Agencia de Tecnología y Certificación Electrónica

Certification Policy of Qualified Certificates for Websites Authentication

Date: 03/05/2018	**Version:** 4.0.1
Status: APPROVED	**Number of pages:** 36
OID: 1.3.6.1.4.1.8149.3.3.4.0	**Classification: PUBLIC**
File: ACCV-CP-3V4.0.1-EN-2018.doc	
Prepared by: Agencia de Tecnología y Certificación Electrónica - ACCV	

Table of Content

1. INTRODUCTION

1.1. Overview

The current document is the Certification Policy for websites authentication, that contains the rules that are subjected to the managements and the 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 rules, acquisition, management and use of certificates, 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 websites authentication.

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.

This Certification Policy assumes 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. Identification

Policy name	Certification Policy of Qualified Certificates of Websites Authentication
Policy qualifier	Certificado cualificado de autenticación de sitios web expedido por el Instituto Valenciano de Finanzas - ACCV (Plaza Nápoles y Sicilia, 6. Valencia CP 46003, ESPAÑA. CIF Q9650010C)
Policy version	4.0.1
Policy status	APPROVED
OID (Object Identifier)	1.3.6.1.4.1.8149.3.3.4.0
Date of issuance	2018 may 3rd
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 http://www.accv.es/pdf-politicas
Location	This Certification Policy can be found at: http://www.accv.es/legislacion_c.htm

1.3. User community and scope of application

1.3.1. Certification Authorities

The CA that can issue the certificates associated to this certification policy is ACCVCA-120 belonged to the Agencia de Tecnología y Certificación Electrónica, which function is to issue final entity certificates for ACCV's subscribers. ACCVCA-120 certificate is valid since the 13th October 2011 until 1st January 2027.

1.3.2. Registration Authorities

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

1.3.3. End Users

1.3.3.1. Subscribers

The group of users that can apply for the certificates that are defined in this policy is composed of private and public entities responsible, representing the applicant entity.

In case of public entities, the applications can be carried out by the 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.

In case of private entities, the certificates can be requested by those persons who have the representative capacity or who have been authorized for managing this type of certificates.

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.

1.3.3.2. Reliable parts

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

a) The users of application clients within the verification of identity of the websites that are connected to and of the data that is transmitted between them channel encryption.

b) The applications and services with SSL and/or TLS support, within the verification of identity of the websites that are connected to and of the data that is transmitted between them channel encryption.

1.4. Use of certificates

1.4.1. Permitted 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 websites. They can be used as an identification mechanism of these sites in an unequivocal way in presence of digital services and applications.

1.4.2. Forbidden uses

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

1.5. Administration Policy of ACCV

1.5.1. Administrative Organization Specification

Name	*Agencia de Tecnología y Certificación Electrónica IVF*
Email address	*accv@accv.es*
Address	*Plaza Nápoles y Sicilia , 6 –46003 Valencia (Spain)*
Telephone number	*+34 902 482 481*
Fax number	*+34·961 971 771*

1.5.2. Person of Contact

Name	*Agencia de Tecnología y Certificación Electrónica IVF*
Email address	*accv@accv.es*
Address	*Plaza Nápoles y Sicilia , 6 –46003 Valencia (Spain)*
Telephone number	*+34 902 482 481*
Fax number	*+34·961 971 771*

1.5.3. Competence for determining the CPS suitability to the Policies

The competent entity that determines the CPS suitability to different Certification Policies of ACCV, is the Sub-direction of the Financial Entities and Electronic Certification – IVF, according to the Statues of the Instituto Valenciano de Finanzas (IVF).

1.6. Definitions and Acronyms

1.6.1. Definitions

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.

1.6.2. Acronyms

SSL: Secure Sockets Layer

TLS: Transport Layer Security

2. Publication and Repository Responsabilities

2.1. Certificates repository

As 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

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

2.4. Access controls on repositories

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

3. Identification and Authentication

3.1. Naming

3.1.1. Types of names

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

3.1.2. Need for Names to be Meaningful

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

3.1.3. Anonymity or Pseudonymity of Subscribers

No pseudonyms are used in the certificates issued under this policy.

