Agencia de Tecnología
y Certificación Electrónica

ACCV Certification Practice Statement (CPS)

Date: 10/09/2023	**Version:** 4.0.12
Estado: APPROVED	**No. of pages:** 76
OID: 1.3.6.1.4.1.8149.2.4.0	**Classification: PUBLIC**
File: ACCV-CPS-V4.0.12-EN-2023.odt	
Prepared by: Agencia de Tecnología y Certificación Electrónica	

Changelog

Version	Author	Date	Observations
4.0.1	ACCV	20/05/2017	No changes.
4.0.2	ACCV	03/09/2018	CAB/Forum modification
4.0.3	ACCV	03/02/2019	Extension OCSP
4.0.4	ACCV	19/07/2019	Corrections RFC3647. Mail modifications.
4.0.5	ACCV	29/07/2019	Serial Number modification
4.0.6	ACCV	15/01/2020	Minor corrections RFC3647. Explicit license.
4.0.7	ACCV	24/02/2020	Minor changes in the Spanish law. Corrections RFC3647
4.0.8	ACCV	20/03/2021	Change the address of the headquarters. Demonstrate Key Compromise
4.0.9	ACCV	20/04/2022	Minor corrections
4.0.11	ACCV	16/04/2023	Review and minor corrections
4.0.12	ACCV	10/09/2023	Adaptation to policy 2.0 CAB/Forum

Table of Contents

1. INTRODUCTION

1.1. Overview

This document contains the mandatory *Certification Practice Statement (CPS)* of Agencia de Tecnología y Certificación Electrónica.

The Agencia de Tecnología y Certificación Electrónica (ACCV) is part the Infraestructures i Serveis de Telecomunicacions i Certificació, SAU (ISTEC), which is a public entity with legal personality and full legal capacity to carry out its purposes, governed by its statutes.

Pursuant to the above and in compliance with the legislation in force and aligned with Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, this Certification Practice Statement (CPS) details the general conditions and regulations of the certification services provided by the Agencia de Tecnología y Certificación Electrónica, in relation to the management of electronic certificates and signature creation and verification data; conditions applicable to the request, issue, use and expiry of the validity of certificates; technical and organizational 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 the activity of Agencia de Tecnología y Certificación Electrónica (ACCV) as Qualified Trust Service Provider. However, the various particularities applicable to each of the different types of issued certificates 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.

Finally, it must be noted that Agencia de Tecnología y Certificación Electrónica (ACCV) is aligned for policies and certificates where applicable with the current versions of the documents "Baseline Requirements for the Issuance and Management of Publicly-Trusted certificates" published at https://www.cabforum.org/. In case of any incompatibility between this document and the requirements of CAB Forum, those requirements will prevail.

1.2. Document name and identification

Name of the document	Certificate Practice Statement (CPS) of ACCV
Document version	4.0.12
Document Status	APPROVED
CPS reference / OID (Object Identifier)	1.3.6.1.4.1.8149.2.4.0
Issue date	2023 September 10th
Expiration date	Not applicable
Location	This CPS can be viewed at http://www.accv.es/pdf-politicas

1.3. PKI participants

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 comprising ACCV.

The Certification Authorities that comprising ACCV are structured in a single hierarchy. This hierarchy is formed by the following certification authorities:

- “ACCVRAIZ1” as first level Root CA. 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 which signature is “ACCVRAIZ1”, and which contains the public key (or signature verification data) of “ACCVRAIZ1” signed with the signature creation data (private key) of “ACCVRAIZ1”. 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:

  9305 7A88 15C6 4FCE 882F FA91 1652 2878 BC53 6417

  With this key, the self-signed certificate of ACCVRAIZ1 is verified, and it is valid from May 5th 2011 until December 31st 2030.

- “ACCVCA-110" as the subordinate Certification Authority of ACCVRAIZ1. Its function is to issue certificates for legal entities. The “ACCVCA-110” certificate is valid from October 13th 2011 until January 1st 2027.

- “ACCVCA-120” as the subordinate Certification Authority of ACCVRAIZ1. Its function is to issue certificates for ACCV subscribers. The “ACCVCA-120” certificate is valid from October 13th 2011 until January 1st 2027.

- “ACCVCA-130” as the subordinate of Certification Authority ACCVRAIZ1. Its function is to issue pseudonym certificates, certificates for the identification of Windows domain users. ACCVCA-130 certificate is valid from October 14th 2011 until January 1st 2027.

1.3.2. Registration authorities

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

Any legal entity can be Registration Authorities provided that the corresponding collaboration agreement has been entered into with ACCV. These Registration Authorities are referred to as User Registration Points or PRUs in the documentation relating to the Agencia de Tecnología y Certificación Electrónica, and they are entrusted with confirmation of the applicant’s identity and delivery of the certificate. The functions of these Registration Authorities, which act on behalf of ACCV, are as follows:

- To verify the identity and any personal circumstances of certificate applicants, 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 qualified certificate.

• To ensure that the signatory is in possession of the signature creation data corresponding to the verification data recorded on the certificate.

All PRUs are under the direct control of the ACCV, using the centralized tools provided by the ACCV for its work.

1.3.3. Subscribers

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 subscriber assumes the responsibility for safekeeping of the signature creation data, without being able to assign its use to any other person under any concept.

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 provided that the possible subscribers are all of the individual or legal entities that can be identified with the mechanisms established in each Certification Policy.

1.3.4. Relying parties

All persons that voluntarily rely on certificates issued by 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 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 any Public Administration or Authority, any enterprise or entity and any citizen can be considered relying parties.

1.3.5. Other participants

1.3.5.1. Applicants

An Applicant 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 case of Certificate Applicant whose Subscriber is a legal person, the aforementioned individual may only be a legal or voluntary representative or administrator with sufficient authority for these purposes of the legal entity that will be the subscriber of the certificate.

1.4. Certificate usage

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

1.4.1. Appropriate certificate uses

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

1.4.2. Prohibited certificate uses

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

1.5. Policy administration

1.5.1. Organization administering the document

Name	*Agencia de Tecnología y Certificación Electrónica*
Email Address	*accv@accv.es*
Address	*Pol. Ademuz, s/n. Floor 5th - 46100 Burjassot (Spain)*
Telephone Number	*+34 963 866 014*

1.5.2. Contact person

Name	*Agencia de Tecnología y Certificación Electrónica*
Email address	*accv@accv.es*
Address	*Pol. Ademuz, s/n. Floor 5th - 46100 Burjassot (Spain)*
Telephone Number	*+34 963 866 014*

The user can provide information about compromised private key or misused certificates using the support form as indicated in the following URL: https://www.accv.es/ayuda/certificates-revocation/how-revoke-certificate/

In the form, the user must paste this key or certificate in PEM format, including the BEGIN and END lines.

1.5.3. Person determining CPS suitability for the policy

The competent entity for determining the suitability of this CPS to the different Certification Policies of ACCV, is Infraestructures i Serveis de Telecomunicacions i Certificació, SA (ISTEC) according to its statutes.

1.5.4. CPS approval procedures

The ISTEC approves the CPS and any amendments. Amendments are made by either updating the entire CPS or by publishing an addendum. ISTEC determines whether an amendment to this CPS requires notice or an OID change.

1.6. Definitions and Acronyms

1.6.1. Definitions

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

- Certification Authority: natural or legal person 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: natural or legal person appointed by ACCV to verify the identity of certificate applicants 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 ACCV as PRUs or User Registration Points.

- Certificate chain: list of certificates from the ACCV root certificate to the end-user 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 ACCV.

- Root certificate: a certificate whose subscriber is a Certification Authority belonging to ACCV hierarchy. This certificate contains the signature verification data of the aforementioned Authority signed with the signature creation data of the Authority as Certification Services Provider.

- Qualified Certificate: Certificate issued by a Trust Services Provider which complies the requirements stipulated in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 regarding verification of applicants' identity and other circumstances and the reliability and guarantees of the certification services provided. To be considered as a qualified certificate, it must appear on the trusted list (TSL) referred to in Article 22(1) of the Regulation.

- Key: sequence of symbols.

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

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

- Certification Practice Statement: One of several documents forming the governance framework in which Certificates are created, issued, managed, and used, made available to the public in electronic form and free of charge by virtue of ACCV's status as Trust 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 in Regulation (EU) No 910/2014 (Annex II Requirements for Qualified Electronic Signature Creation Device).

- 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.

- Records of processing activities: document required by Regulation (EU) 2016/679, which purpose 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 organization that processes personal data on behalf of the data controller.

- Qualified electronic signature: advanced electronic signature based on a qualified certificate and generated by a qualified signature creation device.

- Recognized electronic signature: advanced electronic signature based on a recognized certificate and generated by means of a Secure Signature Creation Device.

- Advanced electronic signature: electronic signature that enables the subscribers personal identity to be established with regard to the signed data and the data integrity 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 fulfills 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).

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

- Certificate Serial Number: unique value that is unmistakably associated with a certificate issued by ACCV.

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

- OCSP Responder: 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): unique sequence of non-negative integer values separated by dots, which can be assigned to registered 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 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, 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 The Secure Hash Algorithms are a family of cryptographic hash functions published by the National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS). The first version of the algorithm was created in 1993 with the name of SHA, although at present it is known as SHA-0 to avoid confusion with later versions. The second version of the system, published under the name of SHA-1, was published two years later. Thereafter SHA-2 was published in 2001 (consisting of several functions: SHA-224, SHA-256, SHA-384, and SHA-512) and the most recent SHA-3, which was selected in a competition for hash functions held by NIST in 2012. The algorithm consists of taking messages of less than 264 bits and generating a summary of fixed length. The probability of finding two different messages producing a single summary is practically zero. For this reason it is used to ensure the integrity of the documents during the Electronic Signature process.

- Time-stamping: recording of the date and time on an electronic document using indelible cryptography 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 (or Applicant): individual who requests the issue of a certificate, after having provided identification.

- Subscriber (or Subject): the holder or signatory of the certificate. The natural or legal 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 standardization.

- Cryptography 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 qualified electronic signatures.

