Agencia de Tecnología y Certificación Electrónica

Certification Policy for Qualified Certificates in qualified electronic signature creation device for citizens

Date: 20/01/2020	**Version:** 7.0.4
Status: APPROVED	**Nº of pages:** 44
OID: 1.3.6.1.4.1.8149.3.6.7.0	**Classification: PUBLIC**
File: ACCV-CP-06V7.0.4-EN-2020.doc	
Prepared by: Agencia de Tecnología y Certificación Electrónica - ACCV	

ISTEC Firmado digitalmente por ISTEC
Fecha: 2020.07.03 11:32:58 +02'00'

Changelog

Version	Author	Date	Observations
7.0.1	ACCV	03/05/2018	RFC3647 Changes
7.0.2	ACCV	18/06/2019	CAB/Forum modification
7.0.3	ACCV	20/01/2020	Mail validation modification
7.0.4	ACCV	10/03/2020	RFC3647 Changes

Table of Content

1 INTRODUCTION

1.1 Overview

The current document is the Certification Policy associated to the qualified certificates for citizens in qualified electronic signature creation device, 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 Agencia de Tecnología y Certificación Electrónica, 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 citizens, in a qualified electronic signature creation device -smart card-. With the qualified certificates and qualified electronic signature creation devices that are associated to this Certification Policy, qualified electronic signatures will be generated.

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 of Qualified Certificates in qualified electronic signature creation device for citizens
Policy qualifier	`Certificado cualificado para Ciudadano expedido por la ACCV (Plaza Nápoles y Sicilia, 6. Valencia CP 46003, ESPAÑA. CIF A40573396)`
Policy version	7.0.4
Policy status	APPROVED
Policy Reference / OID (Object Identifier)	1.3.6.1.4.1.8149.3.6.7.0
Date of issuance	20 January 2020
Date of expiration	Not applicable
Related CPS	Certification Practices Statement (CPS) of the ACCV. Version 4.0. OID: 1.3.6.1.4.1.8149.2.4.0 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 ACCVCA-120 which belongs to the Agencia de Tecnología y Certificación Electrónica, which purpose is to issue end entity certificates for the ACCV subscribers. The certificate of ACCVCA-120 is valid since 13 October 2011 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 located at https://www.accv.es.

1.3.3 Subscribers

The group of users who can apply for the certificates that are defined in this policy is exclusively limited to any natural person in possession of the identification elements that are required (DNI, NIE, etc.).

The storage of the keys and certificates is the Giesecke & Devrient (G&D) Sm@rtCafé Expert 3.2 cryptographic card and its subsequent versions. In case of accrediting another qualified electronic signature creation device, this will be included in this document, at point 6.1.8 Keys hardware/software generation.

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 users of S/MIME electronic mail clients in the scope of the identity verification of the issuer of the electronic mail messages and its encryption.
- 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

In addition to what is specified in the Certification Practices Statement (CPS), ACCV conforms to the current version of the *"Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates"* and the current version of the *"Guidelines for Issuance and Management of Extended Validation Certificates"*, published at https://www.cabforum.org/.In the event of any inconsistency between this Certification Policy and the CAB Forum requirements, those requirements take precedence over the current 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 natural persons. Certification requests performed in name of legal bodies, entities or organization will not be accepted. Therefore, any organization identification will not be necessary.

3.2.3 Authentication of individual identity

Authentication of the identity of the applicant for a certificate will be done by identification with the corresponding Registration Authority. In the case of presenting on site with a Registration Point Operator enabled for the issuance of this type of certificate, the identity must be accredited by presenting the National Identity Document (DNI), Spanish passport, the Foreigner Identification Number (NIE) of the applicant or other means admitted in Law. The presenting on site of the applicant may be dispensed using a power of attorney explicitly delegating the obtaining of the certificate to third party. In the case of remote identification with the Registration Authority, the applicant will access the Personal Certification Services Area (APSC) by identifying himself through a qualified personal certificate of the ACCV or the DNIe.

In this type of certificates the subscriber electronic mail address is included as a necessary element to support the S/MIME protocol. To verify this email account, ACCV will send an email to that account with a unique web link. The applicant must click on this link to confirm the address and thus be able to continue with the generation process. This unique web link will expired in 30 days without possibility of reuse.

3.2.4 Non-verified subscriber information

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

3.2.5 Validation of authority

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

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.

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

The identification and authentication policy for certificate renewal following a revocation without key compromise shall be the same as for initial registration. In the case of finding insurmountable technical problems, ACCV can implement any method that guarantees in a reliable and unequivocal way the applicant identity and the application authentication, explaining in detail each step of the process.

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 at point 3.2.3. *Authentication of an individual identification*, in this Certification Policy.
- Web. Using the Personal Area of the Certification Services (APSC) at http://www.accv.es.
- Phone. 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 a certificate revocation if they have knowledge or suspect about the subscriber private key compromise, or any other fact that would recommended to carry this action out.

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

Those subscribers listed in point 1.3.3 can submit a certificate application.

4.1.2 Enrollment Process and Responsibilities

The citizen applying for a certificate issued under this policy must go to the ACCV's Registration Authority, presenting the necessary documentation established in this policy (point 3.2.3).

The list of authorized Registration Authorities is located at https://www.accv.es.

In the case of on-site applications, the application data is obtained from official documentation provided by 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 statuses through which the application passes. It is the applicant's responsibility to provide accurate information in their application.

In the case of remote applications the data is obtained from the information available in the digital medium 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 statuses through which the application passes. It is the applicant's responsibility to provide accurate information in their application.

Likewise in case of certificate request through remote means, a period of time lower than five years will be demanded since the on-site identification.

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

4.2 Certificate application processing

The Registration Authority is the entity competence in charge of checking the applicant identity, to verify the documentation and validate that the applicant has signed the certification contract. Once the request is completed, the Registration Authority will remit it to ACCV.

4.2.1 Performing identification and authentication functions

Authentication of the identity of the applicant for a certificate will be done by identification with the corresponding Registration Authority using the mechanisms described in section 3.2.3 Authentication of individual identity. Registration Authority Operator checks the documentation and validates the data using publicly accessible records for such verification. In the case of the email address, a validation mechanism is established by sending a unique link to this address, blocking the request until confirmation is carried out.

4.2.2 Approval or rejection of certificate applications

In case of acceptance, Registration Authority will notify the applicant through an email digitally signed to the email address that is listed in the request. Before accepting the application, the applicant must have validated the e-mail address.

In onsite applications, Registration Authority will inform the user of acceptance or rejection directly.

In remote applications the applicant must access the Personal Area of Certification Services (remote Registration Authority) with a personal certificate or the DNIe. If the applicant is able to make the application, the corresponding option will be shown.

In case of rejection the Registration Authority will inform the applicant using the corresponding mechanisms. For on-site applications the Operator shall inform the user directly of the rejection and the reason for it, interrupting the process at that time and canceling the application on the platform. In remote applications the Registration Authority will inform the user in an interactive way preventing the continuation of the process.

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 and in the presence of the applicant. 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 RA 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 certificate issuance takes place once the RA has carried out the necessary verification for validating the certification request. The mechanism that determines the nature and form of performing these checks is this Certification Policy.

In on-site applications the steps are as follows:

- RA uses the data entered by the Operator at the point of on-site registration.

- RA check personal data input

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

- RA sends the signed CSR to the CA

- CA performs a verification of the RA signature and confirms that the form of the CSR is correct

- CA signs the CSR sending it back to the RA

- RA communicates the certificate to the applicant.

In remote applications the steps are as follows:

- Applicant has identified himself with a ACCV qualified certificate or with the DNIe and the personal data associated with the application are extracted from the fields of the certificate.

- Applicant can change the mailing address but both in the case of using the same or changing it will be validated using a unique link sent to that address.

- RA check the personal data input by the applicant in the enrollment URL.

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

- RA sends the signed CSR to the CA

- CA performs a verification of the RA signature and confirms that the form of the CSR is correct

- CA signs the CSR sending it back to the RA

- RA 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 a signed 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 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 Certification Contract is a document that must be accepted by the applicant, and which purpose is to link the person who applies for the website authentication certificate, and the knowledge of usage rules and the submitted data veracity. The Certification Contract form is collected in the Annex I of this 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

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

The certificate renewal must be carried out using the same procedures and identification methods that the initial application.

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.

4.9.3 Procedure for revocation request

The Agencia de Tecnología y Certificación Electrónica accepts revocation requests by the following methods:

4.9.3.1 Face-to-face processing

By the subscriber appearance and identification in a RA and by signing and filling the “Revocation Request Form” that will be provided to him/her and which copy is included in the Annex II of this document.

4.9.3.2 Telematic

There exists a certificate revocation request form at the ACCV web, at http://www.accv.es URL.

4.9.3.3 Phone

Through a phone call to the phone support number of the Agencia de Tecnología y Certificación Electrónica, which is 902482481.

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

In addition to consulting revoked certificates through Certificate Revocation Lists (CRL) and by the OCSP service, it is also possible to check their validity by a web form, which with the citizen identifier (DNIe or NIE), prints out the certificates that fit with this criteria and also, their status. This form can be found at the http://www.accv.es URL.

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 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, through a digitally signed email in a previous moment prior to the certificate disclosure in the Certificate Revocation List, specifying the reasons, date and time the certificate will lose its efficacy and notifying about its non-continuing usage.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

ACCV escrows the encryption keys for enabling the encrypted information recovery in case of losing the necessary keys for its decryption, in case of the holder legal interest or because of a judicial requirement.

The recovery of the encryption keys can be carried out by the subscriber through the Personal Area of the Certification Services at https://www.accv.es, where his/her certificate can be downloaded after an identification based in the authentication certificate and signature.

The Judicial Authority must address a requirement to the Agencia de Tecnología y Certificación Electrónica with the contact data included in the chapter 1.5.1 of this document.

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

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

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.

5.2.4 Roles requiring separation of duties

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

5.3 Personnel controls

This chapter reflects the content of the *Personal 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
According to the specified in the Certification Practices Statement (CPS) of ACCV.

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 sizes for the certificates that are issued under the scope of this Certification Policy is 2048 bits of length at least.

6.1.6 Public key parameters generation and quality checking

The parameters that are defined in the cryptography suite *sha256-with-rsa* which is specified in the ETSI TS 119 312 “Electronic Signatures and Infrastructures (ESI); Cryptographic Suites” document, are used. ModLen=2048 is defined.

Signature suite entry name	Signature algorithm	Signature algorithm parameters	Key generation algorithm	Padding method	Cryptographic hash function
sha256-with-rsa	RSA-PKCSv1_5	MinModLen=2048	rsagen1	emsa-pkcs1-v1_5	SHA-256

6.1.7 Parameters quality checking

The parameters that are defined in the cryptography suite *sha256-with-rsa* which is specified in the ETSI TS 119 312 “Electronic Signatures and Infrastructures (ESI); Cryptographic Suites” document, are used. ModLen=2048 is defined.

Signature suite entry	Signature algorithm	Signature algorithm	Key generation algorithm	Padding method	Cryptographic hash function

name		parameters			
Sha-256-with-rsa	rsa	MinModLen=2048	rsagen1	emsa-pkcs1-v1_5	sha256

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.

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 3.2 72K FIPS 140-2 Level 2

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 escrows the encryption keys for enabling the encrypted information recovery in case of losing the necessary keys for its decryption, in case of the legal interest or because of a judicial requirement.

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

6.2.4 Private key backup

ACCV backups the encryption keys for enabling the encrypted information recovery in case of losing the necessary keys for its decryption, in case of the legal interest or because of a judicial requirement.

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

6.2.5 Private key archival

ACCV stores the encryption keys for enabling the encrypted information recovery in case of losing the necessary keys for its decryption, in case of the legal interest or because of a judicial requirement.

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 signature certificate, is performed into the signature creation device by its own cryptographic chip and they never leave it.

The generation of keys linked to the certificate of encryption and the import into the subscriber signature creation device is carried out with the Certification Authority software.

6.2.7 Private key storage on cryptographic module

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

The generation of keys linked to the certificate of encryption and the import into the subscriber signature creation device is carried out with the Certification Authority software.

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 ACCVCA-120 certificate is valid since 13 October 2011 until 1 January 2027.

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.

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

6.5.1 Specific computer security technical requirements

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

6.5.2 Computer security rating

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

6.6 Life Cycle Security Controls

6.6.1 System development controls

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

6.6.2 Security management controls

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

6.6.3 Life cycle security controls

According to the specified in the Certification Practices Statement (CPS) of 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 two different certificates; one of them for the digital signature and the subscriber authentication, and the other certificate for data encryption. The profile of both certificates is the same excepting the key usages, as it is indicated in the chapter 7.1.2 *Certificate extensions* of this Policy.

7.1.2 Certificate extensions

The extensions that are used by the certificates that are issued within the scope of this 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	
CommonName	String composed in the following manner: NAME SURNAME1 SURNAME2 – NIF:SUBSCRIBERNIF	
OrganizationalUnit	Ciudadanos	
Organization	ACCV	
Country	ES	
Version	V3	
SerialNumber	Certificate unique identifier (32 hexadecimal characters)	
Signature algorithm	sha256withRSAEncryption	
Issuer (Emisor)		
CommonName	ACCVCA-120	
OrganizationalUnit	PKIACCV	
Organization	ACCV	
Country	ES	
Valid since	Date of Issuance	
Valid until	Date of Expiration	
Public Key	Octet String containing the subscriber public key	
Extended Key Usage		
	Client Authentication	
	Email Protection	
CRL Distribution Point	http://www.accv.es/fileadmin/Archivos/certificados/accvca120_der.crl	
SubjectAlternativeName		
RFC822Name	Subscriber electronic mail	

DirectoryName		
	CN=Name|Surname1|Surname2	
	UID=NIF	
Certificate Policy Extensions		
	QCP-n-qscd: certificate policy for EU qualified certificates issued to natural persons with private key related to the certified public key in a QSCD; Itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2)	
Policy OID	1.3.6.1.4.1.8149.3.6.7.0	
Policy CPS Location	http://www.accv.es/legislacion_c.htm*	
Policy Notice	Certificado cualificado para Ciudadano expedido por la ACCV (Plaza Nápoles y Sicilia, 6. Valencia CP 46003, ESPAÑA. CIF A40573396)	
Authority Information Access		
Access Method	Id-ad-ocsp	
Access Location	http://ocsp.accv.es	
Access Method	Id-ad-caIssuers	
Access Location	http://www.accv.es/gestcert/ACCVCA120SHA2.cacert.crt	
Fingerprint issuer	48 72 a4 c3 df 17 4c ef 34 d7 7f e6 a3 b4 e7 be 7d f2 d2 5d	
Hash Algorithm	SHA-256	
KeyUsage (critic)		
Certificate of signature	Digital Signature Non-repudiation	
Certificate of encryption	Key Encipherment Data Encipherment	
QcStatement (sólo cert. de firma)	**Campos QC (Qualified Certificate)**	**QcStatement**
QcCompliance		The certificate is qualified
QcType	eSign	Particular type of qualified certificate
QcSSCD		The private key is located in a qualified electronic signature creation device
QcRetentionPeriod	15y	Retention period of the material information
QcPDS	https://www.accv.es/fileadmin/Archivos/Practicas_de_certificacion/ACCV-PDS-	PKI Disclosure Statement location

	V1.0-EN.pdf	

** The existence of valid certificates that were issued with the pki.gva.es URL instead of accv.es must be excluded. The change of one URL by another is a gradual process which does not involve significant differences in the certificate profile neither the its functionality or usage.*

7.1.3 Algorithms object identifiers (OID)

Object Identifiers (OID) of the Cryptography algorithms:

- SHA1withRSA (1.2.840.113549.1.1.5)
- SHA256withRSA (1.2.840.113549.1.1.11)

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.

All the fields of the certificate of the Subject and the Subject Alternative Name, excepting those that regard DNS name or mail addresses, are obligatory filled with capital letters and without accents.

7.1.5 Name constraints

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

The rest of fields included in the certificate are strictly necessary and are marked in the RFC-3739 for the obtainment of a qualified certificate profile.

7.1.6 Certification Policy object identifier (OID)

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

1.3.6.1.4.1.8149.3.6.7.0

The OID for identifying the type of entity represented in accordance with the ETSI TS 119 411-2 normative is:

0.4.0.194112.1.2 Certification Policy for EU qualified certificates in qualified electronic signature creation device issued to natural persons

7.1.7 Usage of Policy Constraints extension

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

7.1.8 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

7.1.9 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 bussiness 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

According to the 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.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

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

9.16.5 Force Majeure

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

9.17 Other provisions

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

10 Annex I

CERTIFICATION CONTRACT – OID 1.3.6.1.4.1.8149.3.6		
Section 1 – Subscriber data Surname: Name: DNI/NIF: Tel.: Electronic mail address: Post address:		
PIN :	Tel. support: **902 482 481**	**www.accv.es**
Section 2 – Data of the Registration Point Operator Name and surname:		
Section 3 – Date and Signature *I subscribe the current certification contract that is associated to the Certification Policy of Qualified Certificates in qualified electronic signature creation device for Citizens with the OID 1.3.6.1.4.1.8149.3.6, issued by the 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 Signed:	Signature and stamp of the Registration Point Signed*:*	

Copy for the subscriber - Front

CERTIFICATION CONTRACT – OID 1.3.6.1.4.1.8149.3.6

Conditions of use

1. The certificates that are associated to the Certification Policy for Qualified Certificates in qualified electronic signature creation device for Citizens, 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 interpreted in accordance with the European law, the Spanish Juridic Order and the Valencian legislation.

2. The applicant must be a natural person, with a NIF, NIE or another valid identification document in force.

3. The applicant is responsible for the veracity of all the data provided in the registration process. He/she will be responsible for communicating any change in the submitted data.

4. The subscriber is 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 electronic signature is concerned. Therefore it is responsible for the accomplishment of what is established in the Certification Practices Statement of the Agencia de Tecnología y Certificación Electrónica and in the Certification Policy that is associated to this type of certificates.

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 to be submitted for the applicant identification will be the Identity National Document, NIE or Spanish passport, 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 committed to provide all the necessary means for 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 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.

15. The Agencia de Tecnología y Certificación Electrónica has constituted an insurance coverage for an amount of three millions euros (3.000.000,00 €) to cover the risk of liability for damages that may occur with the use of the issued certificates and the digital certification services.

With the signature of this document, the Agencia de Tecnología y Certificación Electrónica is authorized to consult the identity data that is stated in the Interior Ministry, avoiding on this manner the citizen to submit his/her identity document copy.

Copy for the subscriber - Reverse

CERTIFICATION CONTRACT – OID 1.3.6.1.4.1.8149.3.6

Section – Subscriber data
Surname:
Name:
DNI/NIF: Tel.:

Electronic mail address:

Post address:

Section 2 – Data of the Registration Point Operator
Name and surname:

Section 3 – Date and Signature
I subscribe the current certification contract that is associated to the Certification Policy of Qualified Certificates in qualified electronic signature creation device for Citizens with the OID 1.3.6.1.4.1.8149.3.6, issued by the 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:

Nº of request Copy for the ACCV

11 Annex II – Certificate revocation request form

CERTIFICATE REVOCATION REQUEST V3.0
Date:.....
Section 1 – Subscriber data Surname: Name: DNI/NIF:
Section 2 – Certificate identification* Personal Certificate: Nº of the certificate request:
Section 3 – Revocation reason* * The will to revocation of the certificate subscriber is a valid reason for this request.
Section 4 – Authorization* Certificate subscriber *Signature* Registration Point Operator: Signature:

Copy for the ACCV

CERTIFICATE REVOCATION REQUEST

V3.0

Date:.....

Section 1 – Subscriber data
Surname:
Name:
DNI/NIF:

Section 2 – Certificate identification*
Personal Certificate: Nº of the certificate request:

Section 3 – Revocation reason*

* The will to revocation of the certificate subscriber is a valid reason for this request.

Section 4 – Authorization*
Certificate subscriber

Signature

Registration Point Operator:

Signature:

Copy for the applicant