3.1.4. Rules for interpretation of name forms

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

3.1.5. Uniqueness of Names

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

3.1.6. Recognition, Authentication, and Role of Trademarks

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

3.2. Initial Identity Validation

3.2.1. Method to prove possession of private key

As 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 (3.2.4).

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

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.

3.2.3. 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 website qualified 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 (3.2.4).

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. Verification of Requested Domain

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). ACCV will use this information to contact by mail and landline phone 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 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

Contacting by phone, calling Domain Name Registrant´s phone number, requesting and obtaining confirmation of the application associated with the domain name.

Confirming the presence of a random number 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 number 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).

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.

3.3. 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 at point 3.2.3 I*ndividual identity authentication*, 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 – Non-compromised key

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 if 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 its responsible part, on the revocation date with a personal qualified certificate.

ACCV or any entity that make it up can request for a certificate revocation if they knew or suspected about the private key that is associated to the websites authentication certificate compromise, or any other fact that would recommend to carry this action out.

4. Certificate life cycle operational requirements

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

4.1. Certificate Application

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

The process starts by accessing to the Non-Personal Certificate Management Area located at https://npsc.accv.es:8450/npsc. If the websites authentication certificate that is linked to an entity 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, notarial powers and registration in the corresponding registries), in PDF format digitally signed. If the access has been carried out with a certificate that accredits the necessary capability for managing the websites authentication certificates, the Organization, Organizational Unit and the Occupation data of certificate will be used.

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

4.2. Certificate application processing

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.

ACCV will check the application data and accredit the applicant for the websites 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.

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, 3.2.3 and 3.2.4 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. Certificates issuance

ACCV will carry out frequent revisions about web 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.

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 form of performing these checks is this Certification Policy.

The 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 certificate that is linked to. 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.

4.4. Certificates acceptance

The certificates acceptance by the subscribers part is carried out in the moment of the certification contract acceptance associated to each Certification Policy. The contract acceptance involves the knowledge and acceptance of the associated Certification Policy by the subscriber part.

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.

4.5. Key pair and certificate usage

As 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.

4.7. Certificate Rekey

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

4.8. Certificate modification

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

4.9. Certificates revocation and suspension

4.9.1. Circumstances for revocation

4.9.1.1. Reasons for Revoking a Subscriber Certificate

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

4.9.1.2. Reasons for Revoking a Subordinate CA Certificate

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

4.9.2. Who can Request Revocation

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

4.9.3. Procedure for Revocation Request

ACCV accepts 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

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

4.9.5. .Time Within which CA Must Process the Revocation Request

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

4.9.6. Revocation Checking Requirement for Relying Parties

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

4.9.7. CRLs issuance frequency

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

4.9.8. Maximum Latency for CRLs

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

4.9.9. On-line Revocation/Status Checking Availability

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

4.9.10. On-line Revocation Checking Requirements

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

4.9.11. Other Forms of Revocation Advertisements Available

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

4.9.12. Special requirements of compromised key renewal

As 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

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

4.9.15. Procedure for the suspension request

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

4.9.16. Suspension period limit

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

4.10. Certificate Status Services

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

4.11. End of Subscription

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

ACCV will inform the responsible of websites authentication 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

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

4.13. CA certificate keys expiration

ACCV will avoid generating websites authentication 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
As specified in the Certification Practices Statement (CPS) of ACCV.

