Agencia de Tecnología y Certificación Electrónica

Certification Policy for Qualified Certificates in qualified electronic signature creation devices for Public Employees

Date: 12/02/2024	**Version:** 6.0.2
Status: APPROVED	**Number of pages:** 49
OID: 1.3.6.1.4.1.8149.3.13.6.0	**Classification: PUBLIC**
File: ACCV-CP-13V6.0.2-EN-2024.odt	
Prepared by: Agencia de Tecnología y Certificación Electrónica - ACCV	

Changelog

Version	Author	Date	Observations
5.0.1	ACCV	03/05/2018	RFC3647 Changes
5.0.2	ACCV	20/03/2021	Policy Notice
5.0.3	ACCV	20/07/2022	Review and change minor details
5.0.4	ACCV	31/08/2023	EKU S/MIME is eliminated
6.0.1	ACCV	28/09/2023	New hierarchy
6.0.2	ACCV	12/02/2024	Changes in CAs to adjust scope

1 INTRODUCTION

1.1 Overview

The current document is the Certification Policy associated to the qualified certificates in qualified electronic signature creation device for public employees, which contains the rules of management and use the certificates issued within this Certificate Policy. It also describes the roles, responsibilities and relationships between the end user and the Electronic Certification and Technology Agency, and the rules for request, acquisition and generation of the certificate. This document qualifies and complements the Certification Practices Statement (CPS) of the Agencia de Tecnología y Certificación Electrónica.

The Certification Policy that is referred in this document will be used for the issuance of qualified certificates for public employees, in qualified electronic signature creation devices -smart card-.

The current Certification Policy is drafted following the RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" specifications, proposed by Network Working Group for this type of documents, the same as the Certification Practices Statement, for ease the reading and comparison with counterparts documents.

This Certification Policy assumes that the reader has a basic knowledge of Public Key Infrastructure, digital certificates and signature concepts, otherwise is recommended to be trained in these concepts before continuing reading the current document

1.2 Document Name and Identification

Policy name	Certification Policy for Qualified Certificates in qualified electronic signature creation device for Public Employees
Policy Qualifier	`Certificado cualificado de Empleado Público expedido por la ACCV (Pol. Ademuz, s/n. Burjassot, CP 46100, ESPAÑA. CIF A40573396)`
Policy Version	6.0.2
Policy Status	APPROVED
Policy Reference / OID (Object Identifier)	1.3.6.1.4.1.8149.3.13.6.0
Date of issuance	12nd february 2024
Date of expiration	Not applicable.
Related CPS	Certification Practices Statement (CPS) of the ACCV. Version 5.0 OID: 1.3.6.1.4.1.8149.2.5.0 Available at `http://www.accv.es/pdf-politicas`
Location	This Certification Policy can be found at: http://www.accv.es/legislacion_c.htm

1.3 PKI participants

1.3.1 Certification Authorities

The CA that can issue certificates in accordance with this policy is ACCV RSA1 PROFESIONALES and ACCV ECC1 PROFESIONALES belonging to the Agencia de Tecnología y Certificación

Electrónica, whose function is to issue end-entity certificates for ACCV subscribers. The choice of one or another CA will depend on the type of keys used for the issuance of final certificates: RSA or ECDSA.

ACCV RSA1 PROFESIONALES and ACCV ECC1 PROFESIONALES certificates are valid from July 25, 2023 to July 19, 2047.1 until 1 January 2027.

1.3.2 Registration Authorities

The list of Registration Authorities (User Register Points) that manage the certificate requests that are defined in this policy is found at the http://www.accv.es URL.

1.3.3 Subscribers

The group of users who can request the certificates that are defined by this policy is made up of public employees who work for any type of Public Administration (European, statewide, autonomic and local) as well as employees of their instrumental entities, and employees of Corporations and Public Universities, in possession of the identification elements that are required (DNI, NIE, etc.).

The storage of the keys and certificates can be:

- Cryptographic card Giesecke & Devrient (G&D) Sm@rtCafé Expert 7.0 and later versions.

- Cryptographic card ChipDoc v2 on JCOP 3 P60 in SSCD configuration, version V7b4_2

- Cryptographic card ChipDoc v3.2 on JCOP 4 P71 in SSCD configuration version 3.2.0.52

In case of accrediting another qualified electronic signature creation device, this will be included in this document, at point 6.2.1

The right to request certificates that are defined in this Certification Policy is limited to natural persons. Certification requests that are carried out in name of legal body, entity or organization, will not be accepted.

1.3.4 Relying parts

The right to trust in certificates that are issued in accordance with this policy, is limited to:

- The applications and services belonging to the Generalitat, any entity or organization that is linked with the Generalitat or Public Administration or Corporate with which a certification agreement has been signed.
- The applications and services of any Public Administration.
- The applications or services of any public or private entity that requires a secure electronic identification or the citizens digital signature.

1.3.5 Other participants

According to the specified in the Certification Practices Statement (CPS) of ACCV.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

The certificates that are issued by the Agencia de Tecnología y Certificación Electrónica under this Certification Policy, can be used for electronic signature and encryption of any information or document. Likewise, they can be used as an identification mechanism in services and applications.

1.4.2 Prohibited certificate uses

The certificates will be used only in accordance with the purpose and function established in this Certification Policy, and with the existing regulatory framework.

1.5 Policy administration

1.5.1 Organization administering the document

According to the specified in the Certification Practices Statement (CPS) of ACCV.

1.5.2 Contact person

According to the specified in the Certification Practices Statement (CPS) of ACCV.

1.5.3 Person determining CPS suitability for the policy

According to the specified in the Certification Practices Statement (CPS) of ACCV.

1.5.4 CPS approval procedures

According to the specified in the Certification Practices Statement (CPS) of ACCV.

1.6 Definitions and Acronyms

According to the specified in the Certification Practices Statement (CPS) of ACCV.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

According to the specified in the Certification Practices Statement (CPS) of ACCV.

2.2 Publication of certification information

According to the specified in the Certification Practices Statement (CPS) of ACCV.

The Agencia de Tecnología y Certificación Electrónica (ACCV) is adjusted to the current version of the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" document, disclosed at https://www.cabforum.org/. In case of any incompatibility between this Certification Policy and the CAB Forum requirements, those requirements will prevail over this document.

2.3 Time or frequency of publication

According to the specified in the Certification Practices Statement (CPS) of ACCV.

