



# Agencia de Tecnología y Certificación Electrónica

## Certification Policy for Electronic Administrative Headquarters Certificates based on software

<b>Date:</b> 16/07/2019	<b>Version:</b> 4.0.2
<b>Status:</b> APPROVED	<b>Number of pages:</b> 37
<b>OID:</b> 1.3.6.1.4.1.8149.3.15.4.0	<b>Classification:</b> PUBLIC
<b>File:</b> ACCV-CP-15V4.0.2-EN-2109.doc	
<b>Prepared by:</b> Agencia de Tecnología y Certificación Electrónica - ACCV	

## Table of Content

<b>1. INTRODUCTION.....</b>	<b>7</b>
1.1. OVERVIEW.....	7
1.2. DOCUMENT NAME AND IDENTIFICATION.....	7
1.3. PKI PARTICIPANTS.....	8
1.3.1. <i>Certification Authorities</i> .....	8
1.3.2. <i>Registration authorities</i> .....	8
1.3.3. <i>Subscribers</i> .....	8
1.3.4. <i>Relying parts</i> .....	8
1.4. CERTIFICATE USAGE.....	8
1.4.1. <i>Appropriate certificate uses</i> .....	8
1.4.2. <i>Prohibited certificate uses</i> .....	8
1.5. POLICY ADMINISTRATION.....	9
1.5.1. <i>Organization administering the document</i> .....	9
1.5.2. <i>Contact person</i> .....	9
1.5.3. <i>Person determining CPS suitability for the policy</i> .....	9
1.5.4. <i>CPS approval procedures</i> .....	9
1.6. DEFINITIONS AND ACRONYMS.....	9
<b>2. PUBLICATION AND REPOSITORY RESPONSIBILITIES.....</b>	<b>10</b>
2.1. REPOSITORIES.....	10
2.2. PUBLICATION OF CERTIFICATION INFORMATION.....	10
2.3. TIME OR FREQUENCY OF PUBLICATION.....	10
2.4. ACCESS CONTROLS ON REPOSITORIES.....	10
<b>3. IDENTIFICATION AND AUTHENTICATION.....</b>	<b>11</b>
3.1. NAMING.....	11
3.1.1. <i>Type of names</i> .....	11
3.1.2. <i>Need for names to be meaningful</i> .....	11
3.1.3. <i>Anonymity or pseudonymity of subscribers</i> .....	11
3.1.4. <i>Uniqueness of names</i> .....	11
3.1.5. <i>Resolution of names conflicts</i> .....	11
3.1.6. <i>Recognition, authentication and role of trademarks</i> .....	11
3.2. INITIAL IDENTITY VALIDATION.....	11
3.2.1. <i>Method to prove possession of private key</i> .....	11
3.2.2. <i>Authentication of organization identity</i> .....	11
3.2.3. <i>Authentication of individual identity</i> .....	13
3.2.4. <i>Non-verified subscriber information</i> .....	13
3.2.5. <i>Validation of authority</i> .....	13
3.2.6. <i>Criteria for Interoperation</i> .....	13
3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS.....	13
3.3.1. <i>Identification and authentication for routine re-key</i> .....	13
3.3.2. <i>Identification and authentication for re-key after revocation</i> .....	14
3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST.....	14
<b>4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS.....</b>	<b>15</b>
4.1. CERTIFICATE APPLICATION.....	15
4.2. CERTIFICATE APPLICATION PROCESSING.....	15
4.3. CERTIFICATE ISSUANCE.....	15
4.4. CERTIFICATE ACCEPTANCE.....	16
4.5. KEY PAIR AND CERTIFICATE USAGE.....	16
4.6. CERTIFICATE RENEWAL.....	16
4.7. CERTIFICATE RE-KEY.....	16
4.8. CERTIFICATE MODIFICATION.....	16
4.9. CERTIFICATE REVOCATION AND SUSPENSION.....	16



4.9.1.	<i>Circumstances for revocation</i> .....	16
4.9.2.	<i>Who can request revocation</i> .....	16
4.9.3.	<i>Procedure for revocation request</i> .....	16
4.9.4.	<i>Revocation request grace period</i> .....	17
4.9.5.	<i>Time within which CA must process the revocation request</i> .....	17
4.9.6.	<i>Revocation checking requirement for relying parties</i> .....	17
4.9.7.	<i>CRL issuance frequency</i> .....	17
4.9.8.	<i>On-line revocation/status checking availability</i> .....	17
4.9.9.	<i>On-line revocation checking requirements</i> .....	17
4.9.10.	<i>Other forms of revocation advertisements available</i> .....	17
4.9.11.	<i>Special requirements re key compromise</i> .....	17
4.9.12.	<i>Circumstances for suspension</i> .....	17
4.9.13.	<i>Who can request suspension</i> .....	17
4.9.14.	<i>Procedure for suspension request</i> .....	17
4.9.15.	<i>Limits on suspension period</i> .....	17
4.10.	CERTIFICATE STATUS SERVICES.....	17
4.11.	END OF SUBSCRIPTION.....	18
4.12.	KEYS ESCROW AND RECOVERY.....	18
4.13.	CA CERTIFICATE KEYS EXPIRATION.....	18
<b>5.</b>	<b>FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS</b> .....	<b>19</b>
5.1.	PHYSICAL CONTROLS.....	19
5.1.1.	<i>Site location and construction</i> .....	19
5.1.2.	<i>Physical access</i> .....	19
5.1.3.	<i>Power and air conditioning</i> .....	19
5.1.4.	<i>Water exposure</i> .....	19
5.1.5.	<i>Fire prevention and protection</i> .....	19
5.1.6.	<i>Media storage</i> .....	19
5.1.7.	<i>Waste disposal</i> .....	19
5.1.8.	<i>Off-site backup</i> .....	19
5.2.	PROCEDURAL CONTROLS.....	19
5.2.1.	<i>Trusted roles</i> .....	19
5.2.2.	<i>Number of persons required per task</i> .....	19
5.2.3.	<i>Identification and authentication for each role</i> .....	19
5.3.	PERSONNEL CONTROLS.....	20
5.3.1.	<i>Qualifications, experience, and clearance requirements</i> .....	20
5.3.2.	<i>Background check procedures</i> .....	20
5.3.3.	<i>Training requirements</i> .....	20
5.3.4.	<i>Retraining frequency and requirements</i> .....	20
5.3.5.	<i>Job rotation frequency and sequence</i> .....	20
5.3.6.	<i>Sanctions for unauthorized actions</i> .....	20
5.3.7.	<i>Independent contractor requirements</i> .....	20
5.3.8.	<i>Documentation supplied to personnel</i> .....	20
5.3.9.	<i>Regular checks on compliance</i> .....	20
5.3.10.	<i>End of contracts</i> .....	20
5.4.	AUDIT LOGGING PROCEDURES.....	20
5.4.1.	<i>Types of events recorded</i> .....	20
5.4.2.	<i>Frequency of processing log</i> .....	20
5.4.3.	<i>Retention period for audit log</i> .....	20
5.4.4.	<i>Protection of audit log</i> .....	21
5.4.5.	<i>Audit log backup procedures</i> .....	21
5.4.6.	<i>Audit collection system (internal vs. external)</i> .....	21
5.4.7.	<i>Notification to event-causing subject</i> .....	21
5.4.8.	<i>Vulnerability assessments</i> .....	21
5.5.	RECORDS ARCHIVAL.....	21
5.5.1.	<i>Types of records archived</i> .....	21
5.5.2.	<i>Retention period for archive</i> .....	21
5.5.3.	<i>Protection of archive</i> .....	21
5.5.4.	<i>Archive backup procedures</i> .....	21