- Relying third parties or relying parties: parties that put their trust in an ACCV certificate, verifying certificate's validity and legitimacy 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	Agencia de Tecnología y Certificación Electrónica
APSC	Área Personal de Servicios de Certificación (Personal Area of Certification Services)
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DGTIC GVA	Dirección General de Tecnologías de la Información y las Comunicaciones Generalitat Valenciana
FIPS	Federal Information Processing Standard
IETF	Internet Engineering Task Force
IVF	Insitut Valencià de Finances
ISTEC	Infraestructures i Serveis de Telecomunicacions i Certificació
OID	Object Identifier
OCSP	Online Certificate Status Protocol
OPRU	Registration Point Operator
PKI	Public Key Infrastructure
PKIGVA	PKI of the Agencia de Tecnología y Certificación Electrónica
PRU	User Registration Point
RA	Registration Authority
RFC	Request For Comment
Sub CA	Subordinate Certification Authority

2. Publication and repository responsibilities

2.1. Repositories

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.

ACCV repository consists:

a high availability LDAP directory service, accessible at: ldap://ldap.accv.es:389.

OCSP responder according to RFC 6960: http://ocsp.accv.es

URL of access to CRLs with high availability:

ACCVRAIZ1: http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1_der.crl

ACCVCA-110: https://www.accv.es/fileadmin/Archivos/certificados/accvca110_der.crl

ACCVCA-120: https://www.accv.es/fileadmin/Archivos/certificados/accvca120_der.crl

ACCVCA-130: https://www.accv.es/fileadmin/Archivos/certificados/accvca130_der.crl

ACCV repository does not contain information of a confidential nature.

ACCV does not use any other repository operated by any organization other than ACCV.

2.2. Publication of certification information

It is the obligation of the CAs belonging to ACCV trust hierarchy 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 ACCV website in PDF format: http://www.accv.es/fileadmin/Archivos/Practicas_de_certificacion/ACCV-CPS-V4.0.12-EN-2023.pdf

ACCV Certification Policies are public and can be found on ACCV website in PDF format: http://www.accv.es/pdf-politicas

ACCV CA certificates are public and can be found in ACCV repository, in X.509 v3 format. It can also be found at http://www.accv.es.

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

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

2.3. Time or frequency of publication

The CPS and Certification Policies are published each time they are modified, carrying out an annual review to verify compliance and adaptation to new directives and technical standards. This revision shall be indicated by changing the minor version number.

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. Access controls on repositories

Read access to ACCV repository information and its website is free. All Audit, CP, CPS documents required are publicly available.

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

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

3. Identification and Authentication

3.1. Naming

3.1.1. Types of names

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

3.1.2. Need for Names to be Meaningful

In all cases, subjectDN and the issuerDN extensions of Certificates must have a meaning. If the Certification Policy applicable to the type of certificate does not indicate otherwise, the applicant's name and Tax ID Code are used. The names in the Certificates identify the subject and issuer respectively.

3.1.3. Anonymity or Pseudonymity of Subscribers

ACCV does not issue pseudonymous Certificates for server authentication, code-signing, or email use. Pseudonymous is used only in client certificates for client authentication where the names in the subject of the Certificate are meaningful only within the scope of the organization which they are issued to be used and are not generally meaningful outside that scope.

The use of pseudonym will be defined in the corresponding certification policy.

3.1.4. Rules for interpretation of name forms

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) and RFC 2253.

3.1.5. Uniqueness of names

Distinguished names must be unique and unambiguous.

As a general rule, for personal certificates, the subscriber's name will be included as part of the common name of the distinguished name, followed by the subscriber's Tax ID Code (or equivalent identifier), in the format "name - NIF Tax ID Code number".

In the case of web identification certificates (SSL), the full name of the server, including the domain and the organization to which it belongs, shall be included in the CN.

In the case of seal certificates, the name or the signing body shall be included, along with the basic identification data (VAT number or equivalent).

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

3.1.6. Recognition, Authentication, and Role of Trademarks

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.

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

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

The Spanish Patent and Trademark Office of the Ministry of Industry, Trade and Tourism has awarded the following trademarks, which are property of ISTEC.

- "Autoritat de Certificació de la Comunitat Valenciana", 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.

- “Agencia de Tecnología y Certificación Electrónica”, trademark no. 2.943.180, requested to Spanish Official Industrial Property on august 13th 2010.

Agencia de Tecnología y Certificación Electrónica

ACCV deliberately prohibits the use of a name whose right of use is not the property of the subscriber. However, the CA is not required to seek evidence of trademark ownership prior to issuing certificates.

3.2. Initial Identity Validation

3.2.1. Method to prove possession of private key

If 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.

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 organization identity

If Certification Policy deems it necessary for an organization's identity to be authenticated, this policy shall determine the necessary methods for verifying the aforementioned identity.

ACCV assumes no commitments in the issuance of certificates about the use of a trademark, not deliberately allowing the use of a name whose right of use is not the property of the subscriber. However, ACCV is not obliged to seek for evidence of the possession of registered trademarks prior the issuance of certificates. In the event of a dispute, ACCV may reject the application or revoke any certificate without any responsibility (see section 3.1.6).

ACCV uses the mechanisms established by the current technical regulations, specifically from Commission Regulation on Execution (EU) 2015/1502 dated 8 September, 2015, on setting specifications and minimum technical procedures for security levels for electronic identification methods as stipulated in article 8, section 3, of the European Parliament and Council Regulation (EU) number 910/2014, on electronic identification and trust services for electronic transactions in the internal market. See corresponding Policy.

3.2.3. Authentication of individual identity

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

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

In cases where the corresponding Certification Policy indicates it, video identification mechanisms may be used to authenticate the identity of an individual, as indicated in the Order ETD/465/2021, of May 6, which regulates the methods of remote identification by video for the issuance of qualified electronic certificates.

As a general rule, if the certificate includes an e-mail address as data, ACCV will send an email to that address with a unique web link. The applicant must click on this link and verify a captcha to confirm the address and thus be able to continue with the generation process.

ACCV uses the mechanisms established by the current technical regulations, specifically from Commission Regulation on Execution (EU) 2015/1502 dated 8 September, 2015, on setting specifications and minimum technical procedures for security levels for electronic identification methods as stipulated in article 8, section 3, of the European Parliament and Council Regulation (EU) number 910/2014, on electronic identification and trust services for electronic transactions on the domestic market. See corresponding Policy.

3.2.4. Non-verified subscriber information

All the information provided is verified.

3.2.5. Validation of authority

The authority of Certificate Applicants to request Certificates on behalf of someone is verified during the validation of the Applicant's identity. As established by law, a specific power of attorney is necessary for this operation.

3.2.6. Criteria for Interoperation

ACCV neither interoperates nor has cross certification with other CAs.

3.3. Identification and authentication for re-key requests

3.3.1. Identification and authentication for routine re-key

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, after a strong identification based on qualified certificates.

- 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 7.6 of Law 6/2020 of 11 November, regulating certain aspects of electronic trust services, 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 for re-key after revocation – Non-compromised key

The identification and authentication policy for certificate renewal following a revocation without key compromise shall be the same as for initial registration. ACCV can implement any digital method that guarantees in a reliable and unequivocal way the applicant identity and the application authentication because of technical questions and detailing every step that it takes.

3.4. Identification and authentication for revocation request

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. Certificate life cycle operational requirements

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 ACCV.

4.1. Certificate Application

4.1.1. Who Can Submit a Certificate Application

A certificate application can be submitted by the subject of the certificate

4.1.2. Enrollment Process and Responsibilities

ACCV Registration Authority that receives the application is responsible for determining that the type of certificate requested is appropriate to the specific characteristics of the applicant, 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 applicants of the specific information that must be supplied beforehand.

4.2. Certificate application processing

The identifier associated with ACCV as a CAA issue and issuewild records is “accv.es”.

4.2.1. Performing identification and authentication functions

The Registration Authority or Entity is responsible for verifying the identity of the applicant, as well as the documentation and the record that the applicant has signed the certification contract.

4.2.2. Approval or rejection of certificate applications

The Registration Authority or Entity is responsible for approval or rejection of certificate applications. In all cases, the registration authority will inform the applicant of the decision, and in the case of rejection, will motivate the same.

Once the application has been completed, the Registration Authority shall send it to ACCV Certification Authority.

ACCV will use this information to decide on new applications.

4.2.3. Time to process certificate applications

As a general rule, the maximum time to process certificate applications is five working days. Each Certification Policy can reduce the time to process the corresponding certificate applications.

4.3. Certificate Issuance

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.

4.3.1. CA actions during certificate issuance

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

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

Certificate issuance directly by the Root CA require at least two individual authorized by the CA (manager, system administrator or security manager) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation.

When ACCV 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 ACCV repository.

4.3.2. Notification to subscriber by the CA of issuance of certificate

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

4.4. Certificate Acceptance

4.4.1. Conduct constituting certificate acceptance

The certificates acceptance by the subscribers 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.

The user must accept the contract prior to the issuance of a Certificate.

4.4.2. Publication of the certificate by the CA

Once the certificate has been accepted by the subscriber and generated, the certificate will be published in ACCV repository and made available to users.

4.4.3. Notification of certificate issuance by the CA to other entities

Certificates with the EKU server authentication are published in the Certificate Transparency Log Server service (CT) following established policies. As of the date of this document, for at least 3 operators, with a minimum of two different operators. There are no more notifications.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber private key and certificate usage

Certificates issued by ACCV are used for communications between citizens and the Administrations. Certificates can also be used by their holders in any other electronic communications with other entities, organizations, 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.

4.5.2. Relying party public key and certificate usage

The relying party undertakes to:

- The uses of the certificates correspond to the scope.

- The provisions of the CPS are fulfilled

- Check certificate status and check the status of the hierarchy chain before establishing trust.

- Not compromise or use the services offered in a malicious manner.

- Accept the validity of the signature according to current regulations.

- Report any anomaly or problem detected using the appropriate channels.

4.6. Certificate renewal

4.6.1. Circumstance for certificate renewal

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 certificate renewal.

4.6.2. Who may request renewal

Any subscriber can ask for their certificate to be renewed. The specific conditions are indicated in the corresponding policy.

4.6.3. Processing certificate renewal requests

Once within the renewal period, users must follow the steps indicated in the notices received. These steps involve online access to the Certification Services Area at www.accv.es, identifying himself/herself with a personal qualified certificate and the generation of a new certificate or pair of certificates, acting as Registration Authority.

4.6.4. Notification of new certificate issuance to subscriber

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

4.6.5. Conduct constituting acceptance of a renewal certificate

The certificates acceptance by the subscribers 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.