2.4 Access controls on repositories

According to the specified in the Certification Practices Statement (CPS) of ACCV.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of names

According to the specified in the Certification Practices Statement (CPS) of ACCV.

3.1.2 Need for names to be meaningful

According to the specified in the Certification Practices Statement (CPS) of ACCV.

3.1.3 Anonymity or pseudonymity of subscribers

According to the specified in the Certification Practices Statement (CPS) of ACCV.

3.1.4 Rules for interpreting various name forms

According to the specified in the Certification Practices Statement (CPS) of ACCV.

3.1.5 Uniqueness of names

According to the specified in the Certification Practices Statement (CPS) of ACCV.

3.1.6 Recognition, authentication, and role of trademarks

According to the specified in the Certification Practices Statement (CPS) of ACCV.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

According to the specified in the Certification Practices Statement (CPS) of ACCV.

3.2.2 Authentication of organization identity

The request of certificates defined in this Certification Policy is limited to public Administrations or Entities which have a certification agreement, contract or any other formula established, for providing the certification service by ACCV.

The identification of the public Administrations or Entities will be carried out in the Entity register process that will be subscribed by a natural person with capabilities of represent the Administration or Entity.

3.2.3 Authentication of individual identity

The authentication of the identity of a public employee certificate applicant will be carried out through his/her presence in front of the Operator of the Public Employee Registration Point, accrediting himself/herself by submitting his/her Identity National Document (DNI), Spanish passport, the Foreign Identification Number (NIE) or other admitted means in Law.

The determination of the status of public employee is responsibility of the applicant public Administration or Entity, which must verify the status of public employee either in its database of personnel or requesting the document for which the applicant public employee obtains this category.

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

According to the specified in the Certification Practices Statement (CPS) of ACCV.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

The identification and authentication for routine re-key can be carried out using the techniques of initial authentication and identification (described at point 3.2.3. *Authentication of individual identity* of this Certification Policy). In case of remote identification in front of the Registration Authority, the user will access to the Personal Area of the Certification Services (APSC) identifying himself/herself with a personal qualified certificate of the ACCV or the DNIe. Therefore, there exist two mechanisms for the renewal:

- Web forms in the APSC, available at www.accv.es
- A Request of a new certificate by the public Administration or Entity that the subscriber belongs to (see chapter 3.2.3. *An individual identity authentication*, of this Certification Policy).

3.3.2 Identification and authentication for re-key after revocation – Not compromised key.

The policy of identification and authentication for the renewal of a certificate without key compromise will be the same as for the initial register, or some electronic method will be applied for ensuring in a reliable and unequivocal manner the applicant identity and the request authenticity.

3.4 Identification and authentication for revocation request

The identification policy for revocation requests accepts the following identification methods:

- Face-to-face processing. The same method as for the initial register described in the point 3.2.3. *An individual identity authentication*, in this Certification Policy.
- Web. Accessing to the Personal Area of the Certification Services, identifying himself/herself through a personal qualified certificate of the ACCV or with the eDNI (subscriber access)
- Web. Accessing to the Web Front end provided by the ACCV to Public Administrations and Entities for management of Public Employees Certificates (management access)
- Telephone. By answering the questions of the Call Center support, available at the 902482481 phone number.

ACCV or any entity that makes it up can ex-officio request the revocation of a certificate if it has knowledge or suspect about the compromise of the subscriber's private key, or any other event that would recommended to carry out this action.

The certificates revocation request must be carried out by the persons of contact that are registered for the certificates management of every public Administration or Entity when the subscriber, public employee, loses this condition or changes the occupation or the position that is collected in the certificate.

4 Certificate life-cycle operational requirements

The specifications that are contained in this chapter complement the stipulations that are provided in the Certification Practices Statement (CPS) of the ACCV.

4.1 Certificates Application

4.1.1 Who can submit a certificate application

Users listed in 1.3.3 may submit a certificate request.

The application for this type of certificate is the responsibility of the Public Administration or public entities, which must verify the public employee status of the certificate holders by consulting the personnel records of the organization under its jurisdiction. Each of these Entities must provide the ACCV with a set of Administrators who are responsible for obtaining and confirming the users' data, their affiliation to the entity and, if applicable, deliver the signature creation data to the user once the certification contract has been signed. They are also obliged to send the ACCV the corresponding copy of the contract. To register these Organizations and the corresponding Administrators, the entity registration form must be used, as shown in Annex III of this Certification Policy.

4.1.2 Enrollment Process and Responsibilities

To carry out the request for certificates, the tools and applications provided by the ACCV to the Authorized Administrators of the different public bodies must be used. At least the minimum mandatory data required by this policy must be provided (ID, name, surname, Public Body and email address). All data (mandatory and optional) must be obtained from personnel records and official guides of the entity, and the ACCV may request any additional proof or evidence that may be necessary for the verification of the data.

In the case of face-to-face applications, the application data is obtained from the official documentation provided by the applicant and consultation of the available official records, and it is the responsibility of the ACCV to verify the data and ensure the availability of the registration authorities and associated systems, as well as to inform the applicant of the different stages through which the application passes. It is the applicant's responsibility to provide accurate information in their application.

In the case of video identification mechanisms, it is necessary that the evidence is the same and has the same probative value of identity (same quality). The use of identity verification systems by video identification is subject to the corresponding legal basis and associated technical regulations. In the event that this type of mechanism can be used, a full description of the solution will be included in Annex V of this policy.

In the case of non-face-to-face remote applications, the data is obtained from the information available in the qualified digital certificate used to identify the applicant, and it is the responsibility of the ACCV to verify the data and ensure the availability of the registration authorities and associated systems, as well as to inform the applicant of the different stages the application goes through. It is the applicant's responsibility to provide accurate information in their application.

Likewise, in the case of certificate applications through remote, non face-to-face means, a period of time of less than five years from the face-to-face identification shall be required.

ACCV retains information associated with applications indefinitely (with a limit of at least 15 years), including approval or rejection, and the reasons for rejection.

4.2 Certificates request management

After receiving the request for certificates from the authorized persons through the web application and once accepted the economic proposal, if it is the case, the certificates generation and the preparation of its associated documentation will be proceeded. Once completed, it will be redirected to the public Administration or Entity, through the authorized persons for the management.

The persons that are authorized for the certificates management will be responsible for the identification of the users acting as Registration Authority, the delivery of the certificates to the subscribers, confirming the signature of the contract and sending the corresponding copy to the Agencia de Tecnología y Certificación Electrónica.