5.5.5. Requirements for time-stamping of records.....	21
5.5.6. Archive collection system (internal or external).....	21
5.5.7. Procedures for obtaining and verifying the recorded information.....	21
5.6. KEY CHANGEOVER.....	21
5.7. COMPROMISE AND DISASTER RECOVERY.....	22
5.7.1. Incident and compromise handling procedures.....	22
5.7.2. Computing resources, software and/or data are corrupted.....	22
5.7.3. Entity private key compromise procedures.....	22
5.7.4. Business continuity capabilities after a disaster.....	22
5.8. CA OR RA TERMINATION.....	22
<b>6. TECHNICAL SECURITY CONTROLS.....</b>	<b>23</b>
6.1. KEY PAIR GENERATION AND INSTALLATION.....	23
6.1.1. Key pair generation.....	23
6.1.2. Private key delivery to subscriber.....	23
6.1.3. Public key delivery to the certificates issuer.....	23
6.1.4. CA public key delivery to relying parties.....	23
6.1.5. Key sizes.....	23
6.1.6. Public key parameters generation and quality checking.....	23
6.1.7. Key usage purposes (as per X.509 v3 key usage field).....	23
6.1.8. Hardware/software of key generation.....	24
6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROL.....	24
6.2.1. Bastion server characteristics.....	24
6.2.2. Private key (n out of m) multi-person control.....	24
6.2.3. Private key escrow.....	24
6.2.4. Private key backup.....	24
6.2.5. Private key archival.....	24
6.2.6. Private key transfer into or from a cryptographic module.....	24
6.2.7. Private key storage on cryptographic module.....	24
6.2.8. Method of activating private key.....	25
6.2.9. Method of deactivating private key.....	25
6.2.10. Method of destroying private key.....	25
6.2.11. Cryptographic Module Rating.....	25
6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT.....	25
6.3.1. Public key archival.....	25
6.3.2. Certificate operational periods and key pair usage periods.....	25
6.4. ACTIVATION DATA.....	25
6.4.1. Activation data generation and installation.....	25
6.4.2. Activation data protection.....	25
6.4.3. Other aspects of activation data.....	25
6.5. COMPUTER SECURITY CONTROLS.....	25
6.6. LIFE CYCLE TECHNICAL CONTROLS.....	25
6.7. NETWORK SECURITY CONTROLS.....	25
6.8. TIME-STAMPING.....	26
<b>7. CERTIFICATE, CRL, AND OCSP PROFILES.....</b>	<b>27</b>
7.1. CERTIFICATE PROFILE.....	27
7.1.1. Version number (s).....	27
7.1.2. Certificate extensions.....	27
7.1.3. Algorithm object identifiers.....	29
7.1.4. Name forms.....	29
7.1.5. Name constraints.....	29
7.1.6. Certificate policy object identifier.....	29
7.1.7. Usage of Policy Constrains extension.....	29
7.1.8. Policy qualifiers syntax and semantics.....	29
7.1.9. Processing semantics for the critical Certificate Policies extension.....	29
7.2. CRL PROFILE.....	30
7.2.1. Version number (s).....	30
7.2.2. CRL and CRL entry extensions.....	30

7.3. OCSF PROFILE.....	30
7.3.1. <i>Version number (s)</i> .....	30
<b>8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS.....</b>	<b>31</b>
8.1. FREQUENCY OF CIRCUMSTANCES OF ASSESSMENT.....	31
8.2. IDENTITY/QUALIFICATIONS OF ASSESSOR.....	31
8.3. ASSESSOR’S RELATIONSHIP TO ASSESSED ENTITY.....	31
8.4. TOPICS COVERED BY ASSESSMENT.....	31
8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY.....	31
8.6. COMMUNICATION OF RESULTS.....	31
<b>9. OTHER BUSINESS AND LEGAL MATTERS.....</b>	<b>32</b>
9.1. FEES.....	32
9.1.1. <i>Certificate issuance or renewal fees</i> .....	32
9.1.2. <i>Certificate access fees</i> .....	32
9.1.3. <i>Revocation or status information access fees</i> .....	32
9.1.4. <i>Fees for other services</i> .....	32
9.1.5. <i>Refund policy</i> .....	32
9.2. FINANCIAL RESPONSIBILITY.....	32
9.2.1. <i>Insurance coverage</i> .....	32
9.2.2. <i>Fiduciary relationships</i> .....	32
9.2.3. <i>Administrative procedures</i> .....	32
9.3. CONFIDENTIALITY OF BUSINESS INFORMATION.....	32
9.3.1. <i>Scope of confidential information</i> .....	32
9.3.2. <i>Information not within the scope of confidential information</i> .....	32
9.3.3. <i>Certificates revocation/suspension information disclosure</i> .....	33
9.4. PRIVACY OF PERSONAL INFORMATION.....	33
9.4.1. <i>Privacy plan</i> .....	33
9.4.2. <i>Information treated as private</i> .....	33
9.4.3. <i>Information not deemed private</i> .....	33
9.4.4. <i>Responsibility to protect private information</i> .....	33
9.4.5. <i>Notice and consent to use private information</i> .....	33
9.4.6. <i>Disclosure pursuant to judicial or administrative process</i> .....	33
9.4.7. <i>Other information disclosure circumstances</i> .....	33
9.5. INTELLECTUAL PROPERTY RIGHTS.....	33
9.6. REPRESENTATIONS AND WARRANTIES.....	33
9.6.1. <i>CA representations and warranties</i> .....	33
9.6.2. <i>RA representations and warranties</i> .....	33
9.6.3. <i>Relying party representations and warranties</i> .....	33
9.6.4. <i>Relying third parties obligations</i> .....	34
9.6.5. <i>Repository obligations</i> .....	34
9.7. DISCLAIMERS OF WARRANTIES.....	34
9.8. LIMITATIONS OF LIABILITY.....	34
9.8.1. <i>Warranty and warranty limitations</i> .....	34
9.8.2. <i>Segregation of responsibilities</i> .....	34
9.8.3. <i>Loss limitations</i> .....	34
9.9. INDEMNITIES.....	34
9.9.1. <i>Indemnification by Cas</i> .....	34
9.10. TERM AND TERMINATION.....	34
9.10.1. <i>Term</i> .....	34
9.10.2. <i>Termination</i> .....	34
9.10.3. <i>Effect of termination and survival</i> .....	34
9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS.....	34
9.12. AMENDMENTS.....	35
9.12.1. <i>Procedure for amendment</i> .....	35
9.12.2. <i>Notification mechanism and period</i> .....	35
9.12.3. <i>Procedures of Certification Practices Statement approval</i> .....	35
9.13. DISPUTE RESOLUTION PROVISIONS.....	35
9.13.1. <i>Off-court conflict resolution</i> .....	35