The user must accept the contract prior to the issuance of a Certificate.

4.6.6. Publication of the renewal certificate by the CA

Once the certificate has been accepted by the subscriber and generated, the certificate will be published in ACCV repository and made available to users.

4.6.7. Notification of certificate issuance by the CA to other entities

Certificates with the EKU server authentication are published in the Certificate Transparency Log Server service (CT) following established policies. As of the date of this document, for at least 3 operators, with a minimum of two different operators. There are no more notifications.

4.7. Certificate re-key

Certificate rekey require certificate renewal to also be carried out; they cannot be carried out as separate processes.

4.7.1. Circumstance for certificate re-key

Certificate rekey require certificate renewal to also be carried out; they cannot be carried out as separate processes.

4.7.2. Who may request certification of a new public key

Certificate rekey require certificate renewal to also be carried out; they cannot be carried out as separate processes.

ACCV may regenerate CA certificate keys, pursuant to the corresponding generation ceremony document. ACCV may regenerate OCSP and TSA service certificate keys pursuant to internal procedure.

4.7.3. Processing certificate re-keying requests

Certificate rekey require certificate renewal to also be carried out; they cannot be carried out as separate processes.

4.7.4. Notification of new certificate issuance to subscriber

Certificate rekey require certificate renewal to also be carried out; they cannot be carried out as separate processes.

4.7.5. Conduct constituting acceptance of a re-keyed certificate

Certificate rekey require certificate renewal to also be carried out; they cannot be carried out as separate processes.

4.7.6. Publication of the re-keyed certificate by the CA

Certificate rekey require certificate renewal to also be carried out; they cannot be carried out as separate processes.

4.7.7. Notification of certificate issuance by the CA to other entities

Certificate rekey require certificate renewal to also be carried out; they cannot be carried out as separate processes.

4.8. Certificate Modification

No certificate fields modification is allowed. When necessary to modify any information on the certificate, ACCV will revoke the certificate and issue a new one following the established processes.

4.8.1. Circumstance for certificate modification

No certificate fields modification is allowed. When necessary to modify any information on the certificate, ACCV will revoke the certificate and issue a new one following the established processes.

4.8.2. Who may request certificate modification

No certificate fields modification is allowed. When necessary to modify any information on the certificate, ACCV will revoke the certificate and issue a new one following the established processes.

4.8.3. Circumstance for certificate modification

No certificate fields modification is allowed. When necessary to modify any information on the certificate, ACCV will revoke the certificate and issue a new one following the established processes.

4.8.4. Notification of new certificate issuance to subscriber

No certificate fields modification is allowed. When necessary to modify any information on the certificate, ACCV will revoke the certificate and issue a new one following the established processes.

4.8.5. Conduct constituting acceptance of modified certificate

No certificate fields modification is allowed. When necessary to modify any information on the certificate, ACCV will revoke the certificate and issue a new one following the established processes.

4.8.6. Publication of the modified certificate by the CA

No certificate fields modification is allowed. When necessary to modify any information on the certificate, ACCV will revoke the certificate and issue a new one following the established processes.

4.8.7. Notification of certificate issuance by the CA to other entities

No certificate fields modification is allowed. When necessary to modify any information on the certificate, ACCV will revoke the certificate and issue a new one following the established processes.

4.9. Certificate Revocation and Suspension

4.9.1. Circumstances for revocation

4.9.1.1. Reasons for Revoking a Subscriber Certificate

A certificate is revoked in a period not to exceed 24 hours when:

- A valid revocation request is received from the subscriber.
- A valid revocation request is received from an authorized third party, for example a court order.
- 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 key pair generated by a final user proves to be "weak".
- The certificate of a higher RA or CA in the certificate's hierarchy of trust is revoked
- ACCV is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name).
- ACCV is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name.

A certificate must be revoked in a period not exceeding five days, being advisable to revoke in a period not exceeding 24 hours when:

- 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 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.

- ACCV is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed.

4.9.1.2. Reasons for Revoking a Subordinate CA Certificate

A Subordinate CA certificate is revoked when:

- ACCV obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise.
- ACCV obtains evidence that the Certificate was misused.
- ACCV is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this CP or the applicable Certificate Policy or Certification Practice Statement.
- ACCV determines that any of the information appearing in the Certificate is inaccurate or misleading.
- ACCV ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate.
- ACCV's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository.
- Revocation is required by ACCV's Certificate Policy and/or Certification Practice Statement.
- The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties.

The revocation must be made within a period not exceeding 7 days from the request.

4.9.2. Who can Request Revocation

The revocation of a certificate may be requested by the certificate's subscriber or by ACCV, as well as by anyone who knows conclusively that the data associated with the certificate become inaccurate or incorrect.

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. Procedure for Revocation Request

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 after a strong identification process based on a ACCV certificate or a certificate of any other qualified 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.

• After certificate revocation, the certificate subscriber must destroy the private key that corresponds to the certificate and not use the revoked certificate.

In the case of personal certificates there is a request form for certificate revocation on ACCV website at: http://www.accv.es, in the Personal Certification Services Area https://apsc.accv.es/apsc/.

In the case of non personal certificates there is a request form for certificate revocation on ACCV website at: http://www.accv.es, in the Non Personal Certification Services Area https://npsc.accv.es:8450/npsc/.

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

Subscribers, Relying Parties, Application Software Suppliers, and other third parties can report suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates in the URL https://www.accv.es/contacto/. In that URL are the support email and contact telephones.

4.9.4. Revocation Request Grace Period

In the event that a Grace Period is not defined in the Subscriber Agreement, Subscribers are required to request revocation within 24 hours after detecting any problem that invalidates the use of the certificate (the loss or compromise of the Private Key, etc..).

4.9.5. Time Within which CA Must Process 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.

4.9.6. Revocation Checking Requirement for Relying Parties

Revocation checking verification is obligatory for each use of end entity certificates at all times by checking the validity of a digital Certificate against the relevant CRL published or using the OCSP responder.

ACCV makes available to its users several revocation checking services for the certificates it issues (CRL, OCSP, others..). Relying parties must use at least OCSP (preferably) or CRL.

4.9.7. CRL Issuance Frequency

ACCV shall publish a new subCA CRL in its repository at maximum intervals of 5 hours, even if there have been no modifications to the CRL (changes to the status of certificates) during the aforementioned period. The nextUpdate field has a maximum value of 4 days.

ACCV shall publish a new RootCA CRL in its repository at maximum intervals of 6 months, even if there have been no modifications to the CRL (changes to the status of certificates) during the aforementioned period. If a sub is revoked, the CRL will be published in a period not exceeding three hours.

The OCSP is updated prior to the CRL. The most recent information will be the one provided by the OCSP.

The CRL does not contain expired certificates. To inquire about the status of an expired certificate, the valid information will be the one provided by the OCSP.

4.9.8. Maximum Latency for CRLs

The maximum time between the generation of CRLs and posting of the CRLs to the repository is:

- LDAP → it is published immediately

- WEB → a maximum of half an hour

4.9.9. On-line Revocation/Status Checking Availability

ACCV provides an OCSP server for online certificate status verification at: ocsp.accv.es:80 conform to RFC 6960 and RFC 5019.

OCSP responses is signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked.

ACCV provides a service to obtain the status of a certificate beyond its validity period, using its serial number. The access URL to this service is:

https://endor.accv.es/lando/

ACCV maintains the certificate status information indefinitely, guaranteeing this information for at least 15 years.

4.9.10. On-line Revocation Checking Requirements

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 6960.

OCSP supports calls to the service using GET method (in addition to POST method).

For the status of Subscriber Certificates:

- ACCV update information provided via OCSP at least 3 hours.
- OCSP responses from this service have a maximum expiration time of 3 days.

For the status of Subordinate CA Certificates:

- ACCV update information provided via OCSP at least 6 months and within 12 hours after revoking a Subordinate CA Certificate.

If the OCSP responder receives a request for status of a certificate that has not been issued, then the responder respond with a "revoked" status, with reason certificateHold(6) and revocationTime January 1, 1970. ACCV monitor the responder for such requests as part of its security response procedures.

ACCV also provides web services for consultation of the validity status of issued certificates.

4.9.11. Other Forms of Revocation Advertisements Available

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

ACCV provides a service to obtain the status of a certificate beyond its validity period, using its serial number. The access URL to this service is:

https://endor.accv.es/lando/

In case 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.

4.9.12. Special Requirements for re Key Compromise

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

The user can provide the compromised private key using the support form as indicated in the following URL: https://www.accv.es/ayuda/certificates-revocation/how-revoke-certificate/

In the form you must paste this key in PEM format, including the BEGIN and END lines.

4.9.13. Circumstances for suspension

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

ACCV does not permit the suspension of certificates.

4.9.14. Who can Request Suspension

ACCV does not permit the suspension of certificates.

4.9.15. Procedure for Suspension Request

ACCV does not permit the suspension of certificates.

4.9.16. Limits on Suspension Period

ACCV does not permit the suspension of certificates.

4.10. Certificate Status Services

The information related to the verification of the revocation status of the electronic Certificates issued by the ACCV can be consulted through CRLs and/or the Certificate Status Information Service through the OCSP protocol, and are accessible through the following means indicated on our website:

https://www.accv.es/servicios/validacion/

CRL:

CRL ACCVRAIZ1 https://www.accv.es/fileadmin/Archivos/certificados/raizaccv1_der.crl

CRL ACCVCA110 https://www.accv.es/fileadmin/Archivos/certificados/accvca110_der.-crl

CRL ACCVCA120 https://www.accv.es/fileadmin/Archivos/certificados/accvca120_der.-crl

CRL ACCVCA130 https://www.accv.es/fileadmin/Archivos/certificados/accvca130_der.-crl

OCSP: http://ocsp.accv.es

4.10.1. Operational Characteristics

Revoked certificates remain in the CRL until they reach their expiration date.

Once this is reached, they are removed from the List of Revoked Certificates.

OCSP establish an 180 months cutoff, allowing to check the status of the certificate beyond the expiration date.

4.10.2. Service Availability

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

The response time of the OCSP remains lower 1s and the download time of CRL remains lower 10s.

4.10.3. Optional features

There are no access or consultation restrictions for the OCSP or the CRL.