4.2.1 Performing identification and authentication functions

Authentication of the identity of the certificate applicant shall be performed by identification before the corresponding Registration Authority using the mechanisms described in section 3.2.3 Authentication of individual identity. The Registration Authority Operator checks the documentation and validates the data using the publicly accessible records and the agency's own records for such verification.

4.2.2 Approval or rejection of certificate applications

In case of acceptance, the Registration Authority will notify the applicant by e-mail to the e-mail address given in the application.

In face-to-face applications, the Registration Authority will inform the user of the acceptance or rejection directly.

In remote requests, the applicant must access the Certification Services Personal Area (remote Registration Authority) with a personal certificate or the DNIe. If the applicant can make the request, the corresponding option will be displayed.

In case of rejection, the Registration Authority will inform the applicant through the corresponding mechanisms. In face-to-face requests the Operator will directly inform the user of the rejection and the reason for it, interrupting the process at that moment and canceling the request on the platform. In remote applications the Registration Authority will inform the user in the application preventing the continuation of the process.

The ACCV will use this information to decide on new applications.

4.2.3 Time to process certificate applications

Maximum time to process certificate applications is five working days.

4.3 Certificates issuance

ACCV is not responsible for the monitoring, investigation or confirmation about the accuracy of the information that is contained in the certificate subsequently to its issuance. In case of receiving information about the inaccuracy or the current non-applicability of the information that is collected in the certificate, this one can be revoked.

The issuance of the certificate will be made when the ACCV has carried out the necessary verification to validate the certification request. The mechanism that determines the nature and manner of performing such verification is this Certification Policy.

When the ACCV issues a certificate in accordance with a valid certification request, it will send a copy of certificate to the Registration Authority that submitted the request and another copy to the ACCV repository.

Registration Authority will notify the subscriber of the certificate issuance and will provide the certificate or means to obtain it.

4.3.1 CA actions during certificate issuance

The issuance of the certificate takes place once the Registration Authority has performed the necessary checks to validate the certification request. The mechanism that determines the nature and form of these checks is this Certification Policy.

In on-site requests the steps are as follows:

- The Registration Authority uses the data entered by the Operator at the on-site registration point.

- The Registration Authority checks the entry of personal data.

- The Registration Authority generates the key pair and the certificate request indicating the parameters defined in this policy.

- The Registration Authority sends the signed CSR to the Certification Authority.

- The Certification Authority verifies the signature of the Registration Authority and confirms that the form of the CSR is correct.

- The Certification Authority signs the CSR and returns it to the Registration Authority.

- The Registration Authority communicates the certificate to the applicant.

For remote requests with a qualified certificate the steps are as follows:

- The applicant has identified himself with an ACCV qualified certificate or with the DNIe and the personal data associated with the request are extracted from the certificate fields.

- The Registration Authority checks the personal data entered by the applicant in the registration URL.

- The Registration Authority performs the key pair generation and the certificate request indicating the parameters defined in this policy.

- The Registration Authority sends the signed CSR to the Certification Authority.

- The Certification Authority verifies the signature of the Registration Authority and confirms that the form of the CSR is correct.

- The Certification Authority signs the CSR and returns it to the Registration Authority.

- The Registration Authority communicates the certificate to the applicant.

4.3.2 Notification to subscriber by the CA of issuance of certificate

ACCV notifies the subscriber about the issuance of certificate, through an electronic mail to the email address provided in the application process.

4.4 Certificates acceptance

4.4.1 Conduct constituting certificate acceptance

The certificates acceptance by the subscriber is produced in the moment of the signature of the certification contract that is associated to every Certification Policy. The contract acceptance involves the knowledge and acceptance by the subscriber of the associated Certification Policy.

The Certification Contract is a document that must be signed by the applicant and by the Registration Authority Operator, and which purpose is to link the person to be certified with the action of requesting, with the knowledge of the usage rules and the submitted data veracity. The Certification Contract is included in the Annex I of this Certification Policy.

4.4.2 Publication of the certificate by the CA

According to the specified in the Certification Practices Statement (CPS) of ACCV.

4.4.3 Notification of certificate issuance by the CA to other entities

According to the specified in the Certification Practices Statement (CPS) of ACCV.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

According to the specified in the Certification Practices Statement (CPS) of ACCV.

4.5.2 Relying party public key and certificate usage

According to the specified in the Certification Practices Statement (CPS) of ACCV.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

According to the specified in the Certification Practices Statement (CPS) of ACCV.

4.6.2 Who may request renewal

According to the specified in the Certification Practices Statement (CPS) of ACCV.

4.6.3 Processing certificate renewal requests

According to the specified in the Certification Practices Statement (CPS) of ACCV.

4.6.4 Notification of new certificate issuance to subscriber

According to the specified in the Certification Practices Statement (CPS) of ACCV.

4.6.5 Conduct constituting acceptance of a renewal certificate

According to the specified in the Certification Practices Statement (CPS) of ACCV.

4.6.6 Publication of the renewal certificate by the CA

According to the specified in the Certification Practices Statement (CPS) of ACCV.

4.6.7 Notification of certificate issuance by the CA to other entities

According to the specified in the Certification Practices Statement (CPS) of ACCV.

4.7 Certificate re-key

According to the specified in the Certification Practices Statement (CPS) of ACCV.

4.7.1 Circumstance for certificate re-key

According to the specified in the Certification Practices Statement (CPS) of ACCV.

4.7.2 Who may request certification of a new public key

According to the specified in the Certification Practices Statement (CPS) of ACCV.

4.7.3 Processing certificate re-keying requests

According to the specified in the Certification Practices Statement (CPS) of ACCV.

4.7.4 Notification of new certificate issuance to subscriber

According to the specified in the Certification Practices Statement (CPS) of ACCV.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

According to the specified in the Certification Practices Statement (CPS) of ACCV.

4.7.6 Publication of the re-keyed certificate by the CA

According to the specified in the Certification Practices Statement (CPS) of ACCV.

4.7.7 Notification of certificate issuance by the CA to other entities

According to the specified in the Certification Practices Statement (CPS) of ACCV.

4.8 Certificates modification

According to the specified in the Certification Practices Statement (CPS) of ACCV.

4.8.1 Circumstance for certificate modification

According to the specified in the Certification Practices Statement (CPS) of ACCV.

4.8.2 Who may request certificate modification

According to the specified in the Certification Practices Statement (CPS) of ACCV.