9.13.2. <i>Competent jurisdiction</i> .....	35
9.14. GOVERNING LAW.....	35
9.15. COMPLIANCE WITH THE APPLICABLE LAW.....	35
9.16. MISCELLANEOUS CLAUSES.....	35
9.16.1. <i>Entire Agreement</i> .....	35
9.16.2. <i>Assignment</i> .....	35
9.16.3. <i>Severability</i> .....	35
<b>10. ANNEX I.....</b>	<b>36</b>

# 1. INTRODUCTION

## 1.1. Overview

The current document is the Certification Policy for electronic administrative headquarters certificates, that contains the rules that are subjected to the management and usage of the certificates that are defined in this policy. The roles, responsibilities and relations between the end-user and the Agencia de Tecnología y Certificación Electrónica, and the application, acquisition, management and use of certificates rules, are described. This document complements and qualifies the Certification Practices Statement (CPS) of the Agencia de Tecnología y Certificación Electrónica.

The Certification Policy that this document is referred to will be used for the issuance of qualified certificates of electronic administrative headquarters.

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

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

This Certification Policy assumes that the reader has a basic knowledge about the Public Key Infrastructure, digital certificate and signature, in other case the reader is recommended to be trained in these concepts before continuing reading this document.

In the scope of the Certificate Transparency project, the precertificates will be published in the CT Log service of qualified log server providers in order to comply with project requirements.

## 1.2. Document name and identification

Policy name	Certification Policy of Qualified Certificates of electronic administrative headquarters based on software
Policy Qualifier	Certificado cualificado de sede electrónica administrativa expedido por la ACCV (Plz Nápoles y Sicilia, 6. Valencia CP 46003, ESPAÑA. CIF S4611001A)
Policy version	4.0.2
Policy status	APPROVED
OID (Object Identifier)	1.3.6.1.4.1.8149.3.15.4.0
Date of issuance	2019 jul 16th
Expire date	Non-applicable.
Related CPS	Certification Practices Statement (CPS) of ACCV. Version 4.0 OID: 1.3.6.1.4.1.8149.2.4.0 Available at <a href="http://www.accv.es/pdf-politicas">http://www.accv.es/pdf-politicas</a>
Localization	This Certification Policy can be found at: <a href="http://www.accv.es/legislacion_c.htm">http://www.accv.es/legislacion_c.htm</a>

Qlf: <b>PUBLIC</b>	Ref.: ACCV-CP-15V4.0.2-EN-2109.doc	Version: 4.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pg. 7

## 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 Register Authority that manages this type of certificates is the Agencia de Tecnología y Certificación Electrónica (ACCV).

### 1.3.3. Subscribers

The group of users that can apply for the certificates that are defined in this policy is composed of Head of Service or equivalent organizational occupation of Public Administration (European, Statewide, autonomic and local), being these the last responsible for its usage in different projects and information systems.

The support of keys and certificates is software, and the subscriber must guarantee that the location of the private key is a bastion system or that it meets sufficient security conditions to protect the private key it contains.

The certificate application right that is defined in the current Certification Policy is limited to natural persons. Certification applications carried out by legal entities, bodies or organizations will not be accepted.

### 1.3.4. Relying parts

The right to trust in certificates that are issued with the current policy is limited to:

- a) The users of application clients during the process of identity verification of the electronic headquarters that are connected to and of the data that is transmitted between them by an encrypted channel.
- b) The applications and services with SSL and/or TLS support, during the process of identity verification of the electronic headquarters that are connected to and of the data that is transmitted between them by an encrypted channel.

## 1.4. Certificate usage

### 1.4.1. Appropriate certificate uses

The certificates issued by the Agencia de Tecnología y Certificación Electrónica under this Certification Policy can be used for bringing the SSL/TLS capabilities to electronic headquarters. They can be used as an identification mechanism of servers or internet domains in an unequivocal way in presence of digital services and applications.

### 1.4.2. Prohibited certificate uses

The certificates will be used only according to the purpose and aim that the current Certification Policy has established, and with the regulation in force.

Qlf.: <b>PUBLIC</b>	Ref.: ACCV-CP-15V4.0.2-EN-2109.doc	Version: 4.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pg. 8



## 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

In addition to what is specified in the Certification Practices Statement (CPS).

**Bastion:** the process whereby a specific security policy is implemented over an installation of an operating system. The enforcement of an equipment tries to reduce its exposure level, and therefore, the risks and vulnerabilities that are associates to it.

**SSL:** Secure Sockets Layer

**TLS:** Transport Layer Security

Qlf.: <b>PUBLIC</b>	Ref.: ACCV-CP-15V4.0.2-EN-2109.doc	Version: 4.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pg. 9

## 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 host test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate.

VALID

<https://activo.accv.es/test/hola.html>

REVOKED

<https://revocado.accv.es:442/test/hola.html>

EXPIRED

<https://caducado.accv.es:444/test/hola.html>

ACCV conforms to the [current version](#) of the Baseline Requirements for the Issuance and Management of Publicly-Trusted 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.

Qif.: <b>PUBLIC</b>	Ref.: ACCV-CP-15V4.0.2-EN-2109.doc	Version: 4.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pg. 10

## 3. IDENTIFICATION AND AUTHENTICATION

### 3.1. Naming

#### 3.1.1. Type 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. Uniqueness of names

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

#### 3.1.5. Resolution of names conflicts

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 apply for certificates that is defined in the current Certification Policy is limited to natural persons. Certificate application carried out in name of legal entities, bodies or organizations will not be accepted.

Authentication of the identity of the applicant of a certificate is made through the use of his/her personal certificate qualified for the signing the request for the website qualified certificate.

The applicant must submit the necessary documentation which determines

The information related to the organization as the inclusion in the corresponding commercial register, address, locality, state or province, country, operating codes, etc..

The necessary representative capabilities of the entity that owns the referred domain.

The domain possession.

This submitting will be carried out digitally using the sources and applications that ACCV provided to the users for this.

ACCV will check the supplied data (including the country of the applicant) using for this the available information of

Data Protection Agencies

Public Administrations register

Qlf.: <b>PUBLIC</b>	Ref.: ACCV-CP-15V4.0.2-EN-2109.doc	Version: 4.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pg. 11



Commercial register

Verification services and Consultation of identity data

requiring to the applicant the explanations or additional documents that it could consider necessary.

All agencies and registers used are official and of high reliability, providing traceable evidence of all searches.

ACCV keeps this information for the purpose of auditory, permitting its reuse during a no longer period of 13 months since its last check.

