Agencia de Tecnología y Certificación Electrónica

Certification Policy for Electronic Administrative Headquarters Certificates in Hardware Secure Module

Date: 10/09/2023	**Version:** 4.0.10
Status: APPROVED	**Number of pages:** 44
OID: 1.3.6.1.4.1.8149.3.14.4.0	**Classification: PUBLIC**
Archive: ACCV-CP-14V4.0.10-EN-2023.odt	
Prepared by: Agencia de Tecnología y Certificación Electrónica - ACCV	

Version	Author	Date	Observations
4.0.1	ACCV	27/09/2018	No changes.
4.0.2	ACCV	16/07/2019	CAB/Forum modification
4.0.3	ACCV	16/07/2019	Extension OCSP
4.0.4	ACCV	16/01/2020	RFC 3647 compliant
4.0.5	ACCV	09/03/2020	RFC 3647 compliant
4.0.6	ACCV	01/09/2020	Certificate validity
4.0.7	ACCV	20/03/2021	Policy notice
4.0.8	ACCV	20/06/2021	Change Wildcard issuance
4.0.9	ACCV	16/03/2023	OU are removed from profile and changes OID QNCP-w. Review and change minor details
4.0.10	ACCV	10/09/2023	Adaptation to policy 2.0 CAB/Forum

Table of Contents

1. INTRODUCTION

1.1. Overview

The current document is the Certification Policy for electronic administrative headquarters certificates in hardware secure module, 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 relation 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 headquarter in hardware secure module -HSM-.

The current Certification Practices Statement is drafted following the specifications of the RFC 3647 "I*nternet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*" proposed by the *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.

This Certification Policy assumes that the reader has 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 for Electronic Administrative Headquarter Certificates in Hardware Secure Module
Certificate identification	`Certificado cualificado de sede electrónica administrativa expedido por la ACCV (Pol. Ademuz, s/n. Burjassot, CP 46100, ESPAÑA. CIF A40573396)`
Policy version	4.0.10
Policy status	APPROVED
OID (Object Identifier)	1.3.6.1.4.1.8149.3.14.4.0
Date of issuance	2023 September 10th
Expire date	Non-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/CERT-CUALIFICADO-WEB_ACCV-ISTEC_CIF-A40573396_SPAIN

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 Authorities 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 cryptographic secure device -HSM- which is approved by the Ministry with the correspondent features like device insurance, following the established recommendations at European level.

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 and 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.

1.3.5. Other participants

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

1.4. Certificate usage

1.4.1. Appropriate certificate uses

The certificates issued by the Agencia de Tecnología y Certificación Electrónica under this Certification Policy can be used for bringing 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.

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).

HSM: Hardware Security Module

SSL: Secure Sockets Layer

TLS: Transport Security Layer

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.

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 of 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

https://sedeagpd.gob.es/sede-electronica-web/

Public Administrations register

https://face.gob.es/es/directorio/administraciones

https://sede.administracion.gob.es/

Commercial register

https://sede.registradores.org/site/

Patent and trademark office

https://www.oepm.es/en/index.html

Verification services and Consultation of identity data

https://administracionelectronica.gob.es/ctt/SVD

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 but it is not reused, verifying the domain for each request independently.. 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:

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

  (CAB/Forum BR 3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact)

- Contacting by mail, sending a unique random number in the mail to tone 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.

  (CAB/Forum BR 3.2.2.4.4 Constructed Email to Domain Contact)

- Confirming the presence of a random value contained in the content of a file under the "/.well-known/pki-validation" directory 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.

  (CAB/Forum BR 3.2.2.4.18 Agreed-Upon Change to Website v2)

- 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.

(CAB/Forum BR 3.2.2.4.7 DNS Change)

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 issue and issuewild records 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.

The issuance of wildcard certificates is not allowed under this policy, as of 20/06/2021.

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

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 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 verificatio. Exists, 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 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.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

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

4.1. Certificate Application

4.1.1. Who Can Submit a Certificate Application

This type of certificates application is the responsibility of public entities. A certificate application can be submitted by the subject of the certificate or by an authorized representative of the subject.

4.1.2. Enrollment Process and Responsibilities

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 HSM or secure device option in the certificate request.

4.2. Certificate application processing

4.2.1. Performing identification and authentication functions

The applicant identifying himself/herself with a personal qualified certificate into Non-Personal Certificate Management Area (NPSC) located at https://npsc.accv.es:8450/npsc, using the certificate data for performing identification and authentication functions.

After receiving the certificate request in electronic format through the IT platform by the authorized persons and once the economic proposition is accepted, ACCV proceeds to the application revision.

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

In addition to check the associated credentials to the entity, ACCV verifies 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 provides records of these searches and checks so they can be reproduced in every step. For this checking ACCV uses 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.

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

4.2.2. Approval or rejection of certificate applications

In case of acceptance, Register 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 case of reject, Register Authority will notify the applicant through an electronic mail that would be digitally signed to the email address that is listed in the request. The request is canceled and cannot be reused, although it is possible to reuse the documentation provided marked as correct for a period not exceeding 13 months.

This process is carried out by a different ACCV member to the responsible of performing the verification of data. The differentiation of roles is achieved using the established capabilities in the management application.

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. Certificate issuance

4.3.1. CA actions during certificate issuance

The certificate issuance takes place once the Register Authority 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.

When the applicant receives the approval email, must go into NPSC again, identifying himself/herself with a personal qualified certificate for generating and downloading the certificate.

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

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

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.

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. Certificate acceptance

4.4.1. Conduct constituting certificate acceptance

The certificates acceptance by the subscribers takes place at the time of signature of the certification contract associated with each Certification Policy. Acceptance of the contract implies that the subscriber is aware of and accepts the associated Certification Policy.

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

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

4.4.2. Publication of the certificate by the CA

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

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

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

4.5. Key pair and certificate usage

4.5.1. Subscriber private key and certificate usage

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

4.5.2. Relying party public key and certificate usage

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

4.6. Certificate renewal

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

4.6.1. Circumstance for certificate renewal

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

4.6.2. Who may request renewal

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

4.6.3. Processing certificate renewal requests

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

4.6.4. Notification of new certificate issuance to subscriber

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

4.6.5. Conduct constituting acceptance of a renewal certificate

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

4.6.6. Publication of the renewal certificate by the CA

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

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

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

4.7. Certificate re-key

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

4.7.1. Circumstance for certificate re-key
According to the specified in the Certification Practices Statement (CPS) of ACCV.

4.7.2. Who may request certification of a new public key
According to the specified in the Certification Practices Statement (CPS) of ACCV.

4.7.3. Processing certificate re-keying requests
According to the specified in the Certification Practices Statement (CPS) of ACCV.

4.7.4. Notification of new certificate issuance to subscriber
According to the specified in the Certification Practices Statement (CPS) of ACCV.

4.7.5. Conduct constituting acceptance of a re-keyed certificate
According to the specified in the Certification Practices Statement (CPS) of ACCV.

4.7.6. Publication of the re-keyed certificate by the CA
According to the specified in the Certification Practices Statement (CPS) of ACCV.

4.7.7. Notification of certificate issuance by the CA to other entities
According to the specified in the Certification Practices Statement (CPS) of ACCV.

4.8. 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

4.9.1.1. Reasons for Revoking a Subscriber Certificate

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

4.9.1.2. Reasons for Revoking a Subordinate CA Certificate

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

4.9.2. Who can request for 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.

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. CRLs issuance frequency

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

4.9.8. Maximum Latency for CRLs

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

4.9.9. On-line Revocation/Status Checking Availability

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

4.9.10. On-line Revocation Checking Requirements

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

4.9.11. Other Forms of Revocation Advertisements Available

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

4.9.12. Special requirements of compromised key renewal

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

4.9.13. Circumstances for a suspension

A certificate will be suspended if a juridic or administrative authority provided it, for the period of time it establishes.

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

4.9.14. Entities that can apply for the suspension

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

4.9.15. Procedure for the suspension request

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

4.9.16. Suspension period limit

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

ACCV will inform the responsible of Administrative Headquarter certificate about the certificate revocation or suspension which is subscriber or person in charge of, 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 does not deposit any keys associated to this type of certificates.

4.12.2. Session key encapsulation and recovery policy and practices

Session key recovery is not supported.

4.13. CA certificate keys expiration

ACCV will avoid generating Administrative Headquarters certificates that expire subsequently to the CA certificates. For this, websites authentication certificates which validity period exceed the CA's certificate will not be issued and they will be generated with the new CA certificate, with the purpose of avoiding notifying the subscribers about the certificate renewal, in case the CA certificate expires earlier.

5. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

5.1. Physical Controls

5.1.1. Site location and construction
According to the specified in the Certification Practices Statement (CPS) of 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.

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 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.

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
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 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.

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 for the certificate issued under this Certification Policy is generated in the subscriber HSM.

6.1.2. Private key delivery to subscriber

The private key of certificates issued under this Certification Policy is located in the HSM and is generated by the subscriber.

6.1.3. Public key delivery to the certificates issuer

The public key to be certified is generated in the HSM and is delivered to the Certification Authority by the Register Authority through a certificate's request in PKCS#10 format, 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 Root 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 Root keys are created with RSA algorithm.

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

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

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.509v3 key usage field)

Keys defined in this policy will be used for the uses listed in the *1.3 Users 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, CRL, AND OCSP PROFILES*" of this document.

6.2. Private key protection and Cryptographic Module Engineering Controls

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. Cryptographic module standards and controls

The HSM devices that are used in the issuance of the certificates that are associated to this Certification Policy must have ITSEC E5 high certification or equivalent and support PKCS#11 and CSP standards.

It is also accepted the HSM certified by the agency accredited for this purpose at national level (OC-CCN https://oc.ccn.cni.es/index.php/en/)

Key generation is carried out in the HSM.

The minimal requirements for these devices are those specified by the correspondent Organization that has the competences, and according to the European technical normative.

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

The private keys for the certificates that are issued under the scope of this Certification Policy are under the exclusive control of their subscribers.

6.2.3. Private key escrow

In no case subscriber's private keys are held for escrow.

6.2.4. Private key backup

The private keys of the certificates issued in the scope the current policy are not backed up.

6.2.5. Private key archival

The private keys of the certificates issued in the scope the current policy are not filed.

6.2.6. Private key transfer into or from a cryptographic module

The generation of the keys that are associated to the certificate is carried out inside the HSM.

6.2.7. Private key storage on cryptographic module

The generation of the keys that are associated to the certificate is carried out inside the HSM and the private key cannot be extracted by what is stored inside and never leaves it.

6.2.8. Method of activating private key

The private key is generated by the applicant and it is never held by the ACCV. The activation will depend on the chosen HSM mechanisms for generating and storing.

6.2.9. Method of deactivating private key

The private key is generated by the applicant and it is never held by the ACCV. The deactivation will depend on the mechanisms of the HSM chosen for the deactivation of the keys.

6.2.10. Method of destroying private key

The private key is generated by the applicant and it is never held by the ACCV. The destruction will depend on the mechanisms of the HSM chosen for deletion and destruction of the keys.

6.2.11. Cryptographic Module Rating

The hardware security modules meet FIPS 140-2 level 3.

6.3. Other aspects of key pair managements

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

The certificates issued over the scope of the current policy have as maximum 12 months of validity.

The key pair must be generated for each issue, and therefore It has the same validity (12 months as maximum). That is the maximum validity date that is allowed in the application for the certificates issued under this policy.

The ACCVCA-120 certificate is valid since 13th October 2011 until 1st 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 held by ACCV. The activation will depend on the chosen HSM mechanisms for keys generation and storing.

6.4.2. Activation data protection

The subscriber is responsible for its private key activation data protection.

6.4.3. Other aspects of activation data

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

6.5. Computer security controls

6.5.1. Specific computer security technical requirements

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

6.5.2. Computer security rating

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

6.6. Life cycle security controls

6.6.1. System development controls

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

6.6.2. Security management controls

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

6.6.3. Life cycle security controls

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

6.7. Network security controls

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

6.8. Time-stamping

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

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. Certificate Profile

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

7.1.1. Version number

ACCV supports and uses X.509 version 3 (X.509 v3) certificates.

This certification policy specifies the usage of a certificate with two different uses; digital signature, and key encipherment.

7.1.2. Certificate extensions

The extensions that are used by the certificates issued under this policy are:

Field	**Value**
Subject	
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 reside
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
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
BusinessCategory	Government Entity
Locality	Town
State	Province
Country	ES (code ISO 3166-1) Country which law governs the name, that will be Spain, for being public entities.
Version	V3
SerialNumber	Unique identifier of the certificate. Under 32 hexadecimals characters.
Algoritmo de firma	sha256withRSAEncryption
Issuer (Emisor)	
CommonName	ACCVCA-120
OrganizationalUnit	PKIGVA
Organization	ACCV
Country	ES
Effective since	Issuance Date
Effective until	Expiration Date
Public Key	Octet String that contains the headquarter certificate public key.

Extended Key Usage		
	Server Authentication	
	Client Authentication	
CRL Distribution Point		
	distributionPoint	http://www.accv.es/fileadmin/Archivos/certificados/accvca120_der.crl
SubjectAlternativeName		
	dnsName	Headquarter DNS Domain Name
	dnsName (optional)	Headquarter DNS Domain Name
	dnsName (optional)	Headquarter DNS Domain Name
	dnsName (optional)	Headquarter DNS Domain Name
	dnsName (optional)	Headquarter DNS Domain Name
Certificate Policy Extensions		
Policy OID	{itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ovcp(7)} 0.4.0.2042.1.7	
Policy OID	{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)} 2.23.140.1.2.2	
Policy OID	2.16.724.1.3.5.5.1	
Policy OID	QCP-w Qualified certificate of website according to the EU 910/2014 Regulation itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-web (4)	
Policy OID	1.3.6.1.4.1.8149.3.14.4.0	
Policy CPS Location	http://www.accv.es/CERT-CUALIFICADO-WEB_ACCV-ISTEC_CIF-A40573396_SPAIN	
Authority Information Access	*Access Method*	Id-ad-ocsp
	Access Location	http://ocsp.accv.es
	Access Method	Id-ad-caIssuers
	Access Location	http://www.accv.es/gestcert/ACCVCA120SHA2.cacert.crt
Fingerprint issuer	48 72 a4 c3 df 17 4c ef 34 d7 7f e6 a3 b4 e7 be 7d f2 d2 5d	
Algoritmo de hash	SHA-256	
KeyUsage (críticos)		

	Digital Signature Key Encipherment	
SCT List ***1.3.6.1.4.1.11129.2.4.2***	Signed Certificate Timestamp List	
QcStatement	**Campos QC (Qualified Certificate)**	
QcCompliance		The certificate is qualified
QcType	web	Particular type of qualified certificate
QcRetentionPeriod	15y	Retention period of material information
QcPDS	https://www.accv.es/fileadmin/Archivos/Practicas_de_certificacion/ACCV-PDS-V1.0-EN.pdf	Location of PKI Disclosure Statement
QcSCD		Secure signature creation device (SSCD)
CA/Browser Forum Organization Identifier Field	cabfOrganizationIdentifier (OID: 2.23.140.3.1) {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-extensions(3) cabf-organization-identifier(1) }	
	registrationSchemeIdentifier	3 character Registration Scheme identifier (VAT)
	registrationCountry	2 character ISO 3166 country code (ES)
	registrationStateOrProvince	State or Province (optional)
	registrationReference	Registration Reference allocated in accordance with the identified Registration Scheme (CIF)

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

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, excepting the ones that are referred to the DNS names, email address or explicitly defined, are filled necessarily in capital letters, without accents.

SubjectAlternativeName contain at least one entry. Each entry in the SubjectAlternativeName is a dNSName containing the Fully-Qualified Domain Name of a server.

Subject:

commonName (required). It must match one of the DNSName fields of the subjectAlternativeName

serialNumber (required). Administration NIF, as defined in Royal Decree 1065/2007, of July 27.

OrganizationIdentifier (required) Entity NIF, as defined in the European standard ETSI EN 319 412-1

jurisdictionCountry (required) Country code ISO 3166-1

BusinessCategory (required) the following fixed chain

"Govennment Entity"

Organization (required) Designation (“official” name) of the Administration, organism or entity that is the certificate subscriber and the domain owner.

locality (required) Locality, City or Town

state (required) State o province

country (required) Country code ISO 3166-1

7.1.5. Names constraints

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

There are not name constraints defined for certificates issued under this policy.

7.1.6. Certificate policy object identifier

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

1.3.6.1.4.1.8149.3.14.4.0

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

2.16.724.1.3.5.5.1	**Certificate of electronic headquarter of high 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**

In this case an OID is added for identifying the type of entity that is represented following the CAB/Forum guidelines

2.23.140.1.2.2	**Certificates issued in accordance with the CA/Browser Forum's Baseline Requirements - Organization identity asserted**

In this case an OID is added for identifying the type of entity that is represented following the ETSI EN 319 411-1 standard

0.4.0.2042.1.7	**Organizational Validation Certificate Policy (OVCP)**

7.1.7. Usage of Policy Constraints extension

The “*Policy Constraints*” extension is not used in the certificates issued over the scope of the current Certification Policy.

7.1.8. Policy qualifiers syntax and semantics

The Certificate Policies extension can include one Policy Qualifier field (optional):

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

7.1.9. Processing semantics for the critical Certificate Policies extension

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

7.1.10. Signed Certificate Timestamp (SCT) List

Responses from known qualified logs, currently compliant with Chrome's Certificate TransparencyT policy.

Extension OID: 1.3.6.1.4.1.11129.2.4.2

RFC 6962 (Certificate Transparency): https://tools.ietf.org/html/rfc6962

For certificates with a notBefore value greater than or equal to April 21, 2021 (2021-04-21T00:00:00Z), the Number of embedded SCTs based on certificate lifetime:

Certificate lifetime	**# of SCTs from separate logs**	**Maximum # of SCTs per log operator which count towards the SCT requirement**
180 days or less	2	1
181 to 398 days	3	2

For certificates with a notBefore value less than April 21, 2021 (2021-04-21T00:00:00Z), the Number of embedded SCTs based on certificate lifetime:

Lifetime of Certificate	**Number of SCTs from distinct logs**
< 15 months	2
>= 15, <= 27 months	3
> 27, <= 39 months	4
> 39 months	5

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 of circumstances of assessment

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

8.2. Identify/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. Topic 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.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. Fees

9.1.1. Certificate issuance or renewal fees

The rates for the initial issuance and the renewal of the certificates that this certification policy is referred to, are listed in the Price List of the Agencia de Tecnología y Certificación Electrónica. This list is published in ACCV website 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

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

9.2.2. Other assets

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

9.2.3. Insurance or warranty coverage for end-entities

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.

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 parties representations and warranties

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

9.6.4. Relying third parties obligations

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

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 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.

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. Circumstances under which OID must be changed

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 provisions

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.

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

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

9.16.5. Force Majeure

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

9.17. Other provisions

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

10. Annex I

CERTIFICATION CONTRACT – OID 1.3.6.1.4.1.8149.3.14
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 in hardware secure module with OID 1.3.6.1.4.1.8149.3.14, 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:***

Certificate usage conditions

1..The certificates associated to the Certification Policy of Electronic Administrative Headquarters Certificates in Hardware Secure Module, 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 an ACCV 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 12 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 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 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.

Reasons for revocation

These are the reasons you can use to revoke your certificate:

No reason or unspecified.

The subscriber is not required to provide a reason for revocation unless his private key has been compromised.

affiliationChanged

This revocation reason SHOULD be chosen when your organization name or other organization information on the certificate has changed.

superseded

This revocation reason SHOULD be chosen when a new certificate is requested to replace an existing certificate.

cessationOfOperation

This revocation reason SHOULD be chosen when you no longer own all the domain names in the certificate or when you will no longer use the certificate because the web site will no longer be operational.

keyCompromise

This revocation reason MUST be chosen when the subscriber knows or has reason to believe that the private key in their certificate has been compromised. For example if an unauthorized person has gained access to the private key of their certificate. If this reason is selected, ALL CERTIFICATES ISSUED WITH THE SAME KEYS BY THE ORGANIZATION WILL BE REVOKED and ACCV may contact the applicant to gather more information and require additional evidence.

privilegeWithdrawn

The CA detects that there has been a breach on the subscriber side that has not resulted in key compromise, such as that the certificate subscriber provided misleading information in its certificate application or has not complied with its material obligations under the subscriber agreement or terms of use.

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.