4.8.3 Circumstance for certificate modification

According to the specified in the Certification Practices Statement (CPS) of ACCV.

4.8.4 Notification of new certificate issuance to subscriber

According to the specified in the Certification Practices Statement (CPS) of ACCV.

4.8.5 Conduct constituting acceptance of modified certificate

According to the specified in the Certification Practices Statement (CPS) of ACCV.

4.8.6 Publication of the modified certificate by the CA

According to the specified in the Certification Practices Statement (CPS) of ACCV.

4.8.7 Notification of certificate issuance by the CA to other entities

According to the specified in the Certification Practices Statement (CPS) of ACCV.

4.9 Certificates revocation and suspension

4.9.1 Circumstances for revocation

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

4.9.2 Who can request revocation

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

The authorized persons for the management of certificates of an organization can request the revocation of the certificates through the application provided by the ACCV. This request is only allowed for certificates issued to public employees of his/her organization.

When the subscriber of a public employee certificate ceases of being a public employee, the authorized personnel for the certificates management of that Organization has the responsibility to request the revocation of the digital certificate.

4.9.3 Procedures for revocation request

The Agencia de Tecnología y Certificación Electrónica accepts revocation requests by the following processes.

4.9.3.1 Face-to-face processing

With the appearance and identification of the subscriber or the authorized requester of every entity, in the User Register Point and by filling and signing by the same part, the “Revocation Request Form” that will be provided and that is attached in the annex II.

4.9.3.2 Web

There exists a revocation request form of certificates, available at the ACCV web: http://www.accv.es

In addition, the authorized persons for the management of certificates of an organization can request the revocation of the certificates through the application provided by the ACCV. This request is only allowed for certificates issued to public employees of his/her organization.

4.9.3.3 Phone

Through a telephone call to the support number of the Agencia de Tecnología y Certificación Electrónica at 963 985 308.

When the subscriber of a public employee certificate ceases to be a public employee of an Administration, Corporation or Instrumental Entity, the personnel authorized to manage the certificates of said Administration or Entity, or failing that, the Personnel Registry of said Organization shall request the revocation of the digital certificate.

4.9.4 Revocation request grace period

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

4.9.5 Time within which CA must process the revocation request

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

4.9.6 Revocation checking requirement for relying parties

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

4.9.7 CRL issuance frequency

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

4.9.8 Maximum latency for CRLs

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

4.9.9 On-line revocation/status checking availability

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

4.9.10 On-line revocation checking requirements

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

4.9.11 Other forms of revocation advertisements available

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

4.9.12 Special requirements re key compromise

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

4.9.13 Circumstances for suspension

A certificate can be suspended if an administrative or judicial authority provides so, and for the time it establishes.

ACCV does not support certificates suspension as an independent operation over its certificates.

4.9.14 Who can request suspension

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

4.9.15 Procedure for the suspension request

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

4.9.16 Limits of suspension period

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

4.10 Certificate status services

4.10.1 Operational Characteristics

According to the specified in the Certification Practices Statement (CPS) of ACCV.

4.10.2 Service Availability

According to the specified in the Certification Practices Statement (CPS) of ACCV.

4.10.3 Optional features

According to the specified in the Certification Practices Statement (CPS) of ACCV.

4.11 End of the subscription

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

ACCV will inform the subscriber about the certificate suspension or revocation, specifying the reasons, the date and time that his/her certificate will lose its efficacy, and communicating him/her that it can not be used anymore. This information will be carried out with a digitally signed email and before the public disclosure.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

ACCV does not escrow private keys issued under this Policy.

4.12.2 Session key encapsulation and recovery policy and practices

Session key recovery is not supported.

4.13 CA certificate key expiration.

ACCV shall avoid generating public employee certificates that expire after the CA certificates. To do this, public employee certificates whose validity period exceeds that of the CA certificate in question will not be issued and will be generated with the new CA certificate, in order to avoid notifying subscribers to renew their certificate, in the event that the CA certificate expires earlier.

5 Facility, management, and operational controls

5.1 Physical Controls

5.1.1 Site location and construction

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.1.2 Physical access

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.1.3 Power and air conditioning

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.1.4 Water exposure

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.1.5 Fire prevention and protection

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.1.6 Media storage

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.1.7 Waste disposal

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.1.8 Off-site backup

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.2 Procedural Controls

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.2.1 Trusted roles

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.2.2 Number of persons that are required per task

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.2.3 Identification and authentication for each role

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.3 Personnel controls

This chapter reflects the content of the *Personnel Security Controls* document of the ACCV.

5.3.1 Qualifications, experience, and clearance requirements

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.3.2 Background check procedures

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.3.3 Training requirements

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.3.4 Retraining frequency and requirements

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.3.5 Job rotation frequency and sequence

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.3.6 Sanctions for unauthorized actions

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.3.7 Independent contractor requirements

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.3.8 Documentation supplied to personnel

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.3.9 Periodical compliance controls

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.3.10 End of contracts

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.4 Audit logging procedures

5.4.1 Types of events recorded

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.4.2 Frequency of processing log

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.4.3 Retention period for audit log
According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.4.4 Protection of audit log
According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.4.5 Audit log backup procedures
According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.4.6 Audit collection system (internal vs. external)
According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.4.7 Notification to event-causing subject
According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.4.8 Vulnerability assessments
According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.5 Records archival

5.5.1 Types of records archived
According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.5.2 Retention period for archive
According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.5.3 Protection of archive
According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.5.4 Archive backup procedures
According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.5.5 Requirements for time-stamping of records
According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.5.6 Archive collection system (internal or external)
According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.5.7 Procedures to obtain and verify archive information
According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.6 Key changeover
Not stipulated.

5.7 Compromise and disaster recovery

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.7.1 Incident and compromise handling procedures

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.7.2 Computing resources, software, and/or data are corrupted

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.7.3 Entity private key compromise procedures

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.7.4 Business continuity capabilities after a disaster

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

5.8 CA or RA termination

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

6 Technical security controls

6.1 Key pair generation and installation

This chapter is always referred to the keys that are generated for the certificates issued under the scope of this Certification Policy. The information about the keys of the entities that make up the Certification Authority is collected in the chapter 6.1 of the Certification Practices Statement (CPS) of the Agencia de Tecnología y Certificación Electrónica.

6.1.1 Key pair generation

The key pair for the certificates that are issued under the scope of this Certification Policy is generated in the user signature creation device and it never leaves it.

