



Agencia de Tecnología y Certificación Electrónica

Certification Policy for Qualified Certificates based on software for citizens

Date: 20/01/2020	Version: 6.0.3
Status: APPROVED	Number of pages: 45
OID: 1.3.6.1.4.1.8149.3.7.6.0	Classification: PUBLIC
File: ACCV-CP-07V6.0.3-EN-2020.odt	
Prepared by: Agencia de Tecnología y Certificación Electrónica - ACCV	



Changelog

Version	Author	Date	Observations
6.0.1	ACCV	18/06/2019	RFC3647 Changes
6.0.2	ACCV	20/01/2020	CAB/Forum modification
6.0.3	ACCV	02/03/2020	RFC3647 Changes

Table of Content

1. INTRODUCTION.....	11
1.1. OVERVIEW.....	11
1.2. IDENTIFICATION.....	11
1.3. PKI PARTICIPANTS.....	11
1.3.1. Certification Authorities.....	11
1.3.2. Registration Authorities.....	12
1.3.3. Subscribers.....	12
1.3.4. Relying parts.....	12
1.3.5. Other participants.....	12
1.4. CERTIFICATES USAGE.....	12
1.4.1. Appropriate certificate uses.....	12
1.4.2. Prohibited certificate uses.....	12
1.5. POLICY ADMINISTRATION.....	12
1.5.1. Organization administering the document.....	12
1.5.2. Contact person.....	13
1.5.3. Person determining CPS suitability for the policy.....	13
1.5.4. CPS approval procedures.....	13
1.6. DEFINITIONS AND ACRONYMS.....	13
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES.....	14
2.1. REPOSITORIES.....	14
2.2. PUBLICATION OF CERTIFICATION INFORMATION.....	14
2.3. TIME OR FREQUENCY OF PUBLICATION.....	14
2.4. ACCESS CONTROLS ON REPOSITORIES.....	14
3. IDENTIFICATION AND AUTHENTICATION.....	15
3.1. NAMING.....	15
3.1.1. Types of names.....	15
3.1.2. Need for names to be meaningful.....	15
3.1.3. Anonymity or pseudonymity of subscribers.....	15
3.1.4. Rules for interpreting various name forms.....	15
3.1.5. Uniqueness of names.....	15
3.1.6. Recognition, authentication, and role of trademarks.....	15
3.2. INITIAL IDENTITY VALIDATION.....	15
3.2.1. Method to prove possession of private key.....	15
3.2.2. Authentication of organization identity.....	15
3.2.3. Authentication of individual identity.....	15
3.2.4. Non-verified subscriber information.....	16



3.2.5. Validation of authority.....	16
3.2.6. Criteria for interoperation.....	16
3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS.....	16
3.3.1. Identification and authentication for routine re-key.....	16
3.3.2. Identification and authentication for re-key after revocation – Not compromised key.....	16
3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST.....	16
4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS.....	17
4.1. CERTIFICATES APPLICATION.....	17
4.1.1. Who can submit a certificate application.....	17
4.1.2. Enrollment Process and Responsibilities.....	17
4.2. CERTIFICATE APPLICATION PROCESSING.....	17
4.2.1. Performing identification and authentication functions.....	17
4.2.2. Approval or rejection of certificate applications.....	17
4.2.3. Time to process certificate applications.....	18
4.3. CERTIFICATES ISSUANCE.....	18
4.3.1. CA actions during certificate issuance.....	18
4.3.2. Notification to subscriber by the CA of issuance of certificate.....	19
4.4. CERTIFICATES ACCEPTANCE.....	19
4.4.1. Conduct constituting certificate acceptance.....	19
4.4.2. Publication of the certificate by the CA.....	19
4.4.3. Notification of certificate issuance by the CA to other entities.....	19
4.5. KEY PAIR AND CERTIFICATE USAGE.....	19
4.5.1. Subscriber private key and certificate usage.....	19
4.5.2. Relying party public key and certificate usage.....	19
4.6. CERTIFICATE RENEWAL.....	19
4.6.1. Circumstance for certificate renewal.....	20
4.6.2. Who may request renewal.....	20
4.6.3. Processing certificate renewal requests.....	20
4.6.4. Notification of new certificate issuance to subscriber.....	20
4.6.5. Conduct constituting acceptance of a renewal certificate.....	20
4.6.6. Publication of the renewal certificate by the CA.....	20
4.6.7. Notification of certificate issuance by the CA to other entities.....	20
4.7. CERTIFICATE RE-KEY.....	20
4.7.1. Circumstance for certificate re-key.....	20
4.7.2. Who may request certification of a new public key.....	20
4.7.3. Processing certificate re-keying requests.....	20
4.7.4. Notification of new certificate issuance to subscriber.....	20
4.7.5. Conduct constituting acceptance of a re-keyed certificate.....	20