5.1.2. Physical access
As specified in the Certification Practices Statement (CPS) of ACCV.

5.1.3. Power and Air Conditioning
As specified in the Certification Practices Statement (CPS) of ACCV.

5.1.4. Water exposures
As specified in the Certification Practices Statement (CPS) of ACCV.

5.1.5. Fire Prevention and Protection
As specified in the Certification Practices Statement (CPS) of ACCV.

5.1.6. Media Storage
As specified in the Certification Practices Statement (CPS) of ACCV.

5.1.7. Waste disposal
As specified in the Certification Practices Statement (CPS) of ACCV.

5.1.8. Off-Site Backup
As specified in the Certification Practices Statement (CPS) of ACCV.

5.2. Procedural Controls
As specified in the Certification Practices Statement (CPS) of ACCV.

5.2.1. Trusted Roles
As specified in the Certification Practices Statement (CPS) of ACCV.

5.2.2. Number of persons required per task
As specified in the Certification Practices Statement (CPS) of ACCV.

5.2.3. Identification and authentication for each role
As specified in the Certification Practices Statement (CPS) of ACCV.

5.3. Personnel controls

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

5.3.1. Qualifications, Experience, and Clearance Requirements

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

5.3.2. Background check procedures

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

5.3.3. Training requirements

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

5.3.4. Retraining Frequency and Requirements

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

5.3.5. Job Rotation Frequency and Sequence

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

5.3.6. Sanctions for Unauthorized Actions

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

5.3.7. Independent Contractor Requirements

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

5.3.8. Documentation supplied to personnel

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

5.3.9. Regular checks on compliance

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

5.3.10. End of contracts

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

5.4. Audit Logging Procedures

5.4.1. Types of events recorded

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

5.4.2. Frequency of Processing Log

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

5.4.3. Retention period for audit log

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

5.4.4. Protection of Audit Log
As specified in the Certification Practices Statement (CPS) of ACCV.

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

5.4.6. Audit Collection System (Internal vs. External)
As specified in the Certification Practices Statement (CPS) of ACCV.

5.4.7. Notification to Event-Causing Subject
As specified in the Certification Practices Statement (CPS) of ACCV.

5.4.8. Vulnerability Assessments
As specified in the Certification Practices Statement (CPS) of ACCV.

5.5. Records archival

5.5.1. Types of Records Archived
As specified in the Certification Practices Statement (CPS) of ACCV.

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

5.5.3. Protection of Archive
As specified in the Certification Practices Statement (CPS) of ACCV.

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

5.5.5. Register time stamp requirements
As specified in the Certification Practices Statement (CPS) of ACCV.

5.5.6. Archive collection system (internal v. external)
As specified in the Certification Practices Statement (CPS) of ACCV.

5.5.7. Procedures for obtaining and verifying archived information
As specified in the Certification Practices Statement (CPS) of ACCV.

5.6. Key Changeover
Not stipulated.

5.7. Compromise and disaster recovery

5.7.1. Incident and Compromise Handling Procedures

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

5.7.2. Computing Resources, Software, and/or Data are Corrupted

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

5.7.3. Entity Private Key Compromise Procedures

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

5.7.4. Business continuity capabilities after a disaster

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

5.8. CA or RA termination

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

6. Technical security Controls

6.1. Key Pair Generation and Installation

This point is always referred to keys that were generated for certificates issued under the current Certification Policy. The information about the keys of entities that comprising the Certification Authority are found in the point 6.1 of the Certification Practices Statement of ACCV.

6.1.1. Key pair generation

The key pair for the certificate that is issued under this Certification Policy is generated in software support by the certificate subscriber.

6.1.2. Private Key Delivery to Subscriber

The private key is generated by the subscriber, therefore, it is not delivered to him.

6.1.3. Public key delivery to the certificate issuer

The public key to be certified is generated by the subscriber and is delivered to the Certification Authority sending a certification request in PKCS#10 format, digitally signed by the subscriber.

If it is detected that the public key in the request does not meet the requirements (weak key, etc..) it will be rejected.