### **Domain verification**

ACCV will verify the certificates domain and its associated addresses belong to the applicant data using for this the available information of personal and domain registers, demanding to the applicant the explanations or additional documents that could consider necessary. ACCV keeps this information for audit purpose, permitting its reuse during a no longer period of 13 months since its last check. ACCV will not issue certificates to IP addresses or private domain names. In the case of gTLD, only certificates with approved gTLD names will be issued, and will only be issued to subscribers who have control of the gTLD, as it appears in ICANN/IANA.

Specifically:

By consulting the registers assigned to ICANN/IANA. This validation will be performed by WHOIS consults using registers enabled by the public corporate entity Red.es at <http://www.nic.es> or equivalent for national domains, or the provided for generic domains by ICANN ([whois.icann.org](http://whois.icann.org)). ACCV will use this information to contact by mail with registrant until confirming the data accuracy.

Checking that the applicant, whose identity has been verified without a doubt, is one of the registrants of the domain. For this check you must use one or more of the following methods:

- Contacting by mail, sending a unique random number in the mail to the domain name registrant's address, waiting for a time not exceeding 30 days and checking the response that must include the same random number
- Contacting by mail, sending a unique random number in the mail to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name, including a Random Value in the email, and receiving a confirming response utilizing the Random Value., waiting for a time not exceeding 30 days and checking the response that must include the same random number
- Confirming the presence of a random value contained in the content of a file under the "/.well-known/pki-validation" directory, or another path registered with IANA for the purpose of Domain Validation, on the Authorization Domain Name that is accessible by the CA via HTTP/HTTPS over an Authorized Port. Once the value is communicated to the applicant, it will only be valid for 30 days.
- Confirming the presence of a random value for either in a DNS CNAME, TXT or CAA record for either 1) an Authorization Domain Name; or 2) an Authorization Domain Name that is prefixed with a label that begins with an underscore character. Once the value is communicated to the applicant, it will only be valid for 30 days.

ACCV will check for CAA records before issuing the certificate, acting as defined in rfc 6844 and CAB Forum documents if the record is present. The identifier associated with ACCV as a CAA record is "accv.es"

In addition to WHOIS consulting, connection tests with the given domain and DNS response tests using Secure Protocol (e.g. HTTPS) will be performed.

If it is a certificate with a wildcard character (\*), the application to make the request (NPSC) only allows to place the character in a valid position (it is never allowed in a first position to the left of a "registry-controlled" label or public suffix).

Qif.: <b>PUBLIC</b>	Ref.: ACCV-CP-15V4.0.2-EN-2109.doc	Version: 4.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pg. 12

In presence of any irregularity the certificate applicant will be notified by ACCV and its issuance will be suspended until its correction. If that correction does not happen in a month, the request will be denied.

### 3.2.3. Authentication of individual identity

Certificate's applicant identification will be carried out by the use of his/her qualified personal certificate for the signing the request for the Electronic Headquarter Certificate.

The applicant must submit the necessary documentation which determines the representative capabilities of the entity that owns the referred domain and, which also determines that domain possession. This submitting will be carried out digitally using the sources and applications that ACCV provided to the users for this task (3.2.2).

ACCV will check the supplied data (including the country of the applicant) using for this the available information of

Data Protection Agencies

Public Administrations register

Commercial register

Verification services and Consultation of identity data

requiring to the applicant the explanations or additional documents that it could consider necessary. All agencies and registers used are official and of high reliability, providing traceable evidence of all searches. ACCV keeps this information for the purpose of auditory, permitting its reuse during a no longer period of 13 months since its last check.

### 3.2.4. Non-verified subscriber information

All the information provided is verified.

### 3.2.5. Validation of authority

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

### 3.2.6. Criteria for Interoperation

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

## 3.3. Identification and authentication for re-key requests

### 3.3.1. Identification and authentication for routine re-key

The identification and authentication for the certificate renewal can be carried out using the initial authentication and identification methods (described in point 3.2.3. *Authentication of Individual Identity* from this Certification Policy). ACCV can reuse the stored information in the previous checks if there has not passed 13 months since the last data verification. Exist, therefore, one mechanism for the renewal:

- Web-forms in the Non-Personal Certificates Management Area, available at <https://npsc.accv.es:8450/npsc>.

### 3.3.2. Identification and authentication for re-key after revocation

The identification and authentication policy for a certificate renewal after a non-compromised key revocation will be the same as for the initial register, and it is possible to reuse the information that is

Qif.: <b>PUBLIC</b>	Ref.: ACCV-CP-15V4.0.2-EN-2109.doc	Version: 4.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pg. 13



in possession of ACCV is there has not passed 13 months since its last data verification. ACCV can implement any digital method that guarantees in a reliable and unequivocal way the applicant identity and the application authentication because of technical questions and detailing every step that it takes.

### 3.4. Identification and authentication for revocation request

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

- Telematic. Through a revocation form (located in the Non-Personal Certificates Management Area <https://npsc.accv.es:8450/npsc>) accessing by the certificate applicant or an administrator of the organization registered in the application with sufficient capabilities, on the revocation date with a personal qualified certificate.

ACCV or any of the entities that are part of it, can request for a certificate revocation if they knew or suspected the private key that is associated to the certificate that is issued under this Certification Policy is compromised, or any fact that would recommend to carry this action out.

Qlf.: <b>PUBLIC</b>	Ref.: ACCV-CP-15V4.0.2-EN-2109.doc	Version: 4.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pg. 14

## **4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS**

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

### **4.1. Certificate Application**

This type of certificates application is the responsibility of public entities.

The process starts by accessing to the Non-Personal Certificate Management Area located at <https://npsc.accv.es:8450/npsc>. If the headquarters certificate that is linked to a Public Administration is requested for the first time, the applicant must attach the document that accredits him/her as a qualified person for carrying out this application (document certifying the employment relationship or an official journal where the associated information is collected), in PDF format digitally signed. If the access has been carried out with a Public Employee certificate, the Organization, Organizational Unit and the Occupation data of certificate will be used.

ACCV will check the application data and accredit the applicant for the headquarters authentication certificate application, during 13 months since the approval with no need of submitting any additional documentation. In case of identifying with public employee certificate there is no temporal limit existent while the certificate is still in force.

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.

The user must check the bastion server software option in the certificate request.

### **4.2. Certificate application processing**

After receiving the certificate request in electronic format through the IT platform by the authorized persons and once the economic proposition is accepted, it will proceed to the application approval. After the acceptance, the Register Authority will notify the applicant through an electronic mail that would be digitally signed to the email that is listed in the request. The applicant must go into the Non-Personal Certificate Management Area located at <https://npsc.accv.es:8450/npsc> identifying himself/herself with a personal qualified certificate for generating and downloading the certificate.