4.7.6. Publication of the re-keyed certificate by the CA.....	20
4.7.7. Notification of certificate issuance by the CA to other entities.....	21
4.8. CERTIFICATE MODIFICATION.....	21
4.8.1. Circumstance for certificate modification.....	21
4.8.2. Who may request certificate modification.....	21
4.8.3. Circumstance for certificate modification.....	21
4.8.4. Notification of new certificate issuance to subscriber.....	21
4.8.5. Conduct constituting acceptance of modified certificate.....	21
4.8.6. Publication of the modified certificate by the CA.....	21
4.8.7. Notification of certificate issuance by the CA to other entities.....	21
4.9. CERTIFICATE REVOCATION AND SUSPENSION.....	21
4.9.1. Circumstances for revocation.....	21
4.9.2. Who can request revocation.....	21
4.9.3. Procedure for revocation request.....	21
4.9.4. Revocation request grace period.....	22
4.9.5. Time within which CA must process the revocation request.....	22
4.9.6. Revocation checking requirement for relying parties.....	22
4.9.7. CRL issuance frequency.....	22
4.9.8. Maximum latency for CRLs.....	22
4.9.9. On-line revocation/status checking availability.....	22
4.9.10. On-line revocation checking requirements.....	22
4.9.11. Other forms of revocation advertisements available.....	22
4.9.12. Special requirements re key compromise.....	22
4.9.13. Circumstances for the suspension.....	22
4.9.14. Who can request suspension.....	22
4.9.15. Procedure for the suspension request.....	23
4.9.16. Limits of suspension period.....	23
4.10. CERTIFICATE STATUS SERVICES.....	23
4.10.1. Operational Characteristics.....	23
4.10.2. Service Availability.....	23
4.10.3. Optional features.....	23
4.11. END OF SUBSCRIPTION.....	23
4.12. KEY ESCROW AND RECOVERY.....	23
4.12.1. Key escrow and recovery policy and practices.....	23
4.12.2. Session key encapsulation and recovery policy and practices.....	23
5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS.....	24
5.1. PHYSICAL CONTROLS.....	24
5.1.1. Site location and construction.....	24



5.1.2. Physical access.....	24
5.1.3. Power and air conditioning.....	24
5.1.4. Water exposure.....	24
5.1.5. Fire prevention and protection.....	24
5.1.6. Media storage.....	24
5.1.7. Waste disposal.....	24
5.1.8. Off-site backup.....	24
5.2. PROCEDURAL CONTROLS.....	24
5.2.1. Trusted roles.....	24
5.2.2. Number of persons that are required per task.....	24
5.2.3. Identification and authentication for each role.....	24
5.2.4. Roles requiring separation of duties.....	25
5.3. PERSONNEL CONTROLS.....	25
5.3.1. Qualifications, experience, and clearance requirements.....	25
5.3.2. Background check procedures.....	25
5.3.3. Training requirements.....	25
5.3.4. Retraining frequency and requirements.....	25
5.3.5. Job rotation frequency and sequence.....	25
5.3.6. Sanctions for unauthorized actions.....	25
5.3.7. Independent contractor requirements.....	25
5.3.8. Documentation supplied to personnel.....	25
5.3.9. Periodical compliance controls.....	25
5.3.10. End of contracts.....	25
5.4. AUDIT LOGGING PROCEDURES.....	25
5.4.1. Types of events recorded.....	25
5.4.2. Frequency of processing log.....	26
5.4.3. Retention period for audit log.....	26
5.4.4. Protection of audit log.....	26
5.4.5. Audit log backup procedures.....	26
5.4.6. Audit collection system (internal vs. external).....	26
5.4.7. Notification to event-causing subject.....	26
5.4.8. Vulnerability assessments.....	26
5.5. RECORDS ARCHIVAL.....	26
5.5.1. Types of records archived.....	26
5.5.2. Retention period for archive.....	26
5.5.3. Protection of archive.....	26
5.5.4. Archive backup procedures.....	26
5.5.5. Requirements for time-stamping of records.....	26
5.5.6. Archive collection system (internal or external).....	26



5.5.7. Procedures to obtain and verify archive information.....	26
5.6. KEY CHANGEOVER.....	27
5.7. COMPROMISE AND DISASTER RECOVERY.....	27
5.7.1. Incident and compromise handling procedures.....	27
5.7.2. Computing resources, software, and/or data are corrupted.....	27
5.7.3. Entity private key compromise procedures.....	27
5.7.4. Business continuity capabilities after a disaster.....	27
5.8. CA OR RA TERMINATION.....	27
6. TECHNICAL SECURITY CONTROLS.....	28
6.1. KEY PAIR GENERATION AND INSTALLATION.....	28
6.1.1. Key pair generation.....	28
6.1.2. Private key delivery to subscriber.....	28
6.1.3. Public key delivery to certificate issuer.....	28
6.1.4. CA public key delivery to relying parties.....	28
6.1.5. Key sizes.....	28
6.1.6. Public key parameters generation and quality checking.....	28
6.1.7. Parameters quality checking.....	29
6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS.....	29
6.2.1. Cryptographic module standards and controls.....	29
6.2.2. Private key (n out of m) multi-person control.....	29
6.2.3. Private key escrow.....	29
6.2.4. Private key backup.....	29
6.2.5. Private key archival.....	29
6.2.6. Private key transfer into or from a cryptographic module.....	29
6.2.7. Private key storage on cryptographic module.....	30
6.2.8. Method of activating private key.....	30
6.2.9. Method of deactivating private key.....	30
6.2.10. Private key destruction method.....	30
6.2.11. Cryptographic Module Rating.....	30
6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT.....	30
6.3.1. Public key file.....	30
6.3.2. Usage period for public and private keys.....	30
6.4. ACTIVATION DATA.....	30
6.4.1. Activation data generation and installation.....	30
6.4.2. Activation data protection.....	30
6.4.3. Other aspects of activation data.....	31
6.5. COMPUTER SECURITY CONTROLS.....	31
6.5.1. Specific computer security technical requirements.....	31

6.5.2. Computer security rating.....	31
6.6. LIFECYCLE TECHNICAL CONTROLS.....	31
6.6.1. System development controls.....	31
6.6.2. Security management controls.....	31
6.6.3. Life cycle security controls.....	31
6.7. NETWORK SECURITY CONTROLS.....	31
6.8. TIME-STAMPING.....	31
7. CERTIFICATE, CRL AND OCSP PROFILES.....	32
7.1. CERTIFICATE PROFILE.....	32
7.1.1. Version number(s).....	32
7.1.2. Certificate extensions.....	32
7.1.3. Algorithms object identifiers (OID).....	34
7.1.4. Name forms.....	34
7.1.5. Name constraints.....	34
7.1.6. Certification Policy object identifier (OID).....	34
7.1.7. Usage of Policy Constraints extension.....	34
7.1.8. Policy qualifiers syntax and semantics.....	34
7.1.9. Processing semantics for the critical Certificate Policies extension.....	34
7.2. CRL PROFILE.....	35
7.2.1. Version number (s).....	35
7.2.2. CRL and CRL entry extensions.....	35
7.3. OCSP PROFILE.....	35
7.3.1. Version number (s).....	35
7.3.2. OCSP Extensions.....	35
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS.....	36
8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT.....	36
8.2. IDENTIFICATION/QUALIFICATION OF ASSESSOR.....	36
8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY.....	36
8.4. TOPICS COVERED BY ASSESSMENT.....	36
8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY.....	36
8.6. COMMUNICATION OF RESULTS.....	36
8.7. SELF-AUDITS.....	36
9. OTHER BUSSINESS AND LEGAL MATTERS.....	37
9.1. FEES.....	37
9.1.1. Certificate issuance or renewal fees.....	37
9.1.2. Certificate access fees.....	37
9.1.3. Revocation or status information access fees.....	37



9.1.4. Fees of other services.....	37
9.1.5. Refund policy.....	37
9.2. FINANCIAL RESPONSIBILITY.....	37
9.2.1. Insurance coverage.....	37
9.2.2. Other assets.....	37
9.2.3. Insurance or warranty coverage for end-entities.....	37
9.3. CONFIDENTIALITY OF BUSINESS INFORMATION.....	37
9.3.1. Scope of confidential information.....	37
9.3.2. Information not within the scope of confidential information.....	37
9.3.3. Responsibility to protect confidential information.....	37
9.4. PRIVACY OF PERSONAL INFORMATION.....	38
9.4.1. Privacy plan.....	38
9.4.2. Information treated as private.....	38
9.4.3. Information not deemed private.....	38
9.4.4. Responsibility to protect private information.....	38
9.4.5. Notice and consent to use private information.....	38
9.4.6. Disclosure pursuant to judicial or administrative process.....	38
9.4.7. Other information disclosure circumstances.....	38
9.5. INTELLECTUAL PROPERTY RIGHTS.....	38
9.6. REPRESENTATIONS AND WARRANTIES.....	38
9.6.1. CA representations and warranties.....	38
9.6.2. RA representations and warranties.....	38
9.6.3. Subscriber representations and warranties.....	38
9.6.4. Relying party representations and warranties.....	38
9.6.5. Representations and warranties of other participants.....	39
9.7. DISCLAIMERS OF WARRANTIES.....	39
9.8. LIMITATIONS OF LIABILITY.....	39
9.8.1. Warranties and its limitations.....	39
9.8.2. Demarcation of responsibilities.....	39
9.8.3. Loss limitations.....	39
9.9. INDEMNITIES.....	39
9.10. TERM AND TERMINATION.....	39
9.10.1. Term.....	39
9.10.2. Termination.....	39
9.10.3. Effect of termination and survival.....	39
9.11. NOTIFICATIONS.....	39
9.12. AMENDMENTS.....	39
9.12.1. Procedure for amendment.....	39
9.12.2. Notification mechanism and period.....	40



9.12.3. Circumstances under which OID must be changed.....	40
9.13. DISPUTE RESOLUTION PROVISIONS.....	40
9.13.1. Resolution of off-court conflicts.....	40
9.13.2. Competent jurisdiction.....	40
9.14. GOVERNING LAW.....	40
9.15. COMPLIANCE WITH APPLICABLE LAW.....	40
9.16. MISCELLANEOUS PROVISIONS.....	40
9.16.1. Entire agreement.....	40
9.16.2. Assignment.....	40
9.16.3. Severability.....	40
9.16.4. Enforcement (attorneys' fees and waiver of rights).....	40
9.16.5. Force Majeure.....	40
9.17. OTHER PROVISIONS.....	40
ANNEX I - CERTIFICATION CONTRACT.....	41
ANNEX II – CERTIFICATE REVOCATION REQUEST FORM.....	44

1. INTRODUCTION

1.1. Overview

The current document is the Certification Policy associated to the qualified certificates based on software for citizens, 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 based on software for citizens, following the legislation in force.

The current Certification Policy is drafted following the RFC 3674 “*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, to ease the reading or comparison with counterparts documents. This Certification Policy assumes that the reader has basic knowledge about the Public Key Infrastructure, digital certificates and signature concepts, otherwise the reader is recommended to be trained in these concepts before continuing reading the current document.

1.2. Identification

Policy Name	Certification Policy for Qualified Certificates in software support 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	6.0.3
Policy status	APPROVED
Policy Reference / OID (Object Identifier)	1.3.6.1.4.1.8149.3.7.6.0
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.

Qif.: PUBLIC	Ref.: ACCV-CP-07V6.0.3-EN-2020.odt	Version: 6.0.3
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.6.0	Pg. 11 of 45

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 that can apply for the certificates that are defined in this policy, is made up of any natural person who possess the required identification elements (DNI, NIE, etc.).

The keys and certificates is based on software (diskette, hard drive, CDRom or other non cryptographic storage).

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:

1. 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.
2. 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.
3. The applications and services of any Public Administration.
4. 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. Certificates 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 the electronic signature or 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.

Qif.: PUBLIC	Ref.: ACCV-CP-07V6.0.3-EN-2020.odt	Version: 6.0.3
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.6.0	Pg. 12 of 45



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.

Qif.: PUBLIC	Ref.: ACCV-CP-07V6.0.3-EN-2020.odt	Version: 6.0.3
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.6.0	Pg. 13 of 45



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.

Qlf.: PUBLIC	Ref.: ACCV-CP-07V6.0.3-EN-2020.odt	Version: 6.0.3
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.6.0	Pg. 14 of 45

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 right to request the certificates that are 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 non on site 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 DNLe.

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

Qlf.: PUBLIC	Ref.: ACCV-CP-07V6.0.3-EN-2020.odt	Version: 6.0.3
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.6.0	Pg. 15 of 45

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).

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.

1.1.

3.4. Identification and authentication for revocation request

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

- On-site 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 apply for a certificate revocation if they have knowledge or suspect about the subscriber's private key compromise, or any other fact that would recommend to carry out this action.

Qif.: PUBLIC	Ref.: ACCV-CP-07V6.0.3-EN-2020.odt	Version: 6.0.3
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.6.0	Pg. 16 of 45

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 extracted 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 electronic mail that would be digitally signed to the email address that is listed in the request.

In on-site applications the registration authority operator provides the applicant with a 25-character alphanumeric code with the URL to continue the process. At this point the ACCV also sends the mail

Qif.: PUBLIC	Ref.: ACCV-CP-07V6.0.3-EN-2020.odt	Version: 6.0.3
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.6.0	Pg. 17 of 45

with the unique web address to validate the address of the application. In very exceptional cases the generation process can be completed in the RA, by building the key pair and the associated CSR. This CSR is sent to the CA for signature, being returned to the RA and building a key container in PKCS12 format that is delivered to the applicant. This type of generation is only done due to the technical impossibility of the applicant, leaving a record and evidence of the whole process.

In remote applications the applicant must access the Personal Area of Certification Services (remote Registration Authority) with a personal certificate or the DNle. If the applicant is able to make the application, the corresponding option will be shown. As part of the process the applicant must validate the mail address using the same method as in the face to face processing.

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. 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 remitted the request and another copy to the ACCV repository.

RA 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 the generation code and personal data input by the applicant in the enrollment URL
- RA asks the applicant for the construction of the key pair 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 DNle and the personal data associated with the application are extracted from the fields of the certificate.

Qif.: PUBLIC	Ref.: ACCV-CP-07V6.0.3-EN-2020.odt	Version: 6.0.3
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.6.0	Pg. 18 of 45



- 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 asks the applicant for the construction of the key pair 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.

All these processes are done in the generation platform provided by the ACCV.

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.

Qif.: PUBLIC	Ref.: ACCV-CP-07V6.0.3-EN-2020.odt	Version: 6.0.3
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.6.0	Pg. 19 of 45

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.

Qif.: PUBLIC	Ref.: ACCV-CP-07V6.0.3-EN-2020.odt	Version: 6.0.3
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.6.0	Pg. 20 of 45

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. Certificate 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. Certificate 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. On-site 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.

Qif.: PUBLIC	Ref.: ACCV-CP-07V6.0.3-EN-2020.odt	Version: 6.0.3
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.6.0	Pg. 21 of 45

4.9.3.2. Web

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 (DNle 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>.

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 the 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.

Qlf.: PUBLIC	Ref.: ACCV-CP-07V6.0.3-EN-2020.odt	Version: 6.0.3
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.6.0	Pg. 22 of 45

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.

Qif.: PUBLIC	Ref.: ACCV-CP-07V6.0.3-EN-2020.odt	Version: 6.0.3
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.6.0	Pg. 23 of 45

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.

Qif.: PUBLIC	Ref.: ACCV-CP-07V6.0.3-EN-2020.odt	Version: 6.0.3
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.6.0	Pg. 24 of 45



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.

Qif.: PUBLIC	Ref.: ACCV-CP-07V6.0.3-EN-2020.odt	Version: 6.0.3
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.6.0	Pg. 25 of 45

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.

Qif.: PUBLIC	Ref.: ACCV-CP-07V6.0.3-EN-2020.odt	Version: 6.0.3
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.6.0	Pg. 26 of 45

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 point is always referred to the keys that are generated for the certificates that were issued over the scope of the current Certification Policy. The information about the keys of entities that make up the Certification Authority are found at point 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 certificate that is issued under the scope of this Certification Policy can be generated in two places; the subscriber workstation in a process of self-generation without leaving the system, and alternatively, in exceptional cases, the keys could be generated in the Registration Authority User Point (ARCA).

6.1.2. Private key delivery to subscriber

The private key for the certificates that are issued under the scope of this Certification Policy are placed at the subscriber workstation where the key pair was generated. In the case of ARCA generation, it will be delivered to the subscriber and neither copy nor trace will remain on the RA.

6.1.3. Public key delivery to certificate issuer

The public key to be certified is generated in the user workstation 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.

If the key pair is generated in the PRU, a certification request will be created in the same manner, according to the PKCS#10 format for being signed by the CA.

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 name	Signature algorithm	Signature algorithm parameters	Key generation algorithm	Padding method	Cryptographic hash function
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

The certificates issued under this Certificate Policy are software based, so the cryptographic module standards and controls depend on the subscriber's OS.

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 Key pair is based on software. There is not cryptographic devices.

6.2.7. Private key storage on cryptographic module

The Key pair is based on software. There is not cryptographic devices.

6.2.8. Method of activating private key

In case of keys auto-generation, the activation method is established by the user in the moment of generation. If the private key has been generated in the ARCA, the activating will be performed by introducing the password access to this key, which is contained in a PKCS#12 file.

6.2.9. Method of deactivating private key

The deactivation will be performed by closing the application that uses it or closing the related software based cryptographic module.

6.2.10. Private key destruction method

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

The task to be performed consists of deleting the container of the private key.

6.2.11. Cryptographic Module Rating

See section Cryptographic module standards and controls of this Certification Policy.

6.3. Other aspects of key pair management

6.3.1. Public key file

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

6.3.2. Usage period for public and private keys

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

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

The certificate of the "ACCVCA-120" is valid since 13th October 2011 until 1st January 2027.

6.4. Activation data

6.4.1. Activation data generation and installation

In case of keys auto-generation the activation mechanism is established by the user in the moment of generation. The subscriber has the responsibility and obligation to chose the appropriate security mechanisms and maintain the private key under his/her sole control.

If the generation is carried out in the Registration Authority User Point (ARCA) the password of access to the private key or to the file that contains the PKCS#12 will be provided to the subscriber. The subscriber has the responsibility and obligation to change the preset password by a new one of his/her sole knowledge immediately after the PKCS#12 file reception and previous to its first usage.

6.4.2. Activation data protection

The subscriber is responsible for the protection of the activation data of his/her private key.

Qif.: PUBLIC	Ref.: ACCV-CP-07V6.0.3-EN-2020.odt	Version: 6.0.3
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.6.0	Pg. 30 of 45

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. Lifecycle Technical 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 Certificate extensions of this Policy.

7.1.2. Certificate extensions

The extensions that are used by the certificates that are issued under 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:SUBSCRIBERSNIF
OrganizationalUnit	Ciudadanos
Organization	ACCV
Country	ES
Version	V3
SerialNumber	Certificate unique identifier (32 hexadecimal characters)
Algorithm of signature	sha256withRSAEncryption
Issuer	
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		
Policy OID	QCP-n: certificate policy for EU qualified certificates issued to natural persons; ltu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural(0)	
Policy OID	1.3.6.1.4.1.8149.3.7.6.0	
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-calssuers	
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	
Algoritmo de hash	SHA-256	
KeyUsage (críticos)		
Authentication/Signature Certificate	Digital Signature Non-repudiation	
Encryption Certificate	Key Encipherment Data Encipherment	
QcStatement (only certificates of signature)	Fields QC (Qualified Certificate)	QcStatement
QcCompliance		The certificate is qualified
QcType	eSign	Particular type of qualified certificate
QcRetentionPeriod	15y	Retention period of the material information
QcPDS	https://www.accv.es/fileadmin/Archivos/Practicas_de_certificacion/ACCV-PDS-V1.0-EN.pdf	Location of PKI Disclosure Statement

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

7.1.3. Algorithms object identifiers (OID)

Object identifier (OID) of 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 defined by the ACCV for identifying the current policy is the following:

1.3.6.1.4.1.8149.3.7.6.0

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 in software support issued for 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.

Qif.: PUBLIC	Ref.: ACCV-CP-07V6.0.3-EN-2020.odt	Version: 6.0.3
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.6.0	Pg. 34 of 45

7.2. CRL profile

7.2.1. Version number (s)

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

7.2.2. CRL and CRL entry extensions

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

7.3. OCSP profile

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

7.3.1. Version number (s)

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

7.3.2. OCSP Extensions

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

8.2. Identification/qualification of Assessor

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

8.3. Assessor's Relationship to Assessed Entity

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

8.4. Topics Covered by Assessment

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

8.5. Actions Taken as a Result of Deficiency

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

8.6. Communication of results

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

8.7. Self-Audits

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

Qlf.: PUBLIC	Ref.: ACCV-CP-07V6.0.3-EN-2020.odt	Version: 6.0.3
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.6.0	Pg. 36 of 45

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 of 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.

Qlf.: PUBLIC	Ref.: ACCV-CP-07V6.0.3-EN-2020.odt	Version: 6.0.3
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.6.0	Pg. 37 of 45

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.

Qif.: PUBLIC	Ref.: ACCV-CP-07V6.0.3-EN-2020.odt	Version: 6.0.3
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.6.0	Pg. 38 of 45

9.6.5. Representations and warranties of other participants

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

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 that are issued within this Certification Policy in the exercise of providing the 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.

Qif.: PUBLIC	Ref.: ACCV-CP-07V6.0.3-EN-2020.odt	Version: 6.0.3
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.6.0	Pg. 39 of 45

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

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

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.



CERTIFICATION CONTRACT – OID 1.3.6.1.4.1.8149.3.7

Conditions of use

1. The certificates that are associated to the Certification Policy for Qualified Certificates based on software 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 natural person, with a NIF, NIE or any other identification document valid in Law.
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 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 <https://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 certificates that it issues.
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. It is, therefore, 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 period of validity 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 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.
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

Qlf.: PUBLIC	Ref.: ACCV-CP-07V6.0.3-EN-2020.odt	Version: 6.0.3
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.6.0	Pg. 42 of 45



CERTIFICATION CONTRACT – OID 1.3.6.1.4.1.8149.3.7

Section 1 – Subscriber's 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 associated to the Certification Policy for Qualified Certificates based on software for citizens with the OID 1.3.6.1.4.1.8149.3.7, 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.

Signature of the subscriber

Signature and stamp of the Registration Point

Signed:

Signed:

Nº of request

Copy for the ACCV

Qlf.: PUBLIC	Ref.: ACCV-CP-07V6.0.3-EN-2020.odt	Version: 6.0.3
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.6.0	Pg. 43 of 45



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* <p style="font-size: small;">* The will to revocation of the certificate subscriber is a valid reason for this request.</p>	
Section 4 – Authorization* Certificate subscriber <div style="text-align: center; margin-left: auto; margin-right: auto;"><i>Signature</i></div> Registration Point Operator: <div style="text-align: center; margin-left: auto; margin-right: auto;">Signature:</div>	

Copy for the ACCV

CERTIFICATE REVOCATION REQUEST

Qlf.: PUBLIC	Ref.: ACCV-CP-07V6.0.3-EN-2020.odt	Version: 6.0.3
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.6.0	Pg. 44 of 45

V3.0
Date:.....
<p>Section 1 – Subscriber data Surname: Name: DNI/NIF:</p>
<p>Section 2 – Certificate identification* Personal certificate: Nº of the certificate request:</p>
<p>Section 3 – Revocation reason*</p> <p style="margin-top: 20px;">* The will to revocation of the certificate subscriber is a valid reason for this request.</p>
<p>Section 4 – Authorization* Certificate subscriber</p> <p style="text-align: center; margin-top: 20px;"><i>Signature</i></p> <p>Registration Point Operator:</p> <p style="text-align: center; margin-top: 20px;">Signature:</p>

Copy for the applicant