6.1.4. CA Public Key Delivery to Relying Parties

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

6.1.5. Key sizes

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

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

6.1.6. Public key parameters generation and quality checking

The keys of ACCVRAIZ1 and ACCVCA-120 root are created with the 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-v2.1	sha256

6.1.7. Key Usage Purposes (as per X.509 v3 key usage field)

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

The detailed definition of the certificate profile and the usage of keys is located in the section 7 of this document “*Certificate profiles and certificate revocation list*”.

6.1.8. Hardware/software of key generation

The software of key generation is carried out by the certificate subscriber.

6.2. Private key protection and Cryptographic Module Engineering Controls

This point is always referred to the keys that are generated for certificates issued under the scope of the current Certification Policy. The information about the keys of entities that comprising the Certification Authorities is found in point 6.2 of the Certification Practices Statement (CPS) of ACCV.

6.2.1. Bastion server characteristics

The systems where the private keys are stored must accomplish a set of requirements related to the physical and logical security of them. ACCV can ask the subscriber organism to evidence the mechanisms that are used for said systems enforcement, in a discretionary manner.

It is recommended to follow the guidelines that were generated by the NCC (National Cryptography Center) within its CNN-STIC series, specifically oriented to guarantee the information technology systems and the Administration communications.

6.2.2. Private Key (n out of m) Multi-Person Control

The private keys for certificates issued over the scope of the current Certification Policy are located under the exclusive control of their subscribers.

6.2.3. Private key escrow

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

6.2.4. Private key backup

The private keys of the subscribers of the certificates that are defined in the current policy are not guarded, so it is not applicable.

6.2.5. Private key archival

The private keys of the subscribers of the certificates that are defined in the current policy are not guarded, so it is not applicable.

6.2.6. Private key transfer into or from a cryptography module

Not applicable in the scope of the current Policy.

6.2.7. Private key storage on cryptography module

Not applicable in the scope of the current Policy.

6.2.8. Method of Activating Private Key

The private key is generated by the applicant and is never in ACCV possession.

6.2.9. Method of Deactivating Private Key

The private key is generated by the applicant and is never in ACCV possession.

6.2.10. Method of Destroying Private Key

Not stipulated.

6.2.11. Cryptographic Module Rating

Not applicable in the scope of the current Policy.

6.3. Other aspects of key pair management

6.3.1. Public Key Archival

As 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 27 months of validity.

The key that is used for the certificates issuance is created for each issuance, and therefore is valid for 27 months as maximum. That is the maximum validity date that is allowed in the application for the certificates issued under this policy.

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 in ACCV possession.

6.4.2. Activation data protection

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

6.4.3. Other aspects of activation data

Not stipulated.

6.5. Computer security controls

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

6.6. Lifecycle Technical Controls

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

6.7. Network Security Controls

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

6.8. Time-Stamping

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

7. Certificate, CRL, and OCSP profiles

7.1. Certificate profile

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

7.1.1. Number of version(s)

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

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

7.1.2. Certificate extensions

The extensions that are used for the certificate issuance over the scope of the current policy, are:

Field	**Value**
Subject	
SerialNumber	Administration NIF, organism or entity of private or public right that is the certificates subscriber, which the website is linked to.
CommonName	Domain name (DNS) where the certificate will reside.
OrganizationIdentifier (2.5.4.97)	Entity NIF, as set out in the official registers. Codified following the European standard ETSI EN 319 412-1
OrganizationalUnit	Fix chain with the SERVIDORES value
Organization	Designation (“official” name) of the Administration, organism or entity that is the certificate subscriber and the domain owner.
JurisdictionCountry	ES (code ISO 3166-1)
BusinessCategory	One of the following fixed chains "PRIVATE ORGANIZATION", "GOVERNMENT ENTITY", "BUSINESS ENTITY”, o "NON-COMMERCIAL ENTITY”, depending on the organization type
Locality	Locality, City, Town
State	State, Province
Country	ES (code ISO 3166-1)
Version	V3
SerialNumber	Unique identifier of the certificate. Under 32 hexadecimals characters.
Algoritmo de firma	sha256withRSAEncryption
Issuer (Emisor)	
CommonName	ACCVCA-120
OrganizationalUnit	PKIACCV
Organization	ACCV
Country	ES
Válido desde	Issuance Date
Válido hasta	Expiration date