In addition to check the associated credentials to the entity, ACCV will verify in the authorized registers the possession of domain or domains that appear in the certificate request, so there is no doubt about the existence of this possession, as detailed in sections 3.2.2 and 3.2.3 of this policy. ACCV will leave a record of these searches and checks so they can be reproduced in every step. For this checking ACCV will use the mails and phones that were submitted in the register process, being necessary a direct connection between these data and the domains that are included in the application. This acceptance will be carried out by a different ACCV member to the responsible of performing the verification of data. The differentiation of roles is carried out using the established capabilities in the management application.

In this process, ACCV will check that certificate requests do not include domains that can be used for phishing or other fraudulent uses, using available mechanisms and lists.

ACCV will use this information to decide on new applications.

### **4.3. Certificate issuance**

ACCV will carry out frequent revisions about headquarter authentication certificates samples for guaranteeing the data accuracy and the effect. If in the course of these samplings it is confirmed a data change that may involve the domain possession loss, ACCV will revoke the involved certificates. In case of inaccuracy of the information that is contained in the certificate or its non-applicability the same process will be applied. ACCV will leave a documentary proof of all these revisions and actions. ACCV is not responsible for monitoring, investigation or confirmation of the accuracy of the contained

Qlf.: <b>PUBLIC</b>	Ref.: ACCV-CP-15V4.0.2-EN-2109.doc	Version: 4.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pg. 15

information subsequently to its issuance. In case of inaccuracy of the information that is contained in the certificate or its non-applicability, the certificate can be revoked.

The certificate issuance will take place once the Register Authority has carried out the necessary verification for validating the certification request. The mechanism that determines the nature and manner of performing such verification is this Certification Policy.

The responsible of electronic headquarter certificate can ask ACCV to add other users with capacity of carrying out the transactions that are associated to the life cycle of electronic headquarter certificate that is linked to. The Register Authority will check the credential application and will notify the requester about the permit authorization or denial, through a signed electronic mail.

ACCV can carry out this authorization ex-officio in case the electronic headquarter responsible loses the management capabilities and there is no other authorized person.

#### 4.4. Certificate acceptance

Subscribers certificates acceptance is carried out when the Certification Contract that is associated to this Certification Policy is signed. The contract acceptance involves the subscribers knowledge and acceptance of the associated Certification Policy.

The Certification Contract is a document that must be signed by the applicant and its aim is to link the Electronic Headquarter Certificate applicant with the knowledge of rules usage and documents submitted truthfulness. The Certification Contract form can be found in Annex I of this Certification Policy.

#### 4.5. Key pair and certificate usage

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

#### 4.6. Certificate renewal

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.

#### 4.8. Certificate modification

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 ACCV.

##### 4.9.2. Who can request revocation

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

##### 4.9.3. Procedure for revocation request

Agencia de Tecnología y Certificación Electrónica accepts the revocation applications by the following procedures.

Qlf.: PUBLIC	Ref.: ACCV-CP-15V4.0.2-EN-2109.doc	Version: 4.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pg. 16



#### 4.9.3.1. Telematic

By accessing to the Non-Personal Certificates Management Area located at <https://npsc.accv.es:8450/npsc> the user can revoke the certificates that were requested or the ones he/she has a permit for it.

#### 4.9.4. Revocation request grace period

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

#### 4.9.5. Time within which CA must process the revocation request

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

#### 4.9.6. Revocation checking requirement for relying parties

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

#### 4.9.7. CRL issuance frequency

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

#### 4.9.8. On-line revocation/status checking availability

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

#### 4.9.9. On-line revocation checking requirements

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

#### 4.9.10. Other forms of revocation advertisements available

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

#### 4.9.11. Special requirements re key compromise

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

#### 4.9.12. Circumstances for suspension

A certificate will be suspended if a legal or administrative authority so provides, for a period of time that they determine.

ACCV does not support the certification suspension as a separate transaction concerning its own certificates.

#### 4.9.13. Who can request suspension

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

#### 4.9.14. Procedure for suspension request

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

#### 4.9.15. Limits on suspension period

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

### 4.10. Certificate status services

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

Qif.: <b>PUBLIC</b>	Ref.: ACCV-CP-15V4.0.2-EN-2109.doc	Version: 4.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pg. 17

#### 4.11. End of subscription

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

ACCV will notify the Headquarter Certificate person in charge, through a digitally signed email, in a period preceding the previous certification publication in the Certificate Revocation List, about the date and time the certificate shall terminate, and notifying that it must not be used.

#### 4.12. Keys escrow and recovery

ACCV does not deposit any keys associated to this type of certificates.

#### 4.13. CA certificate keys expiration

ACCV will avoid generating Electronic Headquarter certificates which expire subsequently to CA certificates. For this, Electronic Headquarter Certificates which validity period exceed the concerned CA certificate, will not be issued, and a new CA certificate will be generated, with a purpose of avoiding notifying subscribers to renew their certificates, in case the CA certificate expires earlier.

Qlf.: <b>PUBLIC</b>	Ref.: ACCV-CP-15V4.0.2-EN-2109.doc	Version: 4.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pg. 18

## 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 ACCV.

#### 5.1.2. Physical access

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

#### 5.1.3. Power and air conditioning

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

#### 5.1.4. Water exposure

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

#### 5.1.5. Fire prevention and protection

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

#### 5.1.6. Media storage

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

#### 5.1.7. Waste disposal

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

#### 5.1.8. Off-site backup

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

### 5.2. Procedural Controls

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

#### 5.2.1. Trusted roles

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

#### 5.2.2. Number of persons required per task

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

#### 5.2.3. Identification and authentication for each role

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

Qif.: <b>PUBLIC</b>	Ref.: ACCV-CP-15V4.0.2-EN-2109.doc	Version: 4.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pg. 19

### 5.3. Personnel controls

This section reflects the content specified at ACCV's *Personal Security Controls* document.

#### 5.3.1. Qualifications, experience, and clearance requirements

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

#### 5.3.2. Background check procedures

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

#### 5.3.3. Training requirements

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

#### 5.3.4. Retraining frequency and requirements

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

#### 5.3.5. Job rotation frequency and sequence

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

#### 5.3.6. Sanctions for unauthorized actions

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

#### 5.3.7. Independent contractor requirements

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

#### 5.3.8. Documentation supplied to personnel

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

#### 5.3.9. Regular checks on compliance

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

#### 5.3.10. End of contracts

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

### 5.4. Audit logging procedures

#### 5.4.1. Types of events recorded

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

#### 5.4.2. Frequency of processing log

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

#### 5.4.3. Retention period for audit log

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

Qlf.: <b>PUBLIC</b>	Ref.: ACCV-CP-15V4.0.2-EN-2109.doc	Version: 4.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pg. 20

#### 5.4.4. Protection of audit log

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

#### 5.4.5. Audit log backup procedures

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

#### 5.4.6. Audit collection system (internal vs. external)

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

#### 5.4.7. Notification to event-causing subject

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

#### 5.4.8. Vulnerability assessments

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

### 5.5. Records archival

#### 5.5.1. Types of records archived

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

#### 5.5.2. Retention period for archive

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

#### 5.5.3. Protection of archive

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

#### 5.5.4. Archive backup procedures

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

#### 5.5.5. Requirements for time-stamping of records

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

#### 5.5.6. Archive collection system (internal or external)

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

#### 5.5.7. Procedures for obtaining and verifying the recorded information

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

### 5.6. Key Changeover

Not stipulated.

Qif.: <b>PUBLIC</b>	Ref.: ACCV-CP-15V4.0.2-EN-2109.doc	Version: 4.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pg. 21

## 5.7. Compromise and disaster recovery

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

### 5.7.1. Incident and compromise handling procedures

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

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

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

### 5.7.3. Entity private key compromise procedures

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

### 5.7.4. Business continuity capabilities after a disaster

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

## 5.8. CA or RA termination

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

Qlf.: <b>PUBLIC</b>	Ref.: ACCV-CP-15V4.0.2-EN-2109.doc	Version: 4.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pg. 22

## 6. TECHNICAL SECURITY CONTROLS

### 6.1. Key pair generation and installation

This point is referred to the keys that were generated for the certificates issued over the scope of the current Certification Policy. The information about the entities keys which make up the Certification Authority are found in the 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 of the certificate issued under this Certification Policy is software generated by the certificates subscriber.

#### 6.1.2. Private key delivery to subscriber

The private key is generated by the subscriber, therefore, it is not appropriate to deliver it to him/her.

#### 6.1.3. Public key delivery to the certificates issuer

The public key to be certified is generated by the subscriber and is delivered to the Certification Authority by the Register Authority through a certificate's request in PKCS#10 format, and digitally signed by the subscriber.

#### 6.1.4. CA public key delivery to relying parties

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

#### 6.1.5. Key sizes

ACCVRAIZ1 and ACCVCA-120 roots keys are RSA keys length of 4096 bits.

The key size for certificates issued under the scope of this Certification Policy is at least 2048 bits.

#### 6.1.6. Public key parameters generation and quality checking

ACCVRAIZ1 and ACCVCA-120 roots keys are created with RSA algorithm.

Parameters defined in the cryptography suite 001 specified in ETSI TS 102 176-1 "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signature" 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

#### 6.1.7. Key usage purposes (as per X.509 v3 key usage field)

Keys defined in this policy will be used for the uses listed in the 1.3 "User community and scope of application" section of this document.

The detailed definition of the certificate profile and the keys uses are found in the section 7 "Certificate and Certificate Revocation List (CRL) profile" of this document.

Qif.: PUBLIC	Ref.: ACCV-CP-15V4.0.2-EN-2109.doc	Version: 4.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pg. 23



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

### 6.1.8. Hardware/software of key generation

Software key generation is performed by the certificate's subscriber.

## 6.2. Private key protection and cryptographic module engineering control

Keys generated for certificates issued under this Certification Policy will be referred to this section of this document. The information about the keys of entities which compose the Certification Authority is found in the section 6.2 of Agencia de Tecnología y Certificación Electrónica Certification Practices Statement (CPS).

### 6.2.1. Bastion server characteristics

It is recommended systems where the private keys are stored to meet a set of physical and logical security requirements. ACCV can, at its discretion, ask the subscriber to show the mechanisms that were used for said system bastion.

ACCV advises the subscriber organism to apply the NCC (National Cryptography Center) guides in its NCC-STIC serial, specifically for ensuring the safety of information and communication technology systems.

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

The key pair of certificates issued under this Certification Policy is under the exclusive control of their subscribers.

### 6.2.3. Private key escrow

Certificate's subscriber signature, authentication or encryption private keys defined in this policy are not kept.

### 6.2.4. Private key backup

Certificate's subscriber signature, authentication or encryption private keys defined in this policy are not kept., therefore it is not applicable.

### 6.2.5. Private key archival

Private keys are not filed.

### 6.2.6. Private key transfer into or from a cryptographic module

Not applicable in this Policy domain.

### 6.2.7. Private key storage on cryptographic module

The private key is generated by the applicant and is never in ACCV's owning.

Qlf.: <b>PUBLIC</b>	Ref.: ACCV-CP-15V4.0.2-EN-2109.doc	Version: 4.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pg. 24



#### 6.2.8. Method of activating private key

The private key is generated by the applicant and is never in ACCV's owning.

#### 6.2.9. Method of deactivating private key

Not stipulated.

#### 6.2.10. Method of destroying private key

#### 6.2.11. Cryptographic Module Rating

### 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 ACCV.

#### 6.3.2. Certificate operational periods and key pair usage periods

Certificates issued under this policy are valid for 27 months.

The key used for the certificates issuance is generated for each issuance, and therefore they are valid for 27 months as maximum.

The ACCVCA-120 certificate is valid since 13<sup>th</sup> October 2011 until 1<sup>st</sup> January 2027.

### 6.4. Activation data

#### 6.4.1. Activation data generation and installation

The private key is generated by the applicant and is never in the Agencia de Tecnología y Certificación Electrónica owning.

#### 6.4.2. Activation data protection

Responsibility for ensuring the protection of private key activation data is the certificate's person in charge or its owner.

#### 6.4.3. Other aspects of activation data

Not stipulated

### 6.5. Computer security controls

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

### 6.6. Life cycle technical 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 ACCV.

Qif.: <b>PUBLIC</b>	Ref.: ACCV-CP-15V4.0.2-EN-2109.doc	Version: 4.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pg. 25



## 6.8. Time-stamping

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

Qif.: <b>PUBLIC</b>	Ref.: ACCV-CP-15V4.0.2-EN-2109.doc	Version: 4.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pg. 26

## 7. CERTIFICATE, CRL, AND OCSP PROFILES

### 7.1. Certificate profile

#### 7.1.1. Version number (s)

This certification policy specifies a certificate's usage with three different uses; digital signature, subscriber's authentication and data encryption.

#### 7.1.2. Certificate extensions

The extensions used by certificates issued under this policy are:

Field	Value
<b>Subject</b>	
SerialNumber	Administration NIF, organism or entity of public right that is the certificates subscriber, which headquarter is linked to.
CommonName	Primary domain name (DNS) where the certificate will be stored.
OrganizationIdentifier (2.5.4.97)	Entity NIF, as it is collected in the official registers. Encrypted following the European Standard ETSI EN 319 412-1
OrganizationalUnit	Headquarter descriptive name
OrganizationalUnit	Fixed chain with SEDE ELECTRONICA value
Organization	Designation ("official" name) of the Administration, organism or entity of public right that is the certificate subscriber, which headquarter is linked to.
Jurisdiction Country	ES
Business Category	Government Entity
Locality	Town
State	Province
Country	ES State which law governs the name, that will be "Spain", for being public entities.
<b>Version</b>	V3
<b>SerialNumber</b>	Unique identifier of the certificate. Under 32 hexadecimal characters.
<b>Signature Algorithm</b>	sha256withRSAEncryption
<b>Issuer (Emisor)</b>	
CommonName	ACCVCA-120
OrganizationalUnit	PKIGVA
Organization	ACCV
Country	ES
<b>Effective since</b>	Issuance Date
<b>Effective until</b>	Expiration Date
<b>Public Key</b>	Octet String that contains the headquarter certificate public key.
<b>Extended Key Usage</b>	

	Server Authentication	
<b>CRL Distribution Point</b>		
	distributionPoint	<a href="http://www.accv.es/fileadmin/Archivos/certificados/accvca120_der.crl">http://www.accv.es/fileadmin/Archivos/certificados/accvca120_der.crl</a>
<b>SubjectAlternativeName</b>		
	dnsName	Headquarter DNS Domain Name
	dnsName	Headquarter DNS Domain Name
	dnsName	Headquarter DNS Domain Name
<b>Certificate Policy Extensions</b>		
Policy OID	2.16.724.1.3.5.5.2	
Policy OID	QCP-w Qualified certificate of websites according to the UE 910/2014 Regulation itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-web (4)	
Policy OID	1.3.6.1.4.1.8149.3.15.4.0	
Policy CPS Location	<a href="http://www.accv.es/legislacion_c.htm">http://www.accv.es/legislacion_c.htm</a> *	
Policy Notice	Certificado cualificado de sede electrónica administrativa expedido por la ACCV (Plz Nápoles y Sicilia, 6. Valencia CP 46003, ESPAÑA. CIF S4611001A)	
<b>Authority Information Access</b>	Access Method	Id-ad-ocsp
	Access Location	<a href="http://ocsp.accv.es">http://ocsp.accv.es</a>
	Access Method	Id-ad-calssuers
	Access Location	<a href="http://www.accv.es/gestcert/ACCVCA120SHA2.cacert.crt">http://www.accv.es/gestcert/ACCVCA120SHA2.cacert.crt</a>
<b>Fingerprint issuer</b>	48 72 a4 c3 df 17 4c ef 34 d7 7f e6 a3 b4 e7 be 7d f2 d2 5d	
<b>Algoritmo de hash</b>	SHA-256	
<b>KeyUsage (críticos)</b>		
	Digital Signature Key Encipherment	
<b>QcStatement</b>	<b>Campos QC (Qualified Certificate)</b>	
QcCompliance		The certificate is qualified
QcType	web	Particular type of qualified certificate
QcRetentionPeriod	15y	Retention period of material information
QcPDS	<a href="https://www.accv.es/fileadmin/Archivos/Practicas_de_certificacion/ACCV-PDS-V1.0-EN.pdf">https://www.accv.es/fileadmin/Archivos/Practicas_de_certificacion/ACCV-PDS-V1.0-EN.pdf</a>	Location of PKI Disclosure Statement

### 7.1.3. Algorithm object identifiers

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

Certificates issued under this Certification Policy contain the distinguished name X.500 of the certificate's issuer and subscriber in issuer name and subject name fields, respectively.

Issuer name: cn=ACCVCA-120, ou=PKIACCV o=ACCV, c=ES

All the fields of the certificate of the Subject and Subject Alternative Name, excepting the ones that are referred to the DNS name or email address, are filled necessarily in capital letters, without accents.

### 7.1.5. Name constraints

Names contained in the certificates are restricted to the X.500 "Distinguished Name" and must be unique and unambiguous.

### 7.1.6. Certificate policy object identifier

The object identifier defined by ACCV to identify this policy is the following:

1.3.6.1.4.1.8149.3.15.4.0

In this case an OID is added for identifying the type of entity that is represented, following the definition of the National State Administration profiles.

### **2.16.724.1.3.5.5.2 Certificate of electronic headquarter of medium/substantial degree**

In this case an OID is added for identifying the type of entity that is represented following the ETSI TS 119 411-2 standard

### **0.4.0.194112.1.4 Certification policy for EU qualified certificates issued for websites**

### 7.1.7. Usage of Policy Constrains extension

The "*Policy Constraints*" extension is not used in certificates issued under this Certification Policy.

### 7.1.8. Policy qualifiers syntax and semantics

Not stipulated

### 7.1.9. Processing semantics for the critical Certificate Policies extension

The "Certificate Policy" extension identifies the policy which defines the practices ACCV associates with the certificate. Additionally, the extension can contain a policy qualifier.

Qif.: <b>PUBLIC</b>	Ref.: ACCV-CP-15V4.0.2-EN-2109.doc	Version: 4.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pg. 29

## 7.2. CRL profile

### 7.2.1. Version number (s)

CRLs format that is used in the current policy is specified in version 2 (X509 v2).

### 7.2.2. CRL and CRL entry extensions

This Certification Policy supports and uses the CRLs which follow the X.509 standard.

## 7.3. OCSP profile

### 7.3.1. Version number (s)

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

Qif.: <b>PUBLIC</b>	Ref.: ACCV-CP-15V4.0.2-EN-2109.doc	Version: 4.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pg. 30

## 8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

### 8.1. Frequency of circumstances of assessment

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

### 8.2. Identity/qualifications 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.

Qlf.: <b>PUBLIC</b>	Ref.: ACCV-CP-15V4.0.2-EN-2109.doc	Version: 4.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pg. 31

## 9. OTHER BUSINESS AND LEGAL MATTERS

### 9.1. Fees

#### 9.1.1. Certificate issuance or renewal fees

The initial issuance and the certificate renewal fee that this certification policy refers to, is collected in ACCV fees list. This list is published in the ACCV web site [www.accv.es](http://www.accv.es)

#### 9.1.2. Certificate access fees

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

#### 9.1.3. Revocation or status information access fees

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

#### 9.1.4. Fees for other services

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

#### 9.1.5. Refund policy

The are no refunds of the quantities delivered for the payment of this type of certificates.

### 9.2. Financial responsibility

#### 9.2.1. Insurance coverage

As is specified in the Certification Practices Statement (CPS), ACCV offers warranty coverage sufficient for civil responsibility through an RC insurance policy to a value of Three Million Euros (3.000.000 €) which covers the risk of responsibility for damages and losses may come from the use of certificates issued by this Agency, complying with the obligation established in article 20.2 of electronic signature Law 59/2003, 19th of December.

#### 9.2.2. Fiduciary relationships

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

#### 9.2.3. Administrative procedures

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

#### 9.3.2. Information not within the scope of confidential information

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

Qif.: <b>PUBLIC</b>	Ref.: ACCV-CP-15V4.0.2-EN-2109.doc	Version: 4.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pg. 32



### 9.3.3. Certificates revocation/suspension information disclosure

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

## 9.4. Privacy of Personal Information

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

### 9.4.1. Privacy plan

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

### 9.4.2. Information treated as private

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

### 9.4.3. Information not deemed private

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

### 9.4.4. Responsibility to protect private information

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

### 9.4.5. Notice and consent to use private information

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

### 9.4.6. Disclosure pursuant to judicial or administrative process

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

### 9.4.7. Other information disclosure circumstances

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

## 9.5. Intellectual property rights

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

## 9.6. Representations and warranties

### 9.6.1. CA representations and warranties

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

### 9.6.2. RA representations and warranties

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

### 9.6.3. Relying party representations and warranties

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

Qif.: <b>PUBLIC</b>	Ref.: ACCV-CP-15V4.0.2-EN-2109.doc	Version: 4.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pg. 33

#### 9.6.4. Relying third parties obligations

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

#### 9.6.5. Repository obligations

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 ACCV.

### 9.8. Limitations of liability

#### 9.8.1. Warranty and warranty limitations

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

However, no economic limits associated to these certificates transactions by subscribers exist.

#### 9.8.2. Segregation of responsibilities

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

#### 9.8.3. Loss limitations

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

### 9.9. Indemnities

#### 9.9.1. Indemnification by Cas.

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

### 9.10. Term and termination

#### 9.10.1. Term

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

#### 9.10.2. Termination

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

#### 9.10.3. Effect of termination and survival.

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

### 9.11. Individual notices and communications with participants

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

Qif.: <b>PUBLIC</b>	Ref.: ACCV-CP-15V4.0.2-EN-2109.doc	Version: 4.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pg. 34

Every email sent by ACCV for certificates' subscribers which have been issued under this Certification Policy, in the course of providing certification service, will be digitally signed for ensure its authenticity and integrity.

## **9.12. Amendments.**

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

### **9.12.1. Procedure for amendment**

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

### **9.12.2. Notification mechanism and period**

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

### **9.12.3. Procedures of Certification Practices Statement approval**

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

## **9.13. Dispute resolution provisions**

### **9.13.1. Off-court conflict resolution.**

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

### **9.13.2. Competent jurisdiction**

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

## **9.14. Governing law**

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

## **9.15. Compliance with the applicable law**

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

## **9.16. Miscellaneous clauses**

### **9.16.1. Entire Agreement**

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

### **9.16.2. Assignment**

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

### **9.16.3. Severability**

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

Qif.: <b>PUBLIC</b>	Ref.: ACCV-CP-15V4.0.2-EN-2109.doc	Version: 4.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pg. 35



## 10. Annex I

### CERTIFICATION CONTRACT – OID 1.3.6.1.4.1.8149.3.15

#### **Section 1 – Subscribers data**

Surname:

Name:

NIF:

Tel.:

Position or occupation:

Administration-Organization:

Organization CIF:

Email address:

Mailing Address:

#### **Section 2 – Electronic Headquarter to be certified information**

Qualified name:

Alias:

Electronic headquarter descriptive name:

Contact email address:

#### **Section 3 – Date and Signature**

*I subscribe the current certification contract associated to the Certification Policy for electronic administrative headquarters based on software with OID 1.3.6.1.4.1.8149.3.15, issued by Agencia de Tecnología y Certificación Electrónica. I declare I know and accept the usage rules of this type of certificates that are exposed at <http://www.accv.es> Likewise I declare that all submitted data is correct.*

*Applicant's signature*

*Signed:*

Qlf.: PUBLIC	Ref.: ACCV-CP-15V4.0.2-EN-2109.doc	Version: 4.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pg. 36

## CERTIFICATION CONTRACT – OID 1.3.6.1.4.1.8149.3.15

### Certificate usage conditions

- 1.The certificates associated to the Certification Policy of Electronic Administrative Headquarters Certificates, 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 Certification Services Provider and so the referred Certification Policy. Both documents should be considered in accordance with the European Community law, the Spanish legal order and the Valencian Generalitat's law.
  - 2.The certificate applicant must be a natural person, in possession of anACCV qualified certificate of DNIE. The applicant must submit the data regarding to his/her relationship between the Public Administration, Instrumental Body of the Corporate Entity or Administration of Public Right, using the tools provided by ACCV.
  - 3.The certificate applicant, specially authorized for their management by an Administration or public entity part, is responsible for the submitted data veracity along the entire application and register process. He/She will be the responsible for notifying any submitted data change for the certificate collecting.
  - 4.The certificate subscriber is responsible for its private key custody and for communicating as soon as possible about this key loss or robbery.
  - 5.The certificate subscriber is responsible for limiting the certificate usage to the standing in the associated Certification Policy, which is a public document and is available at <http://www.accv.es>
  - 6.The Agencia de Tecnología y Certificación Electrónica is not responsible for the operation of computer servers that use the issued certificates.
  - 7.The Agencia de Tecnología y Certificación Electrónica is responsible for the accomplishments of European, Spanish and Valencian legislation, when is referred to the Electronic Signature. Therefore, it is responsible for the accomplishment of the specified at the Certification Practices Statement of the Agencia de Tecnología y Certificación Electrónica and at the Certification Policy associated to this type of certificates.
  - 8.These certificates period of validity is as maximum for 27 months. For its renewal the same procedures as for the first request or the ones provided in the associated Certification Policy, must be followed.
  - 9.The issued certificates will lose their efficacy, besides its period of validity expiration, when a revocation is produced, when its hardware becomes disabled, in presence of a judicial or administrative resolution which governs the efficacy loss, because of serious inaccuracies of submitted data by the applicant and because of the certificate subscriber death. Other conditions for the efficacy loss are listed in the Certification Practices Statement and in the associated Certification Policy to this type of certificates.
  - 10.The applicant identification will be carried out according to his/her personal digital certificate that was issued by the Agencia de Tecnología y Certificación Electrónica or with his/her DNIE. The applicant must submit the concerning data to its relation with the Public Administration, Instrumental Entity of the Administration or the Corporate Entity of Public Right.
  - 11.In accordance with the provisions of law 15/1.999, 13th December and REGULATION (EU) 2016/679 THE EUROPEAN PARLIAMENT AND THE COUNCIL of April 27, 2016, of Personal Data Protection, the applicant is informed about a computerized file with personal data created under the responsibility of Agencia de Tecnología y Certificación Electrónica, designated "Electronic Signature Users". The purpose of said file is to serve to related uses with certification services provided by the Agencia de Tecnología y Certificación Electrónica. The subscriber authorizes the use of his/her private data that is contained in said file, as necessary, for carrying out the action that are planned in the Certification Policy.
  - 12.The Agencia de Tecnología y Certificación Electrónica undertakes to use all means available for avoiding the alteration, 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, erasure, portability, restriction of processing, and objection over his/her personal data, sending a letter to the Agencia de Tecnología y Certificación Electrónica, through Entry Register of the Generalitat Valenciana and indicating clearly his/her will.
  14. The Agencia de Tecnología y Certificación Electrónica has formed a bank guarantee of three millions euros (3.000.000 €) to deal with the risk of damages actions that issued certificates and digital certification services usage could cause.
- With the signature of the current document the Agencia de Tecnología y Certificación Electrónica is authorized to consult identity data that are listed in the Ministry for Home Affairs (Kingdom of Spain), avoiding the citizen to submit a copy of his/her identity document.

Qlf.: PUBLIC	Ref.: ACCV-CP-15V4.0.2-EN-2109.doc	Version: 4.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.15.4.0	Pg. 37