6.1.2 Private key delivery to subscriber

The private keys for the certificates issued under the scope of the Certification Policy are contained in the signature creation device which is delivered to the subscriber with his/her certificate in the moment of register.

6.1.3 Public key delivery to certificate issuer

The public key to be certified is generated in the signature creation device and is delivered to the Certification Authority by the Register Authority by sending a certification request in PKCS#10 format, digitally signed by the Operator of the Register Authority.

6.1.4 CA public key delivery to relying parties

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

6.1.5 Key sizes

The key size for certificates issued under the scope of this Certification Policy is:

- For RSA keys of at least 2048 bits.
- For ECDSA keys of at least ECC P-256.

6.1.6 Public key parameters generation and quality checking

The parameters defined in the ETSI TS 119 312 document "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites" are used.

The parameters used are as follows:

Signature Suite	Hash Function	Padding Method	Signature algorithm
sha256-with-rsa	sha256	emsa-pkcs1-v1.5	rsa
ecdsa-with-SHA256	sha256		ecdsa

6.1.7 Key Usage Purposes

The certificates issued under the present policy contain the attributes

"KEY USAGE" and "EXTENDED KEY USAGE", as defined in the X.509v3 standard.

The keys that are defined in the current policy will be used for the uses described at the section 1.3 *User community and scope of application* of this document.

The detailed definition of the certificate profile and the usage of keys is located in the section 7 of this document "*Certificate profiles, CRL and OCSP*".

6.2 Private Key Protection and Cryptographic Module Engineering Controls

This chapter is always referred to the keys that are generated for the certificates issued under the scope of this Certification Policy. The information about the keys of entities that make the Certification Authority up, is included in the chapter 6.2 of the Certification Practices Statement (CPS) of the ACCV.

The systems where private keys are stored must meet a series of requirements related to physical and logical security. ACCV may request the subscribing organization to provide evidence of the mechanisms used to comply with these requirements, at its discretion. It is recommended to follow the guidelines generated by the CCN (Centro Nacional de Criptografía) within its CNN-STIC series, specifically aimed at securing the computer systems and communications.

6.2.1 Cryptographic module standards and controls

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.

The qualified signature creation devices (DSCF) that are able for providing support to this type of certificates are the following:

• G&D Smart Cards:

− Giesecke & Devrient (G&D) SmartCafe Expert 7.0 215K FIPS 140-2 Level 2

• BIT4ID Smart Cards:

− ChipDoc v2 on JCOP 3 P60 in SSCD configuration, version V7b4_2

- ChipDoc v3.2 on JCOP 4 P71 in SSCD configuration version 3.2.0.52

6.2.2 Private key (n out of m) multi-person control

The private keys for the signature certificates issued within the scope of this Certification Policy is under the sole control of their subscribers.

6.2.3 Private key escrow

ACCV never escrows keys with usages of Digital Signature or Content Commitment.

6.2.4 Private key backup

ACCV never backups keys with usages of Digital Signature or Content Commitment.

6.2.5 Private key archival

ACCV never archives keys with usages of Digital Signature or Content Commitment.

6.2.6 Private key transfer into or from a cryptographic module

The generation of keys linked to the certificate is carried out into signature creation device by its own cryptographic chip and they never leave it.

6.2.7 Private key storage on cryptographic module

The generation of keys linked to the certificate is carried out into signature creation device by its own cryptographic chip and they never leave it.

6.2.8 Method of activating private key

The subscriber private key is enabled by introducing the PIN of the signature creation device that contains it..

6.2.9 Method of deactivating private key

The subscriber private key deactivation can be achieved by extracting the signature creation device that contains it out of the PC/SC reader.

6.2.10 Method of destroying private key

Destruction must always be preceded by revocation of the certificate associated with the private key, If the key is still active.

6.2.10.1 Signature creation device

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 Certification Policy.

6.3 Other aspects of key pair management

6.3.1 Public key archival

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

6.3.2 Certificate operational periods and key pair usage periods

The certificates that are issued within the scope of this policy are valid for three (3) years.

The key pair that is used for the certificates issuance is created for every issuance, and therefore are valid for three (3) years.

The ACCV RSA1 PROFESIONALES and ACCV ECC1 PROFESIONALES certificates are valid from July 25, 2023 to July 19, 2047.

6.4 Activation data

6.4.1 Activation data generation and installation

The activation data of the private key consists in the signature creation device PIN that contains it and which is submitted to the certificate subscriber.

The signature creation device PIN generation is performed in the moment of its initialization. The PIN and the unlock code -PUK-, will be delivered to the subscriber after signing the certification contract.

It is the responsibility and obligation of the subscriber to safeguard this PIN (and PUK). The subscriber is advised to change this preconfigured PIN to one of his/her own knowledge.

6.4.2 Activation data protection

The subscriber has the responsibility to safeguard the PIN and the PUK securely. The subscriber is recommended to change this preset PIN by another one of his/her exclusive knowledge.

6.4.3 Other aspects of activation data

There are NO other aspects to consider.

6.5 Computer security controls

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

6.6 Life Cycle Security Controls

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

6.7 Network Security Controls

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

6.8 Time-stamping

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

7 Certificate, CRL and OCSP profiles

7.1 Certificate profile

7.1.1 Version number(s)

This certification policy specifies the usage of a certificate with three different uses; Digital Signature, Content Commitment and Key encipherment. The certificate profile is indicated in the chapter 7.1.2 *Certificate extensions* of this Policy.

7.1.2 Certificate extensions

The extensions used by the certificates issued within the scope of the current policy are:

Field	**Value**
Subject	
SerialNumber	Subscriber DNI or NIE. 9 characters filled with zeros on the left side
GivenName	Subscriber name, as it is in the DNI or NIE
SurName	Subscriber surname as it is in the DNI or NIE SURNAME1 SURNAME2
CommonName	String composed in the following manner: NAME SURNAME1 SURNAME2 **– DNI** SUBSCRIBER NIF
Title	Position of the subscriber in the Organization
OrganizationalUnit	Subscriber identification number (unique in an organization)
OrganizationalUnit	Department to which the certificate subscriber belongs
OrganizationalUnit	String with the value CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO
Organization	Designation (“official” name) of the Public Administration, Organization or entity which the certificate subscriber belongs, and which the public employee is linked to.
Country	String with the value ES
Version	V3
SerialNumber	Certificate unique identifier (32 hexadecimal characters)
Signature algorithm	ACCV_RSA1_PROFESIONALES: sha256withRSAEncryption ACCV_ECC1_PROFESIONALES: ecdsa-with-SHA256
Issuer (Emisor)	DN of the CA issuing the certificate (see point 7.1.4)
Válido desde	Date of Issuance
Válido hasta	Date of Expiration
Clave Pública	Octet String that contains the subscriber’s public key
Extended Key Usage	
	Client Authentication

	Adobe Authentic Documents Trust (1.2.840.113583.1.1.5)	
CRL Distribution Point	ACCV_RSA1_CLIENTE: http://www.accv.es/gestcert/accv_rsa1_profesionales.crl ACCV_ECC1_CLIENTE: http://www.accv.es/gestcert/accv_ecc1_profesionales.crl	
SubjectAlternativeName		
DirectoryName		
	CN=Name|Surname1|Surname2	
	UID=NIF	
	Administrative Identity (it is extended in the section 7.1.5)	
Certificate Policy Extensions		
Policy OID	QCP-n: certificate policy for EU qualified certificates issued to natural persons; Itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural(0)	
Policy OID	2.16.724.1.3.5.7.2	
Policy OID	1.3.6.1.4.1.8149.3.13.6.0	
Policy CPS Location	http://www.accv.es/legislacion_c.htm*	
Policy Notice	`Certificado cualificado de Empleado Público expedido por la ACCV (Pol. Ademuz, s/n. Burjassot, CP 46100, ESPAÑA. CIF A40573396)`	
Authority Information Access		
Access Method	Id-ad-ocsp	
Access Location	http://ocsp.accv.es	
Access Method	Id-ad-calssuers	
Access Location	ACCV_RSA1_PROFESIONALES: http://www.accv.es/gestcert/accv_rsa1_profesionales.crt ACCV_ECC1_ PROFESIONALES: http://www.accv.es/gestcert/accv_ecc1_profesionales.crt	
Fingerprint issuer	Fingerprint of the certificate of the CA issuing the certificate (see CPS)	
Algoritmo de hash	SHA-256	
KeyUsage (críticos)		
	RSA Digital Signature	**ECC** Digital Signature

	Non-repudiation Key encipherment	Non-repudiation Key agreement
QcStatement	**Campos QC (Qualified Certificate)**	
QcCompliance		The certificate is qualifies
QcType	eSign	Particular type of qualified certificate
QcRetentionPeriod	15y	Retention period of material information
QcPDS	https://www.accv.es/fileadmin/Archivos/Practicas_de_certificacion/ACCV-PDS-V1.0-EN.pdf	PKI Disclosure Statement Location

7.1.3 Algorithms object identifiers (OID)

Cryptography algorithms' object identifiers (OID):

- SHA1withRSA (1.2.840.113549.1.1.5)
- SHA256withRSA (1.2.840.113549.1.1.11)
- ecdsa-with-SHA256 (1.2.840.10045.4.3.2)

7.1.4 Name forms

The certificates issued by the ACCV contain the certificate issuer and subscriber distinguished name X.500 in the issuer name and subject name fields, respectively.

The Issuer names admitted for certificates issued under this policy are:

- cn=ACCV RSA1 PROFESIONALES,2.5.4.97=VATES-A40573396,o=ISTEC,l=BURJASSOT,s=VALENCIA,c=ES
- cn=ACCV ECC1 PROFESIONALES,2.5.4.97=VATES-A40573396,o=ISTEC,l=BURJASSOT,s=VALENCIA,c=ES

All the fields of the certificate of the Subject and Subject Alternative Name, excepting the ones that are referred to DNS name or electronic addresses, are obligatory filled with capital letters and without accents.

7.1.5 Administrative Identity

For guaranteeing the interoperability between the different AAPP the following data of Administrative Identity is created in the Directory/name object.

Field	Content	Observations
Certificate type	Indicates the certificate nature	Type= certificado electrónico de empleado público OID.2.16.724.1.3.5.7.2.1
Name of the Organization	The Public Administration or Organization to which the certificate subscriber belongs	Subscriber Entity = ie: ACCV OID.2.16.724.1.3.5.7.2.2
NIF of the Organization	Organization identification	Organization NIF ie: S4611001A

	number	OID.2.16.724.1.3.5.7.2.3
Subscriber DNI or NIE	Subscriber DNI or NIE	Subscriber DNI or NIE = ie: 00000000G OID.2.16.724.1.3.5.7.2.4
Personal identification number	Identification number of the subscriber (presumably unique). It is corresponded to the NRP or NIP	Identification number = ie: A02APE1056 OID.2.16.724.1.3.5.7.2.5
Given name	Subscriber Given name	N = Given name of the subscriber according to the DNI or, in foreign case to the NIE or passport OID.2.16.724.1.3.5.7.2.6
First Surname	First surname of the subscriber	SN1 = First surname of the subscriber, according to the DNI or in foreign case, to the NIE or passport OID.2.16.724.1.3.5.7.2.7
Second Surname	Second surname of the subscriber	SN2 = Second surname of the certificate's responsible, according to the DNI or in foreign case, to the passport OID.2.16.724.1.3.5.7.2.8
Electronic mail	Electronic mail of the subscriber	Electronic mail of the subscriber ie: jvalenciano@accv.es OID.2.16.724.1.3.5.7.2.9
Organization unit	Unit, within the Administration, to which the certificate subscriber belongs	Unit = ie: AGENCIA DE TECNOLOGÍA Y CERTIFICACION ELECTRONICA OID.2.16.724.1.3.5.7.2.10
Title	Position that is occupied by the subscriber within the Organization	Position = ie: PROGRAMMER ANALYST OID.2.16.724.1.3.5.7.2.11

ACCV is using the OIDs recommended by the corresponding Ministry..

7.1.6 Name constraints

The names that are contained in the certificates are restricted to distinguished names X.500, unique and unambiguous.

7.1.7 Certification Policy object identifier (OID)

The object identifier that is defined by the ACCV for identifying the current policy is the following:

1.3.6.1.4.1.8149.3.13.6.0

In this case an OID is added for identifying the type of certificate according to the profiles or the Ministry

2.16.724.1.3.5.7.2 Public employee certificate of medium level

In this case an OID is added for identifying the type of entity that is represented according to the ETSI TS 119 411-2 normative.

0.4.0.194112.1.0 Certification Policy for EU qualified certificates that are issued for natural persons

7.1.8 Usage of Policy Constraints extension

The *Policy Constraint* extension is not used in the certificates issued under this Certification Policy.

7.1.9 Policy qualifiers syntax and semantics

The Certificate Policies extension can include two Policy Qualifier fields (both optional):

CPS Pointer: contains the URL where the Certification Policies is published

User notice: contains a description text

7.1.10 Processing semantics for the critical Certificate Policies extension

The extension “Certificate Policy” identifies the policy which defines the practices that the ACCV explicitly associates with the certificate. In addition the extension can contain a policy qualifier.

7.2 CRL profile

7.2.1 Version number (s)

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

7.2.2 CRL and CRL entry extensions

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

7.3 OCSP Profile

7.3.1 Version number(s)

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

7.3.2 OCSP extensions

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

8 Compliance audit and other assessments

8.1 Frequency or circumstances of assessment

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

8.2 Identity/qualifications of assessor

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

8.3 Assessor's relationship to assessed entity

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

8.4 Topics covered by assessment

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

8.5 Actions taken as a result of deficiency

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

8.6 Communication of results

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9 Other business and legal matters

9.1 Fees

9.1.1 Certificate issuance or renewal fees

The fees for the initial issuance and certificates renovation are collected in the Agencia de Tecnología y Certificación Electrónica Fees List. This list is disclosed in the ACCV web page https://www.accv.es.

9.1.2 Certificate access fees

The access to the certificates issued within this certification policy is free and therefore there is no applicable fee over it.

9.1.3 Revocation or status information access fees

The access to the status or revocation information of the certificates is free and therefore, the is no applicable fee over it.

9.1.4 Fees for other services

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.1.5 Refund policy

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.2 Financial responsibility

9.2.1 Insurance coverage

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.2.2 Other assets

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.2.3 Insurance or warranty coverage for end-entities

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.3.2 Information not within the scope of confidential information

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.3.3 Responsibility to protect confidential information

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.4 Privacy of personal information

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.4.1 Privacy plan

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.4.2 Information treated as private

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.4.3 Information not deemed private

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.4.4 Responsibility to protect private information

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.4.5 Notice and consent to use private information

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.4.6 Disclosure pursuant to judicial or administrative process

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.4.7 Other information disclosure circumstances

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.5 Intellectual property rights

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.6 Representations and warranties

9.6.1 CA representations and warranties

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.6.2 RA representations and warranties

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.6.3 Subscriber representations and warranties
According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.6.4 Relying party representations and warranties
According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.6.5 Representations and warranties of other participants
According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.7 Disclaimers of warranties
As specified in the Certification Practices Statement (CPS) of the ACCV.

9.8 Limitations of liability

9.8.1 Warranties and its limitations
According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.8.2 Demarcation of responsibilities
According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.8.3 Loss limitations
According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.9 Indemnities
According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.10 Term and termination

9.10.1 Term
According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.10.2 Termination
According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.10.3 Effect of termination and survival
According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.11 Individual notices and communications with participants
According to the specified in the Certification Practices Statement (CPS) of the ACCV.

All the emails that the ACCV sends to the subscribers of the certificates issued within this Certification Policy, in the exercise of providing certification service, will be digitally signed for guaranteeing its authenticity and integrity.

9.12 Amendments

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.12.1 Procedure for amendment

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.12.2 Notification mechanism and period

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.12.3 Circumstances under which OID must be changed

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.13 Dispute resolution provisions

9.13.1 Resolution of off-court conflicts

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.13.2 Competent jurisdiction

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.14 Governing law

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.15 Compliance with applicable law

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.16.2 Assignment

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

9.16.3 Severability

According to the specified in the Certification Practices Statement (CPS) of the ACCV.

10 Annex I

CERTIFICATION CONTRACT – OID 1.3.6.1.4.1.8149.3.13

Section 1 –*Subscriber data*
Surname:
Name:
DNI/NIF: Tel.:
Occupation or position:
Organizational unit – Department:
Administration - Organization:
CIF of the Organization:

Electronic mail address:

Post address:

PIN : Tel. support **902 482 481** **www.accv.es**

Section 2 – Data of the Operator of the Register Point of Public Employee Certificates
Name and Surname:

Section 3 – *Date and Signature*

I subscribe the current certification contract associated to the Certification Policy for Qualified Certificates in qualified electronic signature creation device for Public Employees with OID 1.3.6.1.4.1.8149.3.13, issued by the la Agencia de Tecnología y Certificación Electrónica. I declare I know and accept the rules of use of this type of certificates that are exposed at http://www.accv.es Likewise, I declare that the exposed data is correct.

Subscriber signature *Signature and stamp of the Registration Point*

Signed: Signed*:*

Copy for the subscriber - Front

CERTIFICATION CONTRACT – OID 1.3.6.1.4.1.8149.3.13

Conditions for the use

1.The certificates that are associated to the Certification Policy for Qualified Certificates in qualified electronic signature creation device for Public Employees, issued by the Agencia de Tecnología y Certificación Electrónica are X.509v3 type and they follow the Certification Practices Statement of the Agencia de Tecnología y Certificación Electrónica, as Qualified Certification Services Provider and the mentioned Certification Policy. Both documents must be considered in accordance with the European Community law, Spanish Legal Framework and the Generalitat legislation.

2.The applicant must be natural persons, with a NIF, NIE or other valid identification document in force, and also must be employee of a Public Administration.

3.The user designated by the Administration for the management of public employee certificates, is responsible for the veracity of the submitted data along the request and register process. This user will be responsible for communicating any change of data.

4.The subscriber is responsible for the custody of the signature creation data, and for communicating as soon as possible about any loss or subtraction of this data.

5.The subscriber is responsible for restricting the certificate usage to what is established in the regarding Certification Policy, which is a public document and it can be found at http://www.accv.es

6.The Agencia de Tecnología y Certificación Electrónica is not responsible for the content of the documents that are signed using the issued certificates.

7.The Agencia de Tecnología y Certificación Electrónica is responsible for the accomplishment of the European, Spanish and Valencian legislation, as far as the electronic signature is concerned. Therefore it is responsible for the accomplishment of the established in the Certification Practices Statement of the Agencia de Tecnología y Certificación Electrónica and in the associated Certification Policy.

8.The validity period of these certificates is for three (3) years. The renewal uses the same process as for the first request or the procedures that are provided in the associated Certification Policy.

9.The issued certificates will lose their validity, in addition to the end of the official period of validity, when a revocation is produced, when the signature creation data store is broken, because of a judicial or administrative resolution that orders the validity loss, because of errors in the submitted data by the applicant or because of the subscriber decease. Other conditions for the validity loss are collected in the Certification Practices Statement and in the Certification Policy that is associated to this type of certificate.

10.The documentation that must be submitted for the applicant identification will be the Identity National Document, NIE or Spanish Passport, all of them valid and in force.

11.In accomplishment with the Organic Law 3/2018 December 5, of Personal Data Protection, the applicant is informed about the existence of an automated file of personal data, created under the responsibility of the Agencia de Tecnología y Certificación Electrónica. The purpose of this file is to serve to the uses related to the certification services that the Agencia de Tecnología y Certificación Electrónica provides. The subscriber expressly authorizes his/her personal data usage that the file contains, as far as necessary for carrying out the provided actions in the Certification Policy.

12.The Agencia de Tecnología y Certificación Electrónica is compromised to provide all the available means with the purpose of avoiding the manipulation, loss or non-authorized access to the personal data that is contained in the file.

13.The applicant can exercise his/her rights of access, rectification, cancellation, portability, restriction of processing and object to processing over his/her personal data, sending a written notification to the Agencia de Tecnología y Certificación Electrónica, through any Register Entry of the Generalitat and clearly indicating this willingness.

14.The subscriber is recommended to change the initial PIN that appears in the current contract with the use of tools provided by the Agencia de Tecnología y Certificación Electrónica.

With the signature of the current document the Agencia de Tecnología y Certificación Electrónica is authorized to consult the identification data that is collected in the Interior Ministry, avoiding the citizen to submit a copy of his/her identification document.

Copy for the subscriber - Reverse

CERTIFICATION CONTRACT – OID 1.3.6.1.4.1.8149.3.13

Section 1 –*Subscriber data*

Surname:
Name:
DNI/NIF: Tel.:
Occupation or position:
Organizational unit – Department:
Administration - Organization:
CIF of the Organization:

Electronic mail address:

Post address:

Section 2 – Data of the Operator of the Register Point of Public Employee Certificates

Name and Surname:

Section 3 – *Date and Signature*

I subscribe the current certification contract associated to the Certification Policy for Qualified Certificates in qualified electronic signature creation device for Public Employees with OID 1.3.6.1.4.1.8149.3.13, issued by the la Agencia de Tecnología y Certificación Electrónica. I declare I know and accept the rules of use of this type of certificates that are exposed at http://www.accv.es Likewise, I declare that the exposed data is correct.

Subscriber Signature *Signature and stamp of the Register Point*

Signed: Signed*:*

Nº of request Copy for the ACCV

11 Annex II – Certificate revocation request form

CERTIFICATE REVOCATION REQUEST

V3.0

Date:.....

Section 1 – Certificate's subscriber data
Section 1 –*Subscriber data*
Surname:
Name:
DNI/NIF: Tel.:
Occupation or position:
Organizational unit – Department:
Administration - Organization:
CIF of the Organization:

Section 2 – Certificate identification*
Personal certificate: Certificate request number:

Section 3 – Revocation reason*

* The simple will of revocation by the certificate subscriber or its applicant is a valid reason for this request.

Section 4 – Authorization*
Subscriber of the certificate

Signature

Requested to the operator of the User Register Point:

Signature:

Copy for the Agencia de Tecnología y Certificación Electrónica

CERTIFICATE REVOCATION REQUEST

V3.0

Date:.....

Section 1 – Subscriber data
Surname:
Name:
DNI/NIF:
Occupation or position:
Organizational unit - Department:
Administration - Organization:
CIF of the Organization:

Section 2 – Certificate identification*
Personal certificate: Certificate's request number:

Section 3 – Revocation reason*

* The simple will of revocation by the certificate subscriber or its applicant is a valid reason for this request.

Section 4 – Authorization*
Certificate's subscriber

Signature

Requested to the operator of the User Register Point:

Signature:

Copy for the applicant

12 Annex III – Entity register request form

Autoritat de Certificació de la Comunitat Valenciana

ALTA ORGANITZACIÓ / *ALTA ORGANIZACIÓN*

A DADES DE LA ORGANITZACIÓ / *DATOS DE LA ORGANIZACIÓN*

NOM DE L'ORGANISME / *NOMBRE DEL ORGANISMO*	CIF
NOM DEL DEPARTAMENT / *NOMBRE DEL DEPARTAMENTO*	
ADREÇA FISCAL / *DOMICILIO FISCAL*	CP

LOCALITAT / *LOCALIDAD*	PROVINCIA / *PROVINCIA*	TELÉFON / *TELEFONO*	FAX

ADREÇA ELECTRÒNICA/ *CORREO ELECTRÓNICO*

B DADES DEL PERSONAL RESPONSABLE / *DATOS DEL PERSONAL RESPONSABLE*

Persones responsables per a la petició dels certificats d' Empleat Públic. Estes persones s'encarregaran de la sol·licitud d'alta, entrega i revocació dels certificats d' Empleat Públic. A més, estes persones es comprometen a informar els usuaris de les seues obligacions i responsabilitats. La responsabilitat de la remisió dels contractes de certificació a l' ACCV recau en l'Organisme sol·licitant.
Els certificats d' Empleat Públic estan definits en la Política de Certificació de Certificats Reconeguts d'empleat públic, disponible en www.accv.es .
/ Personas responsables para la petición de los certificados de Empleado Público. Estas personas se encargaran de la solicitud de alta, entrega y revocación de los certificados de Empleado Público. Además, estas personas se comprometen a informar a los usuarios de sus obligaciones y responsabilidades. La responsabilidad de la remisión de los contratos de certificación a la ACCV recae en el Organismo solicitante.
Los certificados de Empleado Público están definidos en la Política de Certificación de Certificados Reconocidos de empleado público, disponible en www.accv.es .

NOM / *NOMBRE*	COGNOMS / *APELLIDOS*	NIF / NIE	ADREÇA ELECTRÒNICA / *CORREO ELECTRÓNICO*	CÀRREC / CARGO

C MOTIU DE LA PETICIÓ / *MOTIVO DE LA PETICIÓN*

☐ Creació inicial / *Creación inicial.*

☐ Modificació de dades / *Modificación de datos.*

_____, ____ d _____ de _____

Firma del declarant / *Firma del declarante*

Firma del responsable de l'ACCV / *Firma del responsable de la ACCV*

Firma: _____ Firma: _____