Clave Pública	Octet String which contains the certificate public key	
Extended Key Usage		
	Server Authentication Client Authentication	
CRL Distribution Point		
	distributionPoint	http://www.accv.es/fileadmin/Archivos/certificados/accvca120_der.crl
	distributionPoint	http://www.accv.es/gestcert/accvca120_der.crl
SubjectAlternativeName		
	dnsName	Domain Name DNS 1 (matches with the domain in the common name)
	dnsName (optional)	Domain Name DNS 2
	dnsName (optional)	Domain Name DNS 3
Certificate Policy Extensions		
Policy OID	QCP-w Website qualified certificate according to the Regulation UE 910/2014 itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-web (4)	
Policy OID	1.3.6.1.4.1.8149.3.3.4.0	
Policy CPS Location	http://www.accv.es/legislacion_c.htm*	
Policy Notice	Certificado cualificado de autenticación de sitios web expedido por el Instituto Valenciano de Finanzas - ACCV (Plaza Nápoles y Sicilia, 6. Valencia CP 46003, ESPAÑA. CIF S4611001A	
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	SCT responses from qualified logs At least three responses
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	PKI Disclosure Statement location

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

7.1.3. Algorithms 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

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

For certificates issued under this policy:

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 name or email address, 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

OrganizationalUnit (required) fixed string “SERVIDORES”

jurisdictionCountry (required) Country code ISO 3166-1

BusinessCategory (required) One of the following fixed chains

"PRIVATE ORGANIZATION"

"GOVERNMENT ENTITY"

"BUSINESS ENTITY”

"NON-COMMERCIAL ENTITY”

, depending on the organization type

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. Name constraints

The names that are contained in the certificates are restricted to distinguished names X.500, uniques 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 for identifying the current policy is the following:

1.3.6.1.4.1.8149.3.3.4.0

In this case an OID is added for identifying the type of entity that is representing with the regulation ETSI TS 119 411-2

0.4.0.194112.1.4	**Certification Policy for EU qualified certificates issued to websites**

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

Not stipulated.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

The "*Certificate Policy*" extension identifies the policy which defines the practices that ACCV explicitly associates with the certificate. In addition, 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

The number of responses is determined with the life cycle of the certificate according to the following table:

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)

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

7.2.2. CRL and CRL Entry Extensions

The current Certification Policy supports and uses CRLs that follow the standard X.509.

7.3. OCSP profile

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

7.3.1. Version number(s)

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

8. Compliance audit and other assessments

8.1. Frequency or Circumstances of Assessment

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

8.2. Identification/qualification of Assessor

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

8.3. Assessor's Relationship to Assessed Entity

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

8.4. Topics Covered by Assessment

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

8.5. Actions Taken as a Result of Deficiency

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

8.6. Communication of results

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

8.7. Self-Audits

As 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

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

9.1.3. Revocation or Status Information Access Fees

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

9.1.4. Fees of other services

As 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 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

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

9.2.3. Administrative procedures

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

9.3. Confidentiality of Business Information

9.3.1. Scope of Confidential Information

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

9.3.2. Information Not Within the Scope of Confidential Information

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

9.3.3. Certificates revocation/suspension information disclosure
As specified in the Certification Practices Statement (CPS) of ACCV.

9.4. Privacy of Personal Information
As specified in the Certification Practices Statement (CPS) of ACCV.

9.4.1. Privacy Plan
As specified in the Certification Practices Statement (CPS) of ACCV.

9.4.2. Information Treated as Private
As specified in the Certification Practices Statement (CPS) of ACCV.

9.4.3. Information not Deemed Private
As specified in the Certification Practices Statement (CPS) of ACCV.

9.4.4. Responsibility to protect private information
As specified in the Certification Practices Statