthorised with respect to the operations of the Certification Authority, disciplinary measures shall be taken. Actions which contravene the Certification Practice Statement or the relevant Certification Policies in a negligent or malicious way shall be considered to be unauthorised actions.

If any infringement occurs, the Certification Authority shall suspend the access of the persons involved to all the Certification Authority information systems, as soon as it becomes aware of the infringement.

In addition, and according to the seriousness of the infringements, the sanctions provided for in the Civil Service Act, the company collective agreement, or the Workers' Statute shall be applied in accordance with the employment situation of the infringing party.

5.3.7. Personnel appointment requirements

All Certification Authority personnel are subject to a secrecy obligation by virtue of signing the confidentiality agreement when taking up their post. In this agreement, they also undertake to carry out their duties in accordance with this Certification Practice Statement, the ACCV Information Security Policy and the approved procedures of the ACCV.

5.3.8. Documentation provided to personnel

Personnel joining the Certification Authority are provided with access to the following documentation:

- Certification Practice Statement
- Certification Policies
- Privacy policy
- Information Security Policy
- Organisation chart and roles of personnel

Access is provided to documentation relating to regulations and security plans, emergency procedures and all technical documentation necessary for personnel to carry out their roles.

5.3.9. Periodic compliance checks

The check that personnel possess the necessary knowledge is carried out at the end of the training sessions and on a discretional basis, by the training staff responsible for teaching these courses and, as a last resort, by the Training, Support and Communications Manager.

The verification of the existence of the documentation that employees must be familiar with and sign is carried out annually by the Documentation Manager.

The Security Manager carries out an annual review of the compliance of the authorisations granted with the actual privileges given to employees.

5.3.10. Termination of contracts

In the event of the termination of the employment contract of a member of personnel that performs his/her roles in the ACCV, the Security Manager shall proceed to carry out the actions or verifications detailed in the following points, either directly or by issuing instructions for this purpose to the appropriate personnel.

5.3.10.1. Access to organisation locations

The individual's access privileges to the installations of the organisation to which access is restricted must be removed. This involves, as a minimum requirement, removal of the authorisation of access to the following locations

- Removal of the access privilege to the main DPC in Metrored
- Removal of the access privilege to the continuity-preproduction DPC in Tissat
- Removal of the access privilege to IT rooms and offices at Colón, 66

5.3.10.2. Access to Information Systems

The individual's access privileges to the organisation's information systems must be removed, giving special attention to administration and remote access privileges.

- Removal of user privilege in servers
- Removal of user privilege in the ACCV Documentation Repository (RD-ACCV)
- Removal of user privilege in the Incident Control System
- Change known passwords

▪ Root/Administrator servers

▪ FW

▪ Network electronics (switches, load balancers, routers, etc.)

▪ IDS

5.3.10.3. Access to documentation

Removal of access to all information, with the exception of information considered PUBLIC.

Removal of access to the Secure Developers Area on the ACCV website.

5.3.10.4. Issuing information to the rest of the organisation

The rest of the organisation must be clearly informed of the departure of the individual and of his/her loss of privileges. The intention is to thereby minimise the possibility of "social engineering" attacks by former employees..

5.3.10.5. Issuing information to suppliers and collaborating entities

Suppliers and entities collaborating with the ACCV must also be informed of the departure of the individual and that he/she no longer represents the ACCV.

5.3.10.6. Return of material

It must be verified that material provided by ACCV has been returned. For example:

- PC and monitor/laptop
- Furnishings/office keys
- Mobile telephone
- etc.

5.3.10.7. Suspension as PRU Operator

The collaborator's requirement to maintain his/her capacity to function as PRU Operator after leaving the organisation must be reviewed. If this requirement does not exist, his/her access permit to the XRAO system must be revoked.

5.4. Security Control Procedures

5.4.1. Types of events recorded

ACCV records all events relating to:

- Successful or failed attempts to change the security parameters of the operating system.
- Start-up and stoppage of applications.
- Successful or failed attempts to start or end a session.
- Successful or failed attempts to create, modify or delete system accounts.
- Successful or failed attempts to create, modify or delete authorised system users.
- Successful or failed attempts to request, generate, sign, issue or revoke keys and certificates.
- Successful or failed attempts to generate, sign or issue a CRL.
- Successful or failed attempts to create, modify or delete certificate holder information.
- Successful or failed attempts to access installations by authorised or unauthorised personnel.
- Backup, file and restoration.
- Changes to system configuration.
- Software and hardware updates.
- System maintenance.
- Changes of personnel

5.4.2. Log processing frequency

Two levels of audits of recorded events monitoring take place with a weekly and monthly frequency respectively.

5.4.3. Audit log retention period

ACCV shall retain all the audit records generated by the system for a minimum period from the date of their creation of two (2) years for those relating to daily audits, five (5) years for those relating to monthly audits and fifteen (15) years for those relating to annual audits.

5.4.4. Audit log protection

Each audit log contained in these records is encrypted using the public key of a certificate that is issued for the ACCV audit function. The backup copies of these records are stored in a fireproof file locked within the secure ACCV installations.

The destruction of an audit file can only be carried out with the authorisation of the System Administrator, the Security Manager and the ACCV Auditor. This destruction can be begun on the written recommendation of any of these three parties or of the Administrator of the audited service.

5.4.5. Audit log backup procedures

Incremental local and remote copies are generated on a daily basis, in accordance with the ACCV's Backup Copies Policy.

5.4.6. Audit information gathering system (internal v. external)

The audit gathering system on the ACCV's information systems is a combination of automatic and manual processes carried out by the operating systems, the ACCV's applications, and the personnel that operates them.

5.4.7. Notification to the subject causing the event

Not stipulated.

5.4.8. Analysis of vulnerabilities

At least one monthly analysis is carried out of vulnerabilities and perimeter security.

It is the responsibility of the coordinators of the analysis teams to inform the ACCV, via the Security Manager, of any problem preventing the performance of the audits, or the delivery of the resulting documentation. It is the ACCV's responsibility to inform the audit teams of the suspension of analyses.

The security analyses involve the initiation of the specific tasks to correct the vulnerabilities detected and the issue of a counter-report by the ACCV.

5.5. Information and records file

5.5.1. Type of information and events recorded

The information and events recorded are as follows:

- The audit records specified in point 5.4 of this Certification Practice Statement.

- The backup supports of the servers that make up the ACCV infrastructure.

- Documentation relating to the certificates' life cycles, including:

- Certification contract
- Copy of the identification documentation provided by the certificate requester
- Location of the User Registration Point -PRU- where the certificate was issued
- Identity of the Operator of the PRU where the certificate was issued
- Date of the last in-person identification of the subscriber

– Confidentiality agreements

– Agreements signed by the ACCV

– Authorisations for Access to Information Systems (including User Registration Point Operator authorisation).

5.5.2. File retention period.

All the information and documentation relating to the life cycle of certificates issued by the ACCV is retained for a period of 15 years.

5.5.3. File protection.

File access is restricted to authorised personnel.

In addition, events relating to certificates issued by the ACCV are cryptographically protected to guarantee detection of manipulations of their content.

5.5.4. File backup procedures.

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

One copy is made locally and is stored in a fireproof safe in the ACCV's main Data Processing Centre.

The second copy of the data is made in encrypted and remote form and is stored in the continuity/backup Data Processing Centre located in a building other than the ACCV's main DPC building.

5.5.5. Requirements for the time-stamping of records.

The ACCV systems record the time that the records are made. The systems' time is provided by a reliable time source. All the ACCV systems synchronise their time with this source.

5.5.6. Audit information gathering system (internal v. external).

The information gathering system is an internal ACCV system.

5.5.7. Procedures for obtaining and verifying archived information

Only authorised personnel have access to physical backup files and IT files in order to carry out verifications of integrity or other kinds of verifications.

Verifications of the integrity of electronic archives (backups) are carried out automatically at the time of their generation and an incident is created in the event of errors or unexpected events.

5.6. Change of Key

The procedures for providing a new public key to CA users are specified in the corresponding Certification Policy for each type of certificate.

5.7. Recovery in the event of a comprised key or disaster

In the event of the unavailability of the installations of the Certification Authority for a period greater than six hours, the ACCV's Service Continuity Plan shall be activated.

The Continuity Plan guarantees that services identified as critical due to their availability requirement will be available in the Continuity DPC in less than 12 hours following activation of the Plan.

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

If hardware, software and/or data resources are altered or are suspected of having been altered, the operation of the ACCV's services shall be suspended until a secure environment is re-established with the incorporation of new components of creditable effectiveness. In parallel, an audit shall be carried out to identify the cause of the alteration and ensure the non-reoccurrence of the alteration.

In the event of issued certificates being affected, the certificate subscribers shall be notified of this and recertification shall take place.

5.7.2. An entity's public key is revoked

In the event of the revocation of an ACCV entity's certificate, the corresponding CRL shall be generated and published, the entity's operations shall be suspended and the process will begin of generation, certification and start-up of a new entity with the same name as the withdrawn one and with a new key pair.

In the event that the affected entity is a CA, the entity's revoked certificate shall remain accessible in the ACCV repository for the purpose of continuing to permit the verification of the certificates issued during the entity's period of operation.

The entities making up the ACCV that are dependent on the renewed entity shall be informed of the fact and ordered to request their recertification due to the entity having been renewed.

5.7.3. An entity's key is compromised

In the event of the compromise of an entity's key, it shall immediately be revoked in accordance with the provisions in the previous point and this shall be notified to the rest of the entities that are part of ACCV whether they are dependent or not on the affected entity.

Certificates signed by entities dependent on the compromised entity during the period between compromise of the key and revocation of the corresponding certificate, shall in turn be revoked, and their subscribers informed and recertified.

5.7.4. Security installation after a natural disaster or other type of disaster

In the event of a natural disaster affecting the installations of the ACCV's main Data Processing Centre and, therefore, the services provided from this location, the Service Continuity Plan shall be activated, guaranteeing that the services identified as critical due to their availability requirement, shall be available in the Continuity DPC in less than 12 hours following activation of the Plan, and the remaining essential services shall be available within reasonable periods appropriate to their level of necessity and critical nature.

5.8. Cessation of a CA's operations

The causes that can lead to the cessation of the Certification Authority's activity are as follows:

- Compromise of the CA's private key
- Political decision by the Autonomous Government of Valencia

In the event of cessation of its activity as Certification Services Provider, ACCV shall carry out the following actions with a minimum notice period of two months:

- Inform all the subscribers of its certificates and cancel the validity of these certificates by revoking them.
- Inform all the third parties with which it has signed a certification agreement.
- Notify the Department responsible for Information Society and Electronic Signature matters of the cessation of its activity and of what will happen to the certificates, as well as any other relevant circumstance relating to the cessation of activity.
- Send the Department responsible for Information Society and Electronic Signature matters all the information relating to the revoked electronic certificates so that this Department can see to its safekeeping.

6. Technical Security Controls

6.1. Key pair generation and installation

6.1.1. Key pair generation

Key pairs for all the ACCV's internal bodies are generated on cryptographic hardware modules with FIPS 140-1 Level 4 certification.

Key pairs for end entities are generated in accordance with the stipulations in the applicable Certification Policy.

6.1.2. Delivery of private keys to entities

In cases in which the generation of keys is not carried out via methods under the control of the actual end-entity, it shall be the corresponding Certification Policy that specifies the procedure to be used in order to deliver the private key to the end entities.

6.1.3. Delivery of public keys to the certificate issuer

Public keys generated via methods under the control of end entities are sent to the ACCV as part of a request for certification in PKCS#10 format, digitally signed with the private key corresponding to the public key that is requested to be certified.

6.1.4. Delivery of the CA public key to users

The public keys of all the CAs belonging to the ACCV hierarchy of trust can be downloaded from the website: http://www.accv.es.

6.1.5. Size of the keys

Root CA keys and CAGVA keys are RSA keys with a length of 2048 bits.

The size of the keys for each type of certificate issued by the ACCV is stipulated in the Certification Policy applicable to the relevant certificate. In all cases, their size shall never be less than 1024 bits.

6.1.6. Public key generation parameters

Root CA keys and CAGVA keys are created with the RSA algorithm.

The key generation parameters for each type of certificate issued by the ACCV are defined by the Certification Policy applicable to the relevant certificate.

6.1.7. Verification of the quality of the parameters

The procedures and methods of verification of the quality of the key generation parameters for each type of certificate issued by the ACCV are defined by the Certification Policy applicable to the relevant certificate.

6.1.8. Key generation hardware/software

Keys for PKI entities are generated on cryptographic HSM devices with FIPS 140-1 Level 4 certification.

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

6.1.9. Purposes of key use

The purposes of key use for each type of certificate issued by the ACCV are defined by the Certification Policy applicable to the relevant certificate.

All certificates issued by the ACCV contain the extensions *KEY USAGE and EXTENDED KEY USAGE* defined by the standard X.509 v3 for the definition and limitation of such purposes.

6.2. Private Key Protection

6.2.1. Standards for cryptographic modules

It is compulsory for modules used for the creation of keys used by Root CA GVA and CA GVA and the ACCV's RAs to comply with FIPS140-1 level 4 certification.

6.2.2. Multiperson control of private keys

Private keys used by Root CA GVA and CA GVA are under multiperson control.

All these keys are divided into different fragments and a minimum of two of these fragments is required to be able to reform the key again.

6.2.3. Safekeeping of private keys

Subscribers' private keys for signature are not held for safekeeping. Private keys for encryption can be held for safekeeping in accordance with the provisions of the applicable Certification Policy.

Private keys of the Certification Authorities and Registration Authorities that are part of the ACCV are stored in cryptographic hardware devices with FIPS 140-1 level 4 certification.

The rest of the private keys of entities making up the ACCV are contained on cryptographic smartcards in the possession of the Administrators of each entity.

6.2.4. Backup copies of private keys

Backup copies of the private keys of ACCV bodies are stored in encrypted form in secure fireproof files.

6.2.5. Private key file.

Backup copies of the private keys are held in safekeeping in encrypted form in secure fireproof files.

6.2.6. Entry of the private key on the cryptographic module.

Private keys are created on the cryptographic module at the time of the creation of each of the ACCV entities that use these modules.

6.2.7. Private key activation method.

The private key of both the Root CA and the CAGVA is activated by means of the initialisation of the CA software and the activation of the cryptographic hardware that contains the keys.

6.2.8. Private key deactivation method

An Administrator can deactivate the ACCV Certification Authorities' key by stopping the CA software.

6.2.9. Private key destruction method

The destruction of a token can be carried out for the following reasons:

- Cessation of the use of the keys contained
- Deterioration which does not allow efficient use of the token, but does not totally prevent its use.
- Recovery of a lost or stolen token.

Destruction must always be preceded by revocation of the certificate associated with the token, if this is still in force.

6.2.9.1. Cryptographic hardware

There is no provision for the destruction of an HSM, due to its high cost. Instead, it undergoes the initialisation process. During the transfer from “operational” to “initialisation” status, the keys contained on it are securely deleted.

6.2.9.2. Cryptographic cards

Destruction of the Token can occur when the information printed on it loses its validity and a new card has to be issued.

The task to be carried out consists of **Secure Destruction** of the Token of a physical nature.

6.3. Other aspects of key pair management.

6.3.1. The public key file

ACCV maintains a file of all certificates issued for a period of fifteen (15) years.

6.3.2. Period of use for private and public keys

The Root CA GVA certificate is valid for twenty (20) years. The CAGVA certificate is valid for ten (10) years, and the Registration Authorities certificate (XRAO) and the certificates for the remaining ACCV entities are valid for three (3) years.

The period of validity of end entities’ certificates is stipulated by the Certification Policy applicable in each case, and it shall under no circumstances exceed a maximum of four (4) years of validity.

6.4. Activation data

6.4.1. Generation and activation of activation data

The activation data of the ACCV Certification Authorities is generated and stored on cryptographic smart cards in the possession of authorised personnel.

6.4.2. Protection of activation data

Only authorised personnel know the PINs and passwords for accessing activation data.

6.4.3. Other aspects of the activation data

Not stipulated.

6.5. IT Security Controls

The data relating to this section is considered to be confidential information and is only provided to persons who can provide evidence of their requirement to know it.

6.6. Life Cycle Security Controls.

The data relating to this section is considered to be confidential information and is only provided to persons who can provide evidence of their requirement to know it.

6.7. Network Security Controls

The data relating to this section is considered to be confidential information and is only provided to persons who can provide evidence of their requirement to know it.

6.8. Cryptographic Module Engineering Controls

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

The ACCV only uses cryptographic modules with FIPS 140-1 or ITSEC E3 certification.

7. Certificate profiles and certificate revocation lists

7.1. Certificate Profile

7.1.1. Version number

ACCV supports and uses X.509 version 3 (X.509 v3) certificates.

X.509 is a standard developed by the International Telecommunication Union (international United Nations organisation that coordinates telecommunications networks services between Governments and companies) for Public Key Infrastructures and digital certificates.

7.1.2. Certificate extensions

The extensions used in a generic form on the certificates are as follows:

- Key Usage. Marked as critical.
- Basic Constraint. Marked as critical.
- Certificate Policies. Marked as critical.
- Subject Alternative Name. Marked as not critical.
- CRL Distribution Point. Marked as not critical.

The ACCV Certification Policies can establish overall variations of the extensions used for each type of certificate.

7.1.3. Algorithm object identifiers (OID)

Object Identifiers (OID) of the Cryptographic algorithms:

- md5withRSAEncryption (1.2.840.113549.1.1.4)
- SHA1withRSAEncryption (1.2.840.113549.1.1.5)

7.1.4. Name formats

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

7.1.5. Name restrictions

The names contained on the certificates are restricted to X.500 distinguished names, which are unique and allow for no ambiguity.

7.1.6. Object Identifier (OID) of the Certification Policy

To be defined by each Certification Policy.

ACCV has established a policy for assignment of OIDs within its private numbering range. The

OIDs of all the ACCV's Certification Policies begin with the prefix 1.3.6.1.4.1.8149.3

7.1.7. Use of the "Policy Constraints" extension

Not stipulated

7.1.8. Syntax and semantics of policy qualifiers

Not stipulated

7.1.9. Semantic processing for the critical “Certificate Policy” extension

The “*Certificate Policy*” extension identifies the policy that defines the practices that ACCV explicitly associates with the certificate. In addition, 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 the format specified in version 2 (X509 v2).

7.2.2. CRL and extensions

This Certification Practice Statement supports and uses CRLs compliant with standard X.509.

8. Compliance audit

8.1. Frequency of compliance checks for each entity

An audit shall be carried out on the ACCV at least once a year to guarantee the compliance of its running and operating procedures with the provisions included in this CPS.

Other technical and security audits shall be carried out in accordance with the stipulations of the ACCV's Audit Policy, which include an audit on compliance with personal data protection legislation.

8.2. Identification/qualification of the auditor

The auditor shall be selected at the time that each audit is performed.

Any company or person contracted to perform a security audit on ACCV must fulfil the following requirements:

- Adequate and proven training and experience in PKI, security and audit processes for information systems.
- Independence at an organisational level from the ACCV authority, in the case of external audits.

8.3. Relationship between the auditor and the audited entity

Apart from the audit role, the auditor and the audited party (ACCV) must not have any relationship, whether current or planned, of a financial, legal or any other nature that might lead to a conflict of interests.

In compliance with the stipulations of the regulations in force in our legal code on personal data protection, and in view of the fact that in order for the auditor to comply with the services governed by the contract it is necessary to access the personal data of files owned by the ACCV, the auditor shall be considered the Processor, by virtue of the provisions of Article 12 of Organic Law 15/1999 of 13 December.

8.4. Topics covered by the compliance check

The audit shall determine the compliance of the ACCV services with this CPS and the applicable CPs. It shall also determine the risks of non-fulfilment of compliance with the operating procedures defined by these documents.

The aspects covered by an audit shall include, but shall not be limited to:

- Security policy
- Physical security
- Technological evaluation
- Administration of the CA's services
- Selection of personnel
- CPS and CPs in force
- Contracts
- Privacy policy

8.5. Actions to be taken if a deficiency is found.

The identification of deficiencies in the audit shall give rise to the adoption of corrective measures. The Autonomous Secretariat of Telecommunications and the Information Society, in collaboration with the Auditor, shall be responsible for determining these corrective measures.

In the event of a serious deficiency, the Autonomous Secretariat of Telecommunications and the Information Society may decide on the temporary suspension of the ACCV's operations until the deficiencies are rectified, the revocation of the entity's certificate, personnel changes, etc.

8.6. Communication of results

The auditor shall notify the results of the audit to the Autonomous Secretariat of Telecommunications and the Information Society, in its capacity as ultimate head of the ACCV, the ACCV Security Manager, and the managers of the various areas in which non-conformance is detected.

9. Commercial and legal requirements

9.1. Fees

9.1.1. Fees for certificate issue or renewal

The fees for issue and revocation of each certificate are specified in the Certification Policy applicable to the relevant certificate.

9.1.2. Fees for access to certificates

Access to issued certificates, given their public nature, is free of charge and therefore no fee applies to such access.

9.1.3. Fees for access to status or revocation information

Access to information on the status or revocation of certificates is free of charge and therefore no fee is applied.

9.1.4. Fees for other services such as policies information

No fee shall be applied for the service of providing information on this CPS or the Certification Policies administered by ACCV or for any other additional service which is known of at the time of the drawing up this document.

This provision may be modified by the Certification Policy applicable for each case.

9.1.5. Refund policy

In the event that any Certification Policy specifies a fee applicable to the provision of certification services or revocation by ACCV for the type of certificates that it defines, the Policy in question must specify the corresponding refund policy.

9.2. Financial capacity

9.2.1. Compensation to third parties relying on certificates issued by the ACCV.

The ACCV provides a guarantee of sufficient coverage of civil liability in the form of a bank guarantee issued by Caja de Ahorros de Valencia, Castellón y Alicante, Bancaja, for the amount of Three Million Euros (€3,000,000), which covers the risk of liability for damages that could be caused by the use of certificates issued by this Certification Authority, thereby fulfilling the obligation stipulated in Article 20.2 of Act 59/2003 of 19 December on Electronic Signatures.

9.2.2. Fiduciary relations

ACCV does not perform the role of fiduciary agent or any form of representative of subscribers or of third parties that rely on certificates issued by the ACCV.

9.2.3. Administrative processes

ACCV guarantees the regular performance of audits of established processes and procedures. These audits shall be carried out on both an internal and external basis.

9.3. Confidentiality Policy

9.3.1. Confidential information.

The following is expressly declared to constitute confidential information, which may not be disclosed to third parties, except in cases where legal provisions exist:

- The private keys of the entities that make up the ACCV.
- Subscribers' private keys, which the ACCV holds for safekeeping.
- Any information relating to operations carried out by the ACCV.
- Any information relating to security parameters, audit procedures and control.
- Any information of a personal nature provided to the ACCV during the registration process of certificate subscribers, with the exception of the provisions specified in the applicable Certification Policy and the certification contract.
- Business information supplied by the ACCV's suppliers and other persons, which the ACCV has the legally or conventionally established obligation to keep secret.
- Business and emergency continuity plans.
- Records of transactions, including full records and audit records of transactions.
- All the information classified as "CONFIDENTIAL" or "STRICTLY CONFIDENTIAL"

9.3.2. Non-confidential information

The ACCV shall consider the following to be information for public access:

- Information contained in the Certification Practice Statement approved by the ACCV.
- Information contained in the different Certification Policies approved by the ACCV.
- Issued certificates as well as the information contained in these.
- The Certificate Revocation List (CRL)
- Any information qualified as "PUBLIC".

The ACCV's CPS and CPs shall not include information qualified as confidential in point 9.3.1 of this document.

Access is permitted to information not considered confidential, without prejudice to the right of the ACCV to establish the relevant security controls for the purpose of protecting the authenticity and integrity of documents that store information for public access, and thereby preventing unauthorised persons from being able to add to, modify or delete contents.

9.3.3. Communication of information on revocation/suspension of certificates

Information relating to the revocation or suspension of certificates is provided by means of the CRL on the LDAP directory which acts as the ACCV repository.

This information is also available on the ACCV's OCSP validation server at ocsp.accv.es:80

9.4. Personal data protection

The ACCV has a Privacy Policy, published on the ACCV website, which enables compliance with the provisions stipulated in current personal data protection legislation and which informs readers about the ACCV's personal data protection policy.

9.4.1. Personal data protection plan.

In compliance with the requirements stipulated by the ACCV's specific certificate policies, and in accordance with Article 19 of Act 59/2003 of 19 December on Electronic Signatures, any information of a personal nature provided to the ACCV by the subscribers of its certificates shall be handled in accordance with the terms of "Organic Law 15/1999 of 13 December on Personal Data Protection".

In this respect, it should be noted that there is a file of Electronic Signature Users, for which the Autonomous Secretariat of Telecommunications and the Information Society is responsible, created by virtue of the Order of 8 March 2002, (see Official Gazette of the Autonomous Government of Valencia (DOGV) no. 4221 of 4 April 2002 and correction of errors in DOGV no. 4.304 of 31 July 2002), and modified by means of the Order of 26 May 2004 of the Department of Infrastructure and Transport, by virtue of which files of personal data are created, modified and deleted (DOGV 4.772, of 10 June 2004).

The ACCV has a Security Document, which fulfils the obligation stipulated in Article 8 of Royal Decree 994/1999 of 11 June, approving the Regulations on Security Measures for automated files that contain personal data.

9.4.2. Information considered private.

In accordance with the stipulations of Article 3 of Organic Law 15/1999 of 13 December on Personal Data Protection, any information relating to identified or identifiable individuals is considered to be personal data.

Personal information that must not be included either on certificates or on the certificate status verification system is considered to be personal information of a private nature.

In any case, the following data is considered to be private information:

- Certificate requests, whether approved or refused, and any other personal information obtained for the issue and maintenance of certificates.
- Private keys generated and/or stored by the ACCV.
- Any other information identified as "Private information"

In addition, data received by the Certification Services Provider has the legal consideration of basic level data.

Pursuant to Organic Law 15/99, confidential information is protected from loss, destruction, damage, falsification and illegal or unauthorised processing, in accordance with the requirements stipulated in Royal Decree 994/99 of 11 June, which approves the Regulations on Security Measures for automated files that contain personal data.

Under no circumstances shall the ACCV include the data referred to in Article 7 of Organic Law 15/1999 of 13 December on Personal Data Protection in the electronic certificates that it issues.

9.4.3. Information not considered private.

This information refers to the personal information that is included on certificates and on the aforementioned certificate status verification system, in accordance with section 3.1 of this document.

This information, provided at the time of request for certificates in accordance with the terms provided for in Article 17.2 of Act 59/2003 of 19 December on Electronic Signatures, is included on certificates and on the system of verification of certificate status.

The information is not private in nature, owing to a legal imperative ("public data"), but is only published in the deposit if the subscriber consents to this.

In all cases, the following information is not considered confidential:

a. Issued certificates or certificates in the process of being issued

b. A subscriber's status of being subject to a certificate issued by the ACCV.

c. The first name and surnames of the certificate subscriber, and any other circumstances or personal data of the holder, in the event that they are significant in terms of the purpose of the certificate, in accordance with this document.

d. The e-mail address of the certificate subscriber.

e. The economic limits and uses stated on the certificate.

f. The period of validity of the certificate, and the date of issue of the certificate and the date of expiry.

g. The serial number of the certificate.

h. The different statuses or situations of the certificate and the date of commencement of each one of them, specifically: pending generation and/or delivery, valid, revoked, suspended or expired and the reason that led to the change of status.

i. The certificate revocation lists (CRLs), and any other revocation status information.

j. The information contained in the ACCV Deposit.

9.4.4. Responsibilities.

The ACCV guarantees to comply with its legal obligations as certification services provider, in accordance with Act 59/2003 of 19 December, and by virtue of this, and in accordance with Article 22 of the aforementioned Act, it shall be answerable for any damages that it causes in carrying out its own activity, due to non-compliance with the requirements contained in Article 17 of Act 59/2003 relating to personal data protection.

9.4.5. Provision of consent in the use of personal data.

For the purposes of provision of the service, the ACCV must obtain the consent of the owners of the data that is required to provide the certification services. Consent shall be understood to have been obtained with the signature of the certification contract and the collection of the certificates by the user.

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

The ACCV only may communicate information qualified as confidential or which contains personal data in cases in which this is required by the competent public authority and in cases provided for by law.

In specific terms, the ACCV is obliged to reveal the identity of the signatories when this is requested by judicial authorities in exercising the functions that they have been attributed, and in the rest of the cases provided for in Article 11.2 of the LOPD (Organic Law on Personal Data Protection) where this communication is required.

9.4.7. Other cases of communication of information.

In the privacy policy contemplated at the beginning of section 9.4, the ACCV includes requirements for permitting the direct disclosure of information pertaining to the key holder to the key holder him/herself or to third parties.

9.5. Intellectual property rights

All intellectual property rights, including those referring to certificates and CRLs issued by the ACCV, OIDs, this CPS, the Certification Policies that are applicable to it, and any other document, whether electronic or of any other type, owned by the ACCV, belong to the ACCV.

Private keys and public keys are the property of the user, regardless of the physical medium used to store them.

The subscriber shall retain any right that it may hold on the product trademark or trade name recorded on the certificate.

9.6. Obligations and civil liability

9.6.1. Obligations of the Certification Entity

The Certification Authority of the Community of Valencia is obliged to:

- Carry out its operations in accordance with this CPS.
- Protect its private keys.
- Issue certificates in accordance with the Certification Policies that are applicable to them.
- After receiving a valid certificate request, issue a certificate compliant with the X.509 standard and with the request requirements.
- Issue certificates that conform to the information known at the time of their issue, and that are free of data entry errors.
- Guarantee confidentiality in the generation process of signature creation data and its delivery via a secure procedure to the signatory.
- Use reliable systems and products that are protected against any alteration and which guarantee the technical and cryptographic security of the certification processes which they support.
- Use reliable systems to store recognised certificates which permit verification of a certificate's authenticity and prevent unauthorised persons from altering data, restrict its accessibility in cases or to persons indicated by the signatory and permit the detection of any change that affects these security conditions.
- Publish issued certificates in the ACCV's LDAP directory (ldap.accv.es) without alteration.
- Guarantee that the date and the time at which a certificate was issued or its validity was terminated or suspended can be accurately determined.

- Employ personnel with the qualifications, knowledge and experience required for the provision of the certification services offered and the appropriate security and management procedures in the field of electronic signatures.

- Revoke certificates according to the terms of the *Revocation and Suspension of Certificates* section of this document and publish the revoked certificates in the CRL of the ACCV's LDAP directory (ldap.accv.es) with the frequency stipulated in the point *Frequency of issue of CRLs* of this document.

- Publish this CPS and the applicable CP on the website www.accv.es/cps, guaranteeing access to the current versions as well as to previous versions.

- Promptly notify certificate subscribers by e-mail in the event that the CA proceeds with the revocation or suspension of the certificate, and also inform them of the reason that led to this action.

- Collaborate with the audits led by ACCV to validate the renewal of its own keys.

- Operate in accordance with the applicable legislation, specifically with:

    1. Decree 87/2002 of 30 May of the Valencian Government, which governs the use of the advanced electronic signature in the Autonomous Government of Valencia.

    2. Decree 96/1998 of 6 July of the Valencian Government, which governs the organisation of the IT function, the use of information systems and the record of computerised files within the scope of administration of the Autonomous Government of Valencia.

    3. The Order of 3 December 1999 of the Department of Justice and Public Administration which approves the Technical Regulations on Security Measures for the Approval and Authorisation of Applications and Methods of Automated Processing of Information

    4. Act 59/2003 of 19 December on Electronic Signatures.

    5. The Order of 21 February 2000 which approves the regulations of accreditation of certification service providers and of certification of certain products in an electronic form.

    6. The Directive 1999/93/EC of the European Parliament and Council of 13 December 1999, which establishes a Community framework for electronic signatures.

- Where keys exist, protect them by holding them in safekeeping.

- Guarantee the availability of the CRLs in accordance with the provisions of section 4.9.9 *Frequency of issue of CRLs*, of this CPS.

- In the event of ceasing its activity, it must communicate this with a minimum notice of two months from effective cessation, to the holders of the certificates issued by the ACCV, and to the Ministry of Industry, Tourism and Trade, specifying what will happen to the certificates.

- Comply with the specifications contained in the regulations on Personal Data Protection.

- Keep records of all the information and documentation relating to a recognised certificate and the certification practice statements in force at any time for fifteen years from the time of their issue, so that the signatures carried out with the certificates can be verified.

9.6.2. Obligations of the Registration Authority

The persons that operate in the RAs integrated into the hierarchy of the ACCV – 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 that is applicable for the type of certificate requested on each occasion.
- Exhaustively verify the identity of the persons granted the digital certificate processed by the Operators, for which purpose they will require the physical presence of the requester and the presentation of their current National ID Card (not a photocopy), or a Spanish passport. Non-Spanish users must present a Residence Card/Foreigner's ID Card.
- Neither store nor copy the signature creation data of the person to whom they have provided their services.
- Prior to the issue of a certificate, inform the person requesting their services of the obligations that he/she is taking on, the way that he/she must keep the signature creation data safe, the procedure that he/she must follow to communicate the loss or improper use of data or signature creation and verification devices, the price, the necessary conditions for use of the certificate, its limitations of use and the way in which it guarantees its possible asset liability, and the website where they can consult any information on the ACCV, the CPS and the current and previous CPs, applicable legislation, certifications obtained and the applicable procedures for out-of-court resolution of disputes that might arise due to the exercise of the activity.
- Validate and securely send to the CA to which the RA is subordinated a request for certification duly completed with the information provided by the subscriber and digitally signed, and receive the certificates issued in accordance with that request.
- Store securely and until the time that it is sent to the Certification Authority of the Community of Valencia, the documentation provided by the subscriber and the documentation generated by the RA itself during the process of registration or revocation.
- Draw up the Certification Contract with the subscriber in accordance with the stipulations of the applicable Certification Policy.
- Request the revocation of a certificate when it is aware of or suspects the compromise of a private key.
- Authenticate the requests of end users for the renewal or revocation of their certificates, generate digitally signed renewal or revocation requests and send them to their superior CA.
- In the event of the approval of a certification request, notify the subscriber of the issue of the subscriber's certificate and the method of obtaining it.
- In the event of the refusal of a certification request, notify the requester of this refusal and the reason for the refusal.
- For personal certificates, use the certificate request and processing tools in the presence of the person for whom the request shall be carried out, after having carried out a reliable identification.
- Maintain under its strict control the processing tools for digital certificates and notify the Certification Authority of the Community of Valencia of any malfunction or other eventuality that might not comply with normal expected behaviour.
- Send a signed copy of the certification contract and of revocation requests to the Certification Authority of the Community of Valencia.

- Immediately receive and process revocation requests received with attendance in person, after having carried out a reliable identification based on the National ID Card of the requester, or on the Foreigner's ID Card in the case of non-Spanish requesters.
- Collaborate in any aspects of the operation, audit or control of the User Registration Point that are requested of it by the Certification Authority of the Autonomous Government of Valencia.
- The most general and fullest obligation of confidentiality, during and subsequent to the provision of the Registration Authority service, with regard to the information received by the ACCV and the information and documentation which has materialised as a result of the service.

  In the same respect, not to transmit this information to third parties under any circumstances, without the express, written and prior authorisation of the ACCV, in which case it shall transfer the same confidentiality obligation to the aforementioned third parties.

9.6.3. Obligations of subscribers

The subscribers of the certificates issued under this policy are bound by the following obligations:

- Limit and tailor the use of the certificate to legal purposes in accordance with the uses permitted by the relevant Certification Policy and this CPS.
- Apply the necessary care and methods to guarantee the safekeeping of their private key.
- Immediately request the revocation of a certificate in the event of becoming aware of or suspecting the compromise of the private key corresponding to the public key contained in the certificate. The ways in which this request can be carried out are specified in this document in the section 4.9.3 *Revocation request procedure*.
- Not to use a digital certificate that is no longer effective, due to having been suspended, revoked or due to the certificate's period of validity having expired.
- Provide the Registration Authorities with information that they consider accurate and complete in relation to the data that these Authorities request from them to carry out the Registration process, as well as inform the ACCV managers of any modification of this information.
- Pay the fees resulting from the certification services that they request from the corresponding Registration Authority in relation to the services that are requested.

9.6.4. Obligations of third parties relying on certificates issued by the ACCV

Parties that rely on certificates issued by the ACCV are bound by the following obligations:

- Limit reliance on certificates to the permitted uses of the certificates, in accordance with what is set out in the certificate extensions and the relevant Certification Policy.
- Verify the validity of the certificates at the time of carrying out or verifying any operation based on the certificates.
- Take on their responsibility in the correct verification of digital signatures
- Take on their responsibility in the verification of the validity, revocation or suspension of the certificates on which they rely.
- Have full knowledge of the applicable guarantees and responsibilities in the acceptance and use of certificates on which they rely, and agree to abide by these.

9.6.5. Repository obligations

- Keep all certificates issued by the ACCV accessible for end entities.
- Keep information on revoked certificates accessible for end entities in CRL format.

9.7. Disclaimers of guarantees

The ACCV may refuse all guarantees of service that are not linked to obligations stipulated by Act 59/2003 of 19 December on Electronic Signatures, especially guarantees of adaptation for a specific purpose or guarantees of use of certificates for commercial purposes.

9.8. Limitations of liability

9.8.1. Guarantees and limitations of guarantees

The ACCV shall be answerable for damages that it causes to any person in carrying out its activity, when it fails to fulfil the obligations imposed by Decree 87/2002 of 30 May of the Valencian Government on advanced electronic signatures, and Act 59/2003 of 19 December on Electronic Signatures, or it acts negligently.

The ACCV shall be answerable for damages that are caused to the signatory or to third parties in good faith due to the failure of or delay in the inclusion in the certificate validity consultation service of the expiry or suspension of validity of the certificate issued by the ACCV, once it becomes aware of this.

The ACCV shall accept all liability vis-à-vis third parties for the actions of persons who carry out the necessary functions for provision of the certification service.

The ACCV is the Certification Authority of the Autonomous Government of Valencia. The responsibility of the Administration is founded on objective bases and covers any injury that individuals might suffer, provided that it is the consequence of normal or abnormal operations of the public services.

The ACCV only shall be answerable for damage caused by improper use of the recognised certificate, when it has not recorded on it, in a form clearly recognisable by third parties, the limit with regard to its possible use or the amount of the value of the valid transactions that can be carried out using it. It shall not be answerable if the signatory exceeds the limits recorded on the certificate in relation to its possible uses and the individualised amount of the transactions that can be carried out with it or does not use it in accordance with the stipulated conditions communicated to the signatory by the ACCV.

The ACCV shall also not be answerable if the addressee of the electronically signed documents does not check and take into account the restrictions recorded on the certificate in relation to its possible uses and the individualised amount of the transactions that can be carried out with it.

9.8.2. Limitations of liability

The ACCV Registration Entities shall not accept any liability in the event of loss or damage:

- To the services that they provide, in the event of war, natural disasters or any other case of *force majeure*.
- Caused by the use of certificates which exceeds the limits stipulated by the certificates, the relevant Certification Policy and this CPS.
- Caused by the improper or fraudulent use of the certificates or CRLs issued by the ACCV.
- Caused to the signatory or third parties in good faith if the addressee of the electronically signed documents does not check or take into account the restrictions recorded on the certificate in relation to its possible uses, or if the addressee does not take into account the suspension or loss of validity of the certificate published on the CRL, or if the addressee does not verify the electronic signature.

9.8.3. Loss limitations

With the exception of the stipulations set out in this CPS, ACCV shall accept no other obligation nor offer any other guarantee, and in addition shall accept no other liability vis-à-vis subscribers or relying parties.

9.9. Term and termination.

9.9.1. Term.

In the ACCV's legal instruments with subscribers and verifiers, it stipulates a clause which determines the period of validity of the legal contract by virtue of which it provides certificates to subscribers.

9.9.2. Termination.

In the ACCV's legal instruments with subscribers and verifiers, it stipulates a clause which determines the consequences of the termination of the legal contract by virtue of which it provides certificates to subscribers.

9.9.3. Survival.

In the ACCV's legal instruments with subscribers and verifiers, it stipulates survival clauses, by virtue of which certain regulations continue to be in force after the end of the legal contract governing the service between the parties.

9.10. Notifications.

Any notification, demand, request or any other communication required under the practices described in this CPS shall be carried out via an electronic message or document digitally signed in accordance with the CPS or in writing by means of registered post sent to any of the addresses stated in point *1.5 Contact data*. Electronic communications shall become effective once the addressee to whom they have been sent receives them.

9.11. Modifications.

The ACCV can unilaterally modify this document, abiding by the following procedure:

- The modification must be justified from a technical and legal point of view.

- The modification proposed by the ACCV may not violate the provisions contained in the Certification Policies established by the ACCV.

- A modifications control is set up, based on the ACCV's Change Management Policy.

- The implications that the change of specifications has on the user are established, and the need to notify the user of these modifications is planned.

9.11.1. Change specification procedures

The entity with the powers to carry out and approve changes to the CPS and the ACCV's CPs is the Autonomous Secretariat of Telecommunications and the Information Society, the contact data for which is stated in section 1.5.1. of this CPS.

In cases in which the Autonomous Secretariat of Telecommunications and the Information Society considers that the modification of the CPS does not actually reduce the trust that a Certification Policy or its implementation imparts, or does not alter the acceptability of the certificates supported by the policy for the purposes for which they have been used, the lower number of the version of the document and the last Object identifier (OID) number that represents it will be increased, while maintaining the higher number of the version of the document, as well as the rest of its associated OID. It is not considered necessary to notify these types of modifications to subscribers of the certificates corresponding to the modified CP or CPS.

In the event that the Autonomous Secretariat of Telecommunications and the Information Society deems that the changes to the specification in force affect the acceptability of the certificates for specific purposes, the higher number of the version of the document will be increased and the lower number of the version of the document will be set to zero. The last two numbers of the Object identifier (OID) that represents it shall also be modified. These types of modifications shall be notified to the subscribers of the certificates corresponding to the modified CP or CPS by a notification sent to the e-mail address that the user has provided at the time of issue of the certificate, with a notice period of at least 30 days from its publication. The user may accept the modifications or reject them. If the user rejects them, his/her certificate, issued under the instructions of the previous CPS, shall be valid for the purposes included in it, but not for the specific purposes that are included in the new modified CPS or CP. If, after 15 days have elapsed since notification to user, no response has been received from him/her, it shall be considered that the user has not accepted the modification, although he/she can accept it at any subsequent time.

9.11.2. Publication and notification procedures.

Any modification of this Certification Practice Statement or of the Certification Policies Documents shall be published on the ACCV website: www.accv.es.

In addition, any substantial modification of this CPS shall be announced in the *Diari Oficial de la Generalitat Valenciana (*Official Gazette of the Autonomous Government of Valencia*)* in the form of a Ruling by the Autonomous Secretariat of Telecommunications and the Information Society, in the exercise of the competences that it has been attributed as Certification Authority of the Autonomous Government of Valencia.

9.11.3. Certification Practice Statement Approval Procedures

The Autonomous Secretariat of Telecommunications and the Information Society is the competent entity for granting the approval of this Certification Practice Statement and the Certification Policies associated with each type of certificate.

In addition, the Autonomous Secretariat of Telecommunications and the Information Society shall be responsible for the approval and authorisation of the modifications of these documents.

9.12. Dispute resolution.

9.12.1. Out-of-court dispute resolution.

The ACCV may stipulate in the legal instruments in which its relations with subscribers and verifiers are set out the procedures of mediation, arbitration and dispute resolution that are considered appropriate, all of which shall be without prejudice to the administrative procedure legislation.

9.12.2. Competent jurisdiction.

The disputes that arise in the provision of certification services by the ACCV shall be subject to contentious-administrative jurisdiction, pursuant to the provisions of Act 29/1998 of 13 July governing Contentious-Administrative Jurisdiction.

9.13. Applicable Legislation

The functioning and operations of the ACCV, as well as this CPS are governed by the Community, national and Valencian legislation in force at any time.

The following regulations are explicitly assumed to be applicable:

- Decree 87/2002 of 30 May of the Valencian Government, which governs the use of the advanced Electronic Signature in the Autonomous Government of Valencia.
- Decree 96/1998 of 6 July of the Valencian Government, which governs the organisation of the IT function, the use of information systems and the record of computerised files within the scope of administration of the Autonomous Government of Valencia.
- The Order of 3 December 1999 of the Department of Justice and Public Administration which approves the Technical Regulations on Security Measures for the Approval and Authorisation of Applications and Methods of Automated Processing of Information
- Act 59/2003 of 19 December on Electronic Signatures.
- The Order of 21 February 2000 which approves the regulations of accreditation of certification service providers and of certification of certain products in an electronic form.
- Directive 1999/93/EC of the European Parliament and Council of 13 December 1999, which establishes a community framework for electronic signatures.

9.14. Compliance with applicable law.

The ACCV declares that this CPS complies with the requirements stipulated in Act 59/2003 of 19 December on Electronic Signatures.

9.15. Miscellaneous clauses.

No additional stipulations.