4.11. End of subscription

Subscription is completed with

ACCV CA ceases operation

the expiry or revocation of the subscriber certificate without renewal.

4.12. Key escrow and recovery

4.12.1. Key escrow and recovery policy and practices

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.

In case of some kind of non-personal certificates, ACCV may store those certificates and the cipher, identification or signing keys.

In any case, ACCV will store these cryptography keys and implement additional measures that may be necessary to prevent any undue return of the same. The encryption keys are attested by security algorithms proven

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

4.12.2. Session key encapsulation and recovery policy and practices

Session key recovery is not supported.

5. Facility, management and operational controls

5.1. Physical controls

5.1.1. Site location and construction

The information systems of ACCV are located in Data Processing Centers (DPC) with appropriate levels of protection, external walls of the sites are of solid construction, and surveillance 24 hours a day, 7 days a week. Physical barriers are used to segregate secure areas within DPCs and are constructed so as to extend from real floor to real ceiling to prevent unauthorized entry.

5.1.2. Physical access

ACCV Data Processing Centers have different security perimeters, with different security requirements and authorizations. 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 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. Water exposures

ACCV Data Processing Centers are equipped with flood detectors and alarm systems which are appropriate for the environment

5.1.5. Fire Prevention and Protection

ACCV Data Processing Centers are equipped with automated systems for detecting and extinguishing fires.

5.1.6. Media Storage

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 authorized personnel.

5.1.7. Waste Disposal

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

5.1.8. Off-Site Backup

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

5.2. Procedural Controls

ACCV information systems and services are operated in a secure manner, following per-established procedures.

For security reasons, information relating to procedure controls is considered to be confidential or internal use only and is only explained in summarized form.

5.2.1. Trusted Roles

The roles identified for services control and management are as follows:

a. Manager

b. Systems Administrator

c. User Registration Point (PRU) Administrator

d. Certification Authority Operator

e. PRU Operator

f. Training, Support and Communications Manager

g. Security Manager

h. Auditor

i. Legal Expert

j. Documentation Manager

k. Deployment Support Manager

l. Certification Authority Coordinator

5.2.1.1. Manager

At the head of ACCV's staff and under the control of ISTEC's Board of Directors, he is the person responsible for the economic and financial management and the technical and administrative control of ACCV's activities.

It corresponds to the position of Manager of the entity Infraestructures i Serveis de Telecomunicacions i Certificació, SAU (ISTEC).

5.2.1.2. Systems Administrator

He/she is responsible for operating systems and software products installation and configuration, and maintaining and updating the installed products and programs.

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

He/she must ensure that services are provided with the appropriate level of quality and reliability, in accordance with the critical level of these services.

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

He/she must maintain the inventory of servers and equipment comprising ACCV certification platform group.

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

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

5.2.1.3. PRU Administrator

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

He/she is responsible for administrative tasks relating to PRU Operators' authorizations, confidentiality agreements, etc.

He/she must maintain the inventory of PRUs and equipment used for PRU operations.

In exceptional cases, he/she 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, he/she 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.).

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

5.2.1.4. Security Administrator

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

He/she is the individual responsible for managing the perimeter protection systems and specifically managing firewall rules, according to the security rules and in compliance with the Security Responsible.

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

He/she is responsible for resolving or ensuring the resolution of security incidents that have occurred, eliminating vulnerabilities detected, etc. recording always all the incidences that have occurred and all his/her actions.

He/she is responsible for maintaining updated the documents concerned with security devices and, generally, all its tasks.

He/she will notify the Security Responsible of the incoherence between the Security Policy, the Certification Practices Statement, etc. and the real practices.

He/she will control that companies which provide collocation services operate and maintain correctly the physical security systems of DPCs.

In a coordinated manner with the Security Responsible, he/she must take charge of explaining all security mechanisms to the personnel that should know it, raising awareness among ACCV staff and enforcing standards and security policies.

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

5.2.1.5. Certification Authority Operator

He/she assists the Systems Administrators and PRU Administrators in technical or administrative matters that do not require access to the DPC.

He/she must assist the Training, Support and Communications Manager in any tasks instructed.

He/she must collaborate in accordance with the requests of PRU Administrators, with regard to inventory roles, assistance in the installation of systems comprising the PRUs, documentation preparation, collaboration in the training and support of PRU Operators, etc.

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

He/she 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, he/she is responsible for making the local backup copies. This is the only task that the Certification Authority Operator carries out within the DPC.

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

5.2.1.6. User Registration Point Operator

He/she is responsible for functions relating to the identification of certificate applicants, the processing of digital certificates, the revocation of digital certificates and the unblocking of cryptography cards, all while exclusively using the tools and applications provided by the PRU Administrators, and strictly following the approved procedures.

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

5.2.1.7. Training, Support and Communications Manager

He/she is responsible for the maintenance of content of the website of the Agencia de Tecnología y Certificación Electrónica (www.accv.es).

He/she is entrusted with communication and updating duties in relation to ACCV's website.

He/she is responsible for defining the training plan for end users, Call Center agents and personnel involved directly in the operation and administration of ACCV's certification platform. In addition, he/she 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.

He/she must revise the Call Centre incident and response files on a monthly basis, and revise the Call Center agents' scripts.

He/she 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.

5.2.1.8. Security Manager

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

He/she is the individual responsible for managing the perimeter protection systems and specifically managing firewall rules.

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

He/she is responsible for resolving or ensuring the resolution of security incidents that have occurred, eliminating vulnerabilities detected, etc.

He/she is responsible for management and control of the DPC physical security systems, the access control systems, the air conditioning and power supply systems.

He/she 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.

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

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

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

5.2.1.10. Legal expert

He/she is responsible for the legal aspects of the provision of certification services and the formalization of the provision of these services to other entities, with which a certification agreement has to be set up.

He/she 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.

He/she ensures compliance with the electronic signature legislation currently in force, analyzing 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.

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

5.2.1.11. Documentation Manager

He/she is responsible for maintaining ACCV's electronic documentation repository and hard-copy documentation files.

He/she 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.

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

He/she may receive the collaboration of the Certification Authority Operators in carrying out documentary control or inventory tasks.

He/she must guarantee that any certificate issued is associated with a certification contract drawn up in hard copy.

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

5.2.1.12. Deployment Support Manager

He/she is responsible for maintaining contact with development teams of IT applications of user organizations and entities of 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.

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

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

He/she 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 organizations 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 analyze methods of distribution of certificates, creation of PRUs, etc.

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

5.2.1.13. Certification Authority Coordinator

He/she is responsible for monitoring and controlling the performance of the roles attributed to each job profile described above, and for the distribution of new tasks among the profiles.

He/she 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, he/she is responsible for serving as a link with other departments of the Autonomous Government of Valencia.

He/she is responsible for presenting strategic decisions to the Certification Authority management body and for approving tactical decisions.

He/she advises ACCV personnel on training to be taken, retraining courses, etc. and facilitates the implementation of these courses and training plans.

He/she 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 cryptography hardware devices for key generation and storage. Modification of the configuration parameters of cryptography hardware requires authentication by two authorized persons with sufficient privileges.

5.2.3. Identification and authentication for each role

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

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

5.2.4. Roles requiring separation of duties

No identity is authorized to assume both a System Administrator and a Security Manager role;

No identity is authorized to assume both a System Administrator and an Auditor role;

No identity is authorized to assume both a Security Manager and an Auditor role;

5.3. Personnel controls

This section is taken from ACCV Personnel Security Controls document.

5.3.1. Qualifications, Experience, and Clearance Requirements

ACCV 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 organization'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

Before new personnel begin performing any task or work for ACCV, their identity and trust issues will be verified with official records.

5.3.2. Background check procedures

By means of verification of CVs of personnel.

5.3.3. Training requirements

The personnel of ACCV are subject to a specific training plan for carrying out their role within the organization:

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 ACCV.
4. Basic concepts of PKI.
5. Certification Practice Statement and the relevant Certification Policies.
6. Incident management

ACCV maintains records of such training and ensure that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily.

ACCV documents that each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task.

ACCV requires all Validation Specialists to pass an examination provided by the CA on the information verification requirements outlined in the “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates”.

5.3.4. Retraining Frequency and Requirements

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. Job Rotation Frequency and Sequence

No rotation plan has been defined for the personnel Agencia de Tecnología y Certificación Electrónica in the assignment of its tasks..

5.3.6. Sanctions for Unauthorized Actions

In the event that an unauthorized action is carried out regarding 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 unauthorized 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. Independent Contractor Requirements

The external personnel that is involved in the issuance of certificates receives the necessary technical and legal training to carry out their tasks with due diligence (at least the detailed training on section 5.3.3).

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

5.3.8. Documentation Supplied 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
- Organization 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 discretionary 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 authorizations 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 ACCV, the Security Manager shall proceed to carry out the actions or verification detailed in the following points, either directly or by issuing instructions for this purpose to the appropriate personnel.

5.3.10.1. Access to organization locations

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

- Removal of the access privilege to the main DPC in Nixval
- Removal of the access privilege to the continuity-preproduction DPC in Tissat
- Removal of the access privilege to IT rooms and offices at Pol. Ademuz, s/n. Floor 5th, Burjassot

5.3.10.2. Access to Information Systems

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

- o Removal of user privilege in servers

- Removal of user privilege in 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 ACCV website

5.3.10.4. Issuing information to the rest of the organization

The rest of the organization must be clearly informed of the departure of the individual and of his/her loss of privileges. The intention is to thereby minimize 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 ACCV must also be informed of the departure of the individual and that he/she no longer represents 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 organization must be reviewed. If this requirement does not exist, his/her access permit to the XRAO system must be revoked.

5.4. Audit Logging 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 authorized 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 authorized or unauthorized personnel.
- Backup, file and restoration.
- Changes to system configuration.
- Software and hardware updates.
- System maintenance.
- Changes of personnel

All these records are centralized at several points:

- The incident management system (change management, tracking of non-personal certificates, etc...).
- The centralized log system (centralizes via syslog the events of the core systems)
- The Active Directory log for the organization's LAN.

5.4.2. Frequency of Processing Log

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

5.4.3. Retention Period for Audit Log

ACCV shall retain all the relevant 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. Protection of Audit Log

Each audit log contained in these records is encrypted using the public key of a certificate that is issued for 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 authorization of the System Administrator, the Security Manager and 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 ACCV's Backup Copies Policy.

5.4.6. Audit Collection System (Internal vs. External)

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

5.4.7. Notification to Event-Causing Subject

There is no provision for notification regarding the subject giving rise to the log.

5.4.8. Vulnerability Assessments

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

It is the responsibility of the analysis team coordinators to inform ACCV, via the Security Manager, of any problem preventing the performance of the audits, or the delivery of the resulting documentation. It is 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 ACCV.

5.5. Records archival

5.5.1. Types of Records Archived

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 comprising 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 ACCV

- Authorizations for Access to Information Systems (including User Registration Point Operator authorization).

5.5.2. Retention Period for Archive

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

5.5.3. Protection of Archive

Access to the archive is restricted to authorized personnel.

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

5.5.4. Archive backup procedures

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

One copy is made locally and is stored in a fireproof safe in ACCV main Data Processing Center.

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

5.5.5. Requirements for the time-stamping of records

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

5.5.6. Archive collection system (internal v. external)

The information collection system is an internal ACCV system.

5.5.7. Procedures for obtaining and verifying archived information

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

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

5.6. Key changeover

ACCV CA's private signing key is changed periodically. ACCV will stop issuing certificates associated and will proceed to sign or issue new certificates from the corresponding Certification Authority before the end of the validity period is reached, in accordance with the provisions of section 6.3.2. The prior key will continue to sign and publish CRLs until the end of its useful life. The key change or the issuance of a new certificate for the signing of the subscriber certificates will be carried out in such a way that the impact on the subscribers and trusted parties is minimal. All affected entities will be notified prior to a planned key change.

5.7. Compromise and disaster recovery

5.7.1. Incident and Compromise Handling Procedures

The Incident Response Plan and the Disaster Recovery Plan describe all the actions carried out and the material and human resources to solve a specific incident.

These documents detail the actions to:

Notify users, evaluate the incident, activate safeguards

At this point, if necessary, the different actors of the WedPKI ecosystem will be notified using the available and commonly used tools (Bugzilla, distribution lists, etc.) as stipulated in the different recognition policies.

Recover affected services to provide adequate levels

Restore regular operations and processes to normal levels

In the event of the unavailability of the installations of the Certification Authority for a period greater than six hours, ACCV's Incident Response Plan and a Disaster Recovery Plan shall be activated.

The Disaster Recovery 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.

ACCV annually test, review, and update these procedures.

5.7.2. Computing Resources, Software, and/or Data are Corrupted

If hardware, software and/or data resources are altered or are suspected of having been altered, the operation of 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 re-certification shall take place.

All these actions are included in the incident response plan.

5.7.3. Entity Private Key Compromise Procedures

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

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

The entities comprising ACCV that are dependent on the renewed entity shall be informed about the fact and ordered to request their re-certification due to the entity having been renewed.

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 re-certified.

5.7.4. Business continuity capabilities after a disaster

In the event of a natural disaster affecting the installations of ACCV's main Data Processing Center 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 the Plan activation, and the remaining essential services shall be available within reasonable and appropriate periods to their level of necessity and critical nature.

5.8. CA or RA termination

The causes that can lead to the termination of the Certification Authority operations are as follows:

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

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

- To duly inform about their intentions to terminate their activity to all the subscribers of their certificates, as well as to third parties with whom it has signed a contract / agreement or who may be affected.

- To finalize any contract / agreement that allows acting on your behalf in the procedure of issuing certificates.

- With the consent of the subscribers, transfer to another Qualified Trust Service Provider those certificates that remain valid on the effective date of cessation of activity. If this transfer is not accepted or not possible, the certificates will be revoked.

- To communicate to the Ministry that at that moment it has the competences in the matter, the cessation of its activity and the destination that it will give to the certificates, as well as any other relevant circumstance related to the cessation of activity.

- To send to the Ministry competent in the matter all the information related to the revoked certificates so that the latter takes care of their custody to the pertinent effects.

6. Technical Security Controls

6.1. Key pair generation and installation

6.1.1. Key pair generation

6.1.1.1. CA Key Pair Generation

Following this procedure, ACCV will prepare and follow a Key Generation Script, have a Qualified Auditor witness the CA Key Pair generation process, and have a Qualified Auditor issue a report opining that the CA followed its key ceremony during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair.

This procedure describes the following:

- roles participating in the ceremony;
- functions to be performed by every role and in which phases;
- responsibilities during and after the ceremony; and
- requirements of evidence to be collected of the ceremony.

The procedure of issuing, signing and distributing of new CA Certificate, specifying that before the expiration of the Certificate a new one is generated, thus avoiding possible interruptions in the operations from any entity that can trust the Certificate.

For reasons of security and quality, the Keys that ACCV needs to carry out its activities as a Trust Service Provider will be generated by the Entity itself inside its own infrastructures, in a physically secure environment and by at least two authorised persons.

Key pairs for all ACCV internal components are generated on cryptography hardware modules with FIPS 140-1 Level 4 certification. In the case of components of CA type, there is audited documentation of the creation ceremony, which includes the steps followed, the personnel involved and the distribution of the activation mechanisms. All these steps are carried out and recorded in the presence of a qualified auditor and in a secured environment.

Key algorithms and lengths employed are based on standards that are broadly recognised for the purpose for which they are generated.

The technical components necessary to create Keys are designed so that a Key is only generated once and so that a Private Key cannot be calculated using its Public Key.

6.1.1.2. RA Key Pair Generation

Not stipulated

6.1.1.3. Subscribers Key Pair Generation

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

6.1.2. Private Key Delivery to Subscriber

In cases when keys generation 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. Public Key Delivery to Certificate Issuer

Public keys generated via methods under the control of end entities are sent to 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.

If it is detected that the public key in the request does not meet the requirements (weak key, etc..) it will be rejected.

6.1.4. CA Public Key Delivery to Relying Parties

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

6.1.5. Key sizes

The keys for ACCVRAIZ1 and the CAs in the same hierarchy are RSA keys with a length of 4096 bits

The key sizes for each certificate type issued by ACCV are defined in the related Certification Policy. In every case, key sizes will never be less than 2048 bits.

6.1.6. Public key parameters generation and quality checking

The keys for ACCVRAIZ1 and the CAs in the same hierarchy are created with RSA algorithm.

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

Parameters defined at ETSI TS 119 312 “Electronic Signatures and Infrastructures (ESI); Cryptographic Suites” document, are used (6 - Signature schemes).

The padding scheme used is emsa-pkcs1-v2.1 (according to RFC 3447 section 9.2).

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

6.1.7. Key Usage Purposes (as per X.509 v3 key usage field)

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

All subscribers certificates issued by 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.

Private Keys corresponding to Root Certificates is not used to sign Certificates except in the following cases:

Self-signed Certificates to represent the Root CA itself

Certificates for SubCAs, and, if the case arises, Cross Certificates.

Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates)

Certificates for OCSP Response verification and Time Stamping service.

6.1.8. Key generation hardware/software

Keys for CA entities are generated on cryptography HSM devices with FIPS 140-1 Level 4 certificaion.

The key generation devices used are:

- Thales Nshield 500e F2, with EAL-4+ and FIPS 140-2 Level3 certifications

- AEP Keyper Enterprise Model 9720, with FIPS-140-2 Level4 certification

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

6.2. Private key protection and Cryptographic Module Engineering Controls

ACCV shall protect its Private Key(s) in accordance with the provisions of this CPS and in a compliance with CA/Browser Forum's Baseline Requirements

6.2.1. Cryptographic module standards and controls

It is compulsory for modules used for the creation of keys used by every CAs integrated in the trust hierarchies comply with an appropriated security certification for its functionality and the security that it requires.

A hardware security module (HSM) is a security device that generates and protects cryptographic keys. Such products must therefore meet at least with FIPS 140-2 Level 3 criteria, or Common Criteria EAL 4+ for the corresponding protection profile. ACCV holds procedures and policies to check that an HSM has not been manipulated during transport and storage

Cryptographic devices with qualified electronic signature certificates, suitable as qualified signature creation devices (DSCF), meet the requirements of security level CC EAL4+, although certifications complying with a minimum of ITSEC E3 or FIPS 140-2 Level 2 security criteria or equivalent are also acceptable. The European reference standard for subscriber devices used is Commission Implementing Decision (EU) 2016/650 dated 25 April, 2016.

6.2.2. Private Key (n out of m) Multi-Person Control

Private keys used by the CAs than conform the trust hierarchy are under multi-person control.

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

Not applicable in the case of subscriber's private keys.

6.2.3. Private key escrow

In no case subscriber’s private keys for signature are 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 ACCV are stored in cryptography hardware devices with FIPS 140-2 level 3 certification.

The rest of the private keys of entities comprising ACCV are contained on cryptography smartcards in the possession of the Administrators of each entity.

6.2.4. Private key backup

There are no backup of the private keys of ACCV entities, instead there is a procedure for activation of backup cryptographic module keys of the CA (root or subordinate) which can be applied in the case of contingency.

All private keys are under the exclusive control of the ACCV

6.2.5. Private key archival

Backup copies of the expired private keys of ACCV entities are held in safekeeping in encrypted form in secure fireproof lockbox, accessible only by authorized personnel with at least dual access.

All private keys are under the exclusive control of the ACCV.

6.2.6. Private key transfer into or from a cryptography module

Private keys are created on the cryptography module at the time of the creation of each ACCV entity that use these modules, fulfilling the requirements defined in section 6.2.1.

6.2.7. Private key storage on cryptography module

Private keys are created on the cryptography module at the time of the creation of each ACCV entity that use these modules, fulfilling the requirements defined in section 6.2.1.

6.2.8. Method of Activating Private Key

The private keys of each of the CAs that conform trust hierarchies are activated by means of the initialization of the CA software and the activation of the cryptography hardware that contains the keys

6.2.9. Method of Deactivating Private Key

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

6.2.10. Method of Destroying Private Key

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

- Cessation of the use of the contained keys.
- 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.

6.2.10.1. Cryptography hardware

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

6.2.10.2. Cryptography smartcards

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.

6.2.11. Cryptographic Module Rating

See section 6.2.1 of this CPS.

6.3. Other aspects of key pair management.

6.3.1. Public Key Archival

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

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

ACCVRAIZ1 certificate is valid until December 31st of 2030 and the CAs certificates integrated in its hierarchy have a validity of 4 years less than the root CA. 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 five (5) years of validity

6.4. Activation data

6.4.1. Activation Data Generation and Installation

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

6.4.2. Activation Data Protection

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

6.4.3. Other aspects of activation data

There are NOT other aspects to consider.

6.5. Computer Security Controls

6.5.1. Specific computer security technical requirements

ACCV implements an Information Security Management System (ISMS) based in standard **ISO-27001** and establishes controls and procedures for its correct compliance.

- Operational controls
    - User procedures documented
    - Safe delete procedures for storage and removable media, so obsolete equipment.
    - Contingency and Continuity plans
    - Antivirus and Antimalware
    - Strict policy on which types of software users may install
- Security data exchanges
    - Transmission with CA and RA
    - Transmission with CA and RA Databases
    - User data
- Access control
    - Dual factor based authentication for CA and RA operators
    - Use the principle of least privilege
    - Unique and nominal user IDs
    - Periodic audits of the privileges applied
    - Strict provisioning procedures
    - Enforcement guides for passwords and security tokens.

ACCV has a security policy and procedures to guarantee security.

6.5.2. Computer security rating

ACCV implements an Information Security Management System (ISMS) based in standard **ISO-27001** and establishes controls and procedures for its correct compliance.

During the continuous evaluation of the ISMS, impact and risk analysis are carried out that assess the computer security.

6.6. Lifecycle Technical Controls

6.6.1. System development controls

ACCV implements an Information Security Management System (ISMS) based in standard **ISO-27001** and establishes controls and procedures for its correct compliance.

There are several procedures and guidelines from ACCV associated with development control:

- Development and Testing Policy
- ACCV Development Best Practices Guidelines
- Change Control Procedure
- Capacity Management
- Business Continuity Plan

All these procedures have the corresponding documentary support in the ACCV document manager.

The characteristics of the ACCV development system:

Continuous integration process

Tools to analyze and detect anomalies in the code

Strict separation between the development and test platform and the working platform

The test and real data are independent

Test and development never work with real data

The production process is carried out after an exhaustive approval process, following the change control procedure, always warranting the roll-back.

6.6.2. Security management controls

ACCV implements an Information Security Management System (ISMS) based in standard **ISO-27001** and establishes controls and procedures for its correct compliance.

There are several procedures and guidelines from ACCV associated with security control:

- Staff Security Functions and Controls
- Asset Inventory
- Procedure for the safe use of devices and media
- Business Continuity Plan
- Change Control Procedure
- Incident Management Procedure
- Vulnerability Management Procedure

All these procedures have the corresponding documentary support in the ACCV document manager.

Certificate subscribers can contact the ACCV to report any incident using the channels specified in:

https://www.accv.es/contacto/

ACCV keeps a detailed record of all incidents, as well as the solutions implemented in its resolution, as specified in the ISMS.

6.6.3. Life cycle security controls

ACCV performs security and vulnerability tests periodically in the different phases of the software life cycle (SDL).

- Threat modeling to avoid errors in the design phase

- Automatic code review tools to detect bugs, vulnerabilities and code smells (Sonarqube)

- Vulnerability scanning and penetration testing.

6.7. Network Security Controls

ACCV protects physical access to network management devices and has an architecture that distribute the traffic based on its security characteristics, creating clearly-defined network sections. These sections are divided by multi-level zoning, using multiple redundant firewalls. Confidential information transferred via insecure networks is encrypted using SSL protocols.

6.8. Time-Stamping

ACCV operates a qualified Time Stamping Authority (TSA).

The rules and procedures that regulate the TSA can be found in their respective policy on https://www.accv.es/quienes-somos/practicas-y-politicas-de-certificacion/politicas-de-certificacion/. The anonymous access URL is in:

http://tss.accv.es:8318/tsa

7. Certificate, CRL, and OCSP profiles

7.1. Certificate Profile

ACCV generates serial numbers with 127 bits of entropy. The core application forces this behavior. Implements a singleton serial number generator using SecureRandom. This generator generates random 16 octec (128 bits) serial numbers.

7.1.1. Version Number(s)

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 organization that coordinates telecommunications networks services between Governments and companies) for Public Key Infrastructures and digital certificates

7.1.2. Certificate extensions; application of RFC 5280

Certificate extensions, their criticality, and cryptographic algorithm object identifiers, are provisioned according to the IETF RFC 5280 standards and comply with CAB Forum Baseline Requirements.

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

- Key Usage. Marked as critical in all cases.

  Root CA and SubCA: KeyCertSign CRLSign

  Subscriber: Established in the associated certification policy

- Basic Constraint.

  RootCA and SubCA

  Present and marked as critical.

  CA field TRUE

  Subscriber: Not present

- Certificate Policies. Present in all cases and marked as not critical.
- Subject Alternative Name. Present in all cases and marked as not critical.
- CRL Distribution Point. Present in all cases and marked as not critical.
- extkeyUsage

  RootCA and SubCA: Not present

  Subscriber: Established in the associated certification policy.

- authorityInformatioAccess: Present in all cases and marked as not critical.
- nameConstraints: Not present.

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

In all cases the specifications and limits established in RFC-5280 will be met.

7.1.3. Algorithm object identifiers

Object Identifiers (OID) of the Cryptography algorithms:

- SHA1withRSAEncryption (1.2.840.113549.1.1.5)
- SHA256withRSAEncryption (1.2.840.113549.1.1.11)
- rsaEncryption (1.2.840.113549.1.1.1)

Effective 16 January 2015, ACCV doesn´t issue Subscriber Certificates utilizing the SHA-1 algorithm with an Expiry Date greater than 1 January 2017.

ACCV indicates the RSA key with rsaEncryption (OID: 1.2.840.113549.1.1.1) algorithm identifier. The parameter is present, and is an explicit NULL.

The AlgorithmIdentifier for RSA keys is byte-for-byte identical with the following hex-encoded bytes: **300d06092a864886f70d0101010500**.

7.1.4. Name Forms

Subject and Issuer Names for all possible certification paths are byte-for-byte identical.

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

In the case of RootCA or SubCAs

Issuer name: cn=ACCVRAIZ1, ou=PKIACCV o=ACCV, c=ES

Subject:

commonName (required). It must match the name of ACCV entity, such that the certificate's Name is unique across all certificates issued by the issuing certificate.

OrganizationalUnit (required) fixed string “PKIACCV”

Organization (required) fixed string “ACCV”

country (required) Country code ISO 3166-1

ACCV Certification Policies establish the overall variations of the name forms used for each type of certificate.

7.1.4.1. Name encoding

Rules applied when encoding a Name:

- Each Name contains an RDNSequence.
- Each RelativeDistinguishedName contains exactly one AttributeTypeAndValue.
- Each RelativeDistinguishedName, if present, is encoded within the RDNSequence in the order that it appears in Section 7.1.2. of the Certificate Policy.
- Each Name does not contain more than one instance of a given AttributeTypeAndValue across all RelativeDistinguishedNames.

7.1.5. Name constraints

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

There are not name constraints defined in SubCA certificates.

7.1.6. Certificate Policy Object Identifier

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 ACCV's Certification Policies begin with the prefix 1.3.6.1.4.1.8149.3

In the case of RootCA and SubCA have as policy any policy.

7.1.7. Usage of Policy Constraints Extension

To be defined by each Certification Policy.

7.1.8. Policy Qualifiers Syntax and Semantics

To be defined by each Certification Policy.

7.1.9. Processing Semantics for the Critical Certificate Policies 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(s)

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

The serial number of the revoked certificates will be listed in the CRL until they achieve its expiration date.

7.2.2. CRL and CRL Entry Extensions

This Certification Practice Statement supports and uses CRLs compliant with standard X.509 and support the following fields:

Version: Set to v2

Signature Algorithm: Identifier of the algorithm used to sign the CRL

Hash Algorithm: Identifier of the algorithm used to hash the CRL

Issuer: The distinguished name of the Issuing CA

This update: Time of CRL issue

Next update: Time of the next CRL update

CRL Number: Sequential CRL number

Issuer Key Identifier: CA issuer fingerprint

Revoked certificates: List of revoked certificates.

reasonCode (OID 2.5.29.21)

If present, this extension is not marked critical.

If a CRL entry is for a Root CA or Subordinate CA Certificate this CRL entry extension is present. In subscriber certificates its CRL entry extension is omitted when the CRLReason indicated is unspecified (0).

ACCV will do everything possible to the CRLReason indicate the most appropriate reason for revocation of the Certificate.

Only the following CRLReasons can be present in the CRL reasonCode extension for Subscriber Certifificates:

- keyCompromise (RFC 5280 CRLReason #1): Indicates that it is known or suspected that the Subscriber's Private Key has been compromised.
- affiliationChanged (RFC 5280 CRLReason #3): Indicates that the Subject's name or other Subject Identity Information in the Certificate has changed, but there is no cause to suspect that the Certificate's Private Key has been compromised.
- superseded (RFC 5280 CRLReason #4): Indicates that the Certificate is being replaced because: the Subscriber has requested a new Certificate.
- cessationOfOperation (RFC 5280 CRLReason #5): Indicates that the website with the Certificate is shut down prior to the expiration of the Certificate, or if the Subscriber no longer owns or controls the Domain Name in the Certificate prior to the expiration of the Certificate.
- privilegeWithdrawn (RFC 5280 CRLReason #9): Indicates that there has been a subscriber-side infraction that has not resulted in keyCompromise, such as the Certificate Subscriber provided misleading information in their Certificate Request or has not upheld their material obligations under the Subscriber Agreement or Terms of Use.

ACCV inform Subscribers about the revocation reason options listed above and provide explanation about when to choose each option. Tools that ACCV provides to the Subscriber allow for these options to be easily specified when the Subscriber requests revocation of their Certificate, with the default value being that no revocation reason is provided.

The privilegeWithdrawn reasonCode is not available to the Subscriber as a revocation reason option, because the use of this reasonCode is determined by the CA and not the Subscriber.

7.3. OCSP profile

ACCV also publishes Certificate status information using Online Certificate Status Protocol (OCSP). This OCSP service works according to the standard defined in RFC 6960 and RFC 5019.

Concretely it is guaranteed that if the OCSP responder receives a request for status of a certificate that has not been issued, not respond with a "good" status. The response must be "revoked", with specify the revocation reason certificateHold (6), and must specify the revocationTime January 1, 1970.

If OCSP response is based on a CRL entry, the revocation reason code for the response will be the same as that obtained from the CRL.

ACCV operates an OCSP service at http://ocsp.accv.es, 24x7.

7.3.1. Version number(s)

OCSP service works according to the standard defined in RFC 6960 and RFC 5019.

7.3.2. OCSP Extensions

The ACCV OCSP supports the extensions:

- NONCE (optional)
- Archive Cutoff
- Extended Revoked Definition

The singleExtensions of ACCV's OCSP responses does not contain the reasonCode (OID 2.5.29.21) CRL entry extension.

8. Compliance audit and other assessments

ACCV carries out the necessary controls to ensure that:

- Issue Certificates and operate the services in accordance with all law applicable to its business
- Meets the technical requirements set
- Complies with the audit requirements set forth in this section

8.1. Frequency or Circumstances of Assessment

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

Certificates capable of issuing new certificates and all their operations fall within the scope of the audit, these operations are divided into an unbroken sequence of audit periods. An audit period must not exceed one year in duration.

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

If ACCV does not have a valid Audit Report indicating compliance with one of the audit schemes listed in Section 8.4, then, before issuing Publicly-Trusted Certificates, we will successfully complete a point-in-time readiness assessment performed in accordance with applicable standards under one of the audit schemes listed in Section 8.4. The point-in-time readiness assessment will be completed no earlier than twelve (12) months prior to issuing Publicly-Trusted Certificates and will be followed by a complete audit under such scheme within ninety (90) days of issuing the first Publicly-Trusted Certificate.

8.2. Identification/qualification of Assessor

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

The CA's audit shall be performed by a Qualified Auditor. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills:

- Independence from the subject of the audit;
- The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme (see Section 8.4);
- Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
- For audits conducted in accordance with the WebTrust standard: licensed by WebTrust;
- Bound by law, government regulation, or professional code of ethics; and
- Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage

8.3. Assessor's Relationship to Assessed 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 ACCV, the auditor shall be considered the Processor, by virtue of the provisions of Article 4.8 of Regulation (EU) 2016/679 of 27 April 2016.

8.4. Topics Covered by Assessment

The audit shall determine the compliance of ACCV services with this CPS and the applicable CPs. It shall also determine the risks of non-fulfillment 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

ACCV carries out at least one annual audit under these schemes:

- "WebTrust for CAs v2.1 or newer" and "WebTrust for CAs SSL Baseline with Network Security v2.3 or newer".

- Regulation (EU) No. 910/2014 of the European Parliament and of the Council of July 23, 2014 (eIDAS)

In addition to the necessary audits established by the legislation in force and by the technical norms of application for the fulfillment of its functions.

ACCV incorporate periodic monitoring and/or accountability procedures to ensure that its audits continue to be conducted in accordance with the requirements of the scheme.

Audits will be conducted by a Qualified Auditor, as specified in Section 8.2.

8.5. Actions Taken as a Result of Deficiency

The identification of deficiencies in the audit shall give rise to the adoption of corrective measures. ACCV, in collaboration with the Auditor, shall be responsible for determining these corrective measures.

In the event of a serious deficiency, ISTEC may decide on the temporary suspension of 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 ACCV Security Manager, and the managers of the various areas in which non-conformance is detected. The Audit Report shall state explicitly that it covers the relevant systems and processes used in the issuance of all Certificates that assert one or more of the policy identifiers listed in Section 7.1.6.1.

The Audit Report must contain at least the following clearly-labelled information:

- name of the organization being audited;
- name and address of the organization performing the audit;
- the SHA-256 fingerprint of all Roots and Subordinate CA Certificates, including Cross Certificates, that were in-scope of the audit;
- audit criteria, with version number(s), that were used to audit each of the certificates (and associated keys);
- a list of the CA policy documents, with version numbers, referenced during the audit;
- whether the audit assessed a period of time or a point in time;
- the start date and end date of the Audit Period, for those that cover a period of time;
- the point in time date, for those that are for a point in time;
- the date the report was issued, which will necessarily be after the end date or point in time date.

An authoritative English language version of the publicly available audit information must be provided by the Qualified Auditor and ACCV will keep public and accessible audit reports, ensuring that no more than three months will pass from the end of the previous audit period.

The Audit Report must be available as a PDF, and shall be text searchable for all information required. Each SHA-256 fingerprint within the Audit Report must be uppercase letters and must not contain colons, spaces, or line feeds.

8.7. Self-Audits

ACCV constantly monitors compliance with procedures and policies, establishing periodic controls of relevant indicators and performing self-audits. In the case of non-personal website and electronic headquarters certificates, at least quarterly on a randomly selected sample of three percent of the Certificates issued during the period immediately following the previous self-audit sample.

9. Other business and legal matters

9.1. Fees

9.1.1. Certificate Issuance or Renewal Fees

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

9.1.2. Certificate Access Fees

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

9.1.3. Revocation or Status Information Access Fees

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

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 Responsibility

9.2.1. Insurance Coverage

ACCV provides a guarantee of sufficient coverage of civil liability being a public agency and liable as such for damages, as set forth in article 9, section 3, subsection b) of law 6/2020 of 11 November, regulating certain aspects of electronic trust services, which covers the risk of liability for damages that could be caused by the use of certificates issued by this Certification Authority.

9.2.2. Other assets

No other assets to consider.

9.2.3. Insurance or warranty coverage for end-entities

ACCV provides a guarantee of sufficient coverage of civil liability being a public agency and liable as such for damages, as set forth in article 9, section 3, subsection b) of law 6/2020 of 11 November, regulating certain aspects of electronic trust services, which covers the risk of liability for damages that could be caused by the use of certificates issued by this Certification Authority.

9.3. Confidentiality of Business Information

9.3.1. Scope of 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 comprising ACCV.
- Subscribers' private keys, which ACCV holds for safekeeping.
- Any information relating to operations carried out by ACCV.
- Any information relating to security parameters, audit procedures and control.
- Any information of a personal nature provided to 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 ACCV's suppliers and other persons, which 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. Information Not Within the Scope of Confidential Information

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

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

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

Information that is not considered as confidential access is permitted, without prejudice to the right of 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 unauthorized persons from being able to add to, modify or delete contents.

9.3.3. Responsibility to protect the confidential information

ACCV is responsible of the protection of the confidential information generated or communicated during all operations.

For end entities, the certificate subscribers are responsible to protect their own private key and all activation information needed to access or use the private key.

ACCV shall be entitled to disclose confidential information to the extent required by law. Specifically, records that certify the trustworthiness of the information included on the certificate will be disclosed if required as evidence in judicial proceedings. In these cases, the consent of the certificate subscriber is not required.

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

This information is also available on ACCV's OCSP validation server at ocsp.accv.es:80 and in the validation service https://endor.accv.es/lando/

9.4. Privacy of Personal Information

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

9.4.1. Privacy Plan

In compliance with the requirements stipulated in each of the Certification Policies and according with Article 5 of Regulation (EU) 910/2014 (eIDAS), any information of a personal nature provided to ACCV by the subscribers of its certificates shall be handled in accordance with the terms of "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data" and "Organic Law 3/2018 of 5 December on the Protection of Personal Data and the Guarantee of Digital Rights".

In that way, ACCV is responsible of the file 'Electronic Signature Users' in front of Spanish Agency of Data Protection. That file was created and lately modified by the following acts:

- Order of March 8, 2002 of the Conselleria de Innovación y Competitividad, by virtue of which computerized files with personal nature data are created (vid. DOGV nº 4.221de on 4 April 2002 and errors correction in the DOGV nº 4.304, of 31st July 2002)
- Order of May 26, 2004 of the Department of Infrastructure and Transport, by virtue of which computerized files with personal nature data are created, modified and canceled (DOGV 4.772, on 10 June 2004)
- Decree 149/2007, of September 7, of the Consell, which approves the Statute of Ente Prestador de Servicios de Certificación Electrónica de la Comunitat Valenciana. (DOGV 5,596, dated 11 September 2007)
- Law 5/2013, of 23 December, on Fiscal Measures, Administrative and Financial Management, and Organization of the Generalitat. (DOCV 7,181 of 27 December 2013)
- Decree 15/2014, dated January 24, of the Consell, which approves the Regulation of Organization and Functioning of the Institut Valencià de Finances (IVF). (DOCV 7202 of January 29, 2014)
- Law 21/2017, of 28 December, on Fiscal Measures, Administrative and Financial Management, and Organization of the Generalitat. (DOCV 8.202 of 30 December 2017)
- Law 27/2018, of 27 December, on Fiscal Measures, Administrative and Financial Management, and Organization of the Generalitat. (DOCV 8.453 of 28 December 2018)

The file consists of identity data of the users (name, Id card number), contact information (postal address, email address), needed for the digital certification service provision. These data are considered by the Personal Data Protection Spanish law as basic level data.

ACCV has a Security Document, which has been adjusted to comply with current regulations on all matters relating to personal data protection

9.4.2. Information Treated as Private

In accordance with the stipulations of Article 4.1 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, 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 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 Regulation (EU) 2016/679 of 27 April 2016, confidential information is protected from loss, destruction, damage, falsification and illegal or unauthorized processing (article 5.1.f)

In no case ACCV includes data referred in article 9.2 of Regulation (EU) 2016/679 of 27 April 2016, in the digital certificates issued.

9.4.3. Information not Deemed 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.

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 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 ACCV repository.

9.4.4. Responsibility to protect private information.

ACCV guarantees to comply with its legal obligations as certification services provider, in accordance with Regulation (EU) 910/2014 (eIDAS), and by virtue of this, and in accordance with Article 24 of the aforementioned Regulation, it shall be responsible for any damages that it causes in carrying out its own activity, due to non-compliance with the requirements contained in Article 8 of Law 6/2020 of 11 November, relating to personal data protection

9.4.5. Notice and consent to use private information

For the purposes of provision of the service, 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. Disclosure pursuant to judicial or administrative process

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, 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 52 of the Organic Law 3/2018 of 5 December on the Protection of Personal Data and the Guarantee of Digital Rights, where this communication is required.

9.4.7. Other information disclosure circumstances

In the privacy policy contemplated at the beginning of section 9.4, ACCV includes requirements for permitting the direct disclosure of information pertaining to the subscriber to the subscriber themselves or to third parties

9.5. Intellectual property rights

All intellectual property rights, including those referring to certificates and CRLs issued by ACCV, OIDs, and any other document that is not explicitly mentioned, whether electronic or of any other type, owned by ACCV, belong to ACCV.

CPS and Certification Policies are issued by ACCV, and licensed under a Creative Commons Attribuion-NoDerivatives 4.0 (CC BY-ND 4.0).

Private keys and public keys are the property of the subscriber, 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. Representations and warranties

9.6.1. CA representations and warranties

ACCV 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, to 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 cryptography security of the certification processes which they support.

• Use reliable systems to store qualified certificates which permit verification of a certificate's authenticity and prevent unauthorized 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 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 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 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 220/2014 of 12 December of the Valencian Government, which governs the use of the advanced electronic signature in the Autonomous Government of Valencia.

2. Law 6/2020 of 11 November, regulating certain aspects of electronic trust services

3. European Parliament and Council Regulation (EU) number 910/2014, on electronic identification and trust services for electronic transactions on the domestic market.

4. Law 39/2015, October 1st, about the Common Administrative Procedure of Public Administrations

5. Decree 15/2014 of 24 January of the Consell, which approves the Regulation of the Organization and Functioning of Institut Valencià de Finances (IVF).

6. Law 21/2017, of 28 December 2017 Generalitat Valenciana, which approves integration in Generalitat Valenciana of the functions and competencies in matters of certification and electronic signature developed by the Institut Valencià de Finances (IVF)

7. Law 27/2018, of 27 December 2018 Generalitat Valenciana, which approves the creation of the new organization, ISTEC

8. Order ETD/465/2021, of May 6, regulating remote video identification methods for issuing qualified electronic certificates

9. Order ETD/743/2022, of July 26, which modifies Order ETD/465/2021, of May 6, which regulates the methods of remote identification by video for the issuance of qualified electronic certificates.

10. Royal Decree 203/2021, of March 30, which approves the Regulations for the performance and operation of the public sector by electronic means.

- 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 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 qualified 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.

Root CAs shall be responsible for the performance and warranties of the Subordinates CAs, for the Subordinates CAs' compliance with these Requirements, and for all liabilities and indemnification obligations of the Subordinates CAs under these Requirements, as if Root CAs were the Subordinate CAs issuing the Certificates.

9.6.2. RA representations and warranties

The persons that operate in the RAs integrated into the hierarchy of 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 applicant 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 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 ACCV 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 ACCV of any malfunction or other eventuality that might not comply with normal expected behavior.

• Send a signed copy of the certification contract and of revocation requests to ACCV.

• 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 applicants.

• Collaborate in any aspects of the operation, audit or control of the User Registration Point that are requested of it by ACCV

• 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 ACCV and the information and documentation which has materialized 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 authorization of ACCV, in which case it shall transfer the same confidentiality obligation to the aforementioned third parties.

9.6.3. Subscriber representations and warranties

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

- To 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.

- To apply the necessary care and methods to guarantee the safekeeping of their private key.

- Immediately to 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.

- To 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 ACCV managers of any modification of this information.

- To pay the fees resulting from the certification services that they request from the corresponding Registration Authority in relation to the services that are requested.

ACCV require, as part of the Subscriber Agreement or Terms of Use, that the Applicant make the commitments and warranties in this section for the benefit of the CA and the Certificate Beneficiaries.

Prior to the issuance of a Certificate, ACCV shall obtain, for the express benefit of the CA and the Certificate Beneficiaries, either:

- The Applicant's agreement to the Subscriber Agreement with the CA, or

- The Applicant's acknowledgement of the Terms of Use.

ACCV shall implement a process to ensure that each Subscriber Agreement or Terms of Use is legally enforceable against the Applicant. In either case, the Agreement must apply to the Certificate to be issued pursuant to the certificate request. ACCV may use an electronic or "click-through" Agreement provided that the CA has determined that such agreements are legally enforceable. A separate Agreement will be used for each certificate request.

9.6.4. Relying party representations and warranties

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

- To 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.

- To verify the validity of the certificates at the time of carrying out or verifying any operation based on the certificates.

- To take on their responsibility the correct verification of digital signatures

- To take on their responsibility the verification of the validity, revocation of the certificates on which they rely.

- To 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.

- In the case of qualified certificates, verify that the service identifier is included in the most recent version of the corresponding Trusted List published by the responsible body of the European Commission.

9.6.5. Representations and warranties of other participants

No guarantees or representations are considered for other participants.

9.7. Disclaimers of warranties

ACCV may refuse all guarantees of service that are not linked to obligations stipulated by Law 6/2020 of 11 November, regulating certain aspects of electronic trust services, and Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, especially guarantees of adaptation for a specific purpose or guarantees of use of certificates for commercial purposes.

9.8. Limitations of liability

ACCV shall be responsible for damages that it causes to any person in carrying out its activity, when it fails to fulfill the obligations imposed by Law 6/2020 of 11 November, regulating certain aspects of electronic trust services, Decree 220/2014 of 12 December of the Valencian Government, and European Parliament and Council Regulation (EU) number 910/2014, on electronic identification and trust services for electronic transactions on the domestic market, or it acts negligently.

ACCV shall be responsible 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 validation service of the expiry of validity of the certificate issued by ACCV, once it becomes aware of this.

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.

ACCV is the Agencia de Tecnología y Certificación Electrónica, 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.

ACCV only shall be responsible for damage caused by improper use of the qualified certificate, when it has not recorded on it, in a form clearly recognizable 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 responsible if the signatory exceeds the limits recorded on the certificate in relation to its possible uses and the individualized 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 ACCV.

ACCV shall also not be responsible 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 individualized amount of the transactions that can be carried out with it.

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 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 revocation or loss of validity of the certificate published on the CRL, or if the addressee does not verify the electronic signature.

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. Indemnities

9.9.1. Indemnification by CAs.

ACCV is a government entity, so it is not applicable.

9.10. Term and termination.

9.10.1. Term

In 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.

The CPS, the PDS and the various CPs come into effective at the time of their publication.

9.10.2. Termination

In 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.

This CPS, the PDS and the various CPs will be derogated when a new version of the document is published. The new version will replace the previous document in its entirety.

9.10.3. Effect of termination and survival.

In 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.

For current certificates issued under a previous Certification Policy and Practices Statement, the new version shall prevail over the previous one in all that does not oppose it.

9.11. Individual notices and communications with participants

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.

9.12. Amendments

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 ACCV may not violate the provisions contained in the Certification Policies established by ACCV.

- A modifications control is set up, based on 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.

9.12.1. Procedure for amendment

The entity with the powers to carry out and approve changes to the CPS and Certificate Policies is the ISTEC Manager, the contact data for which is stated in section 1.5.1. of this CPS.

In cases in which the ISTEC Manager 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 ISTEC Manager 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.

9.12.2. Notification mechanism and period

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

9.12.3. Circumstances under which OID must be changed

ISTEC Manager 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, ISTEC Manager shall be responsible for the approval and authorization of the modifications of these documents including the decision of the changes assigned to the OID.

9.13. Dispute resolution provisions

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.

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

9.14. Governing law

The functioning and operations of 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 220/2014 of 12 December of the Valencian Government, which governs the use of the advanced electronic signature in the Autonomous Government of Valencia
- Law 6/2020 of 11 November, regulating certain aspects of electronic trust services
- Law 39/2015, October 1st, about the Common Administrative Procedure of Public Administrations

- Law 40/2015, 1 October, of Legal Regime of the public Sector
- Law 5/2013, of December 23, 2013, on Fiscal Measures, Administrative and Financial Management, and Organization of the Generalitat.
- Law 21/2017, of 28 December 2017 Generalitat Valenciana, which approves integration in Generalitat Valenciana of the functions and competencies in matters of certification and electronic signature developed by the Institut Valencià de Finances (IVF)
- Law 27/2018, of 27 December 2018 Generalitat Valenciana, which approves the creation of the new organization, ISTEC
- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market
- Order ETD/465/2021, of May 6, regulating remote video identification methods for issuing qualified electronic certificates

9.15. Compliance with applicable law

ACCV declares that this CPS complies with the legislation given in section 9.14.

9.16. Miscellaneous provisions

9.16.1. Entire Agreement

This CPS and all documents referred to herein constitute the entire agreement between the parties, superseding all other agreements that may exist with respect to the same matter.

All the third parties that rely on the certificates assume in their entirety the content of the latest version of this document, the PDS and the corresponding CP.

9.16.2. Assignment

This CPS shall be binding upon the successors, executors, heirs, representatives, administrators, and assigns, whether express, implied, or apparent, of the parties.

The invalidity of one of the clauses contained in this CPS will not affect the rest of the clauses. In such a case, the aforementioned clause will be considered without application.

9.16.3. Severability

In case of conflict of any part of this document with current legislation of any jurisdiction in which a CA operates or issues certificates, after the corresponding legal review, ACCV can modify the conflicting points the minimum extent necessary to fulfill the aforementioned legislation.

In such event, (prior to issuing a certificate under the modified requirements) ACCV will include in subsections of this Section information about the Law requiring modification and the specific change implemented by ACCV.

ACCV will also (prior to issuing a certificate under the modified requirement) inform interested parties such as the CAB Forum of the relevant information newly added.

9.16.4. Enforcement (attorneys' fees and waiver of rights)

ACCV may seek indemnification and attorneys' fees from a party for damages, losses, and expenses related to that party's conduct. ACCV's failure to enforce a provision of this CPS does not waive ACCV's right to enforce the same provision later or right to enforce any other provision of this CPS. To be effective, waivers must be in writing and signed by ACCV.

9.16.5. Force Majeure

ACCV will accept no liability for the non-fulfillment or the delayed fulfillment of any of the obligations contained in the CPS, if such non-fulfillment or delay is the consequence of a force majeure event, unforeseeable circumstances or any circumstance on which direct control cannot be exerted.

The operation of the Internet is beyond ACCV's reasonable control

9.17. Other provisions

In case of loss of the QSCD certification of any of the qualified devices that the ACCV was using, which are detailed in point 6.2.1 of the applicable Certification Policy, ACCV will take the necessary measures to minimize the possible impact, informing the supervising body thereof and paralyzing the issuance of certificates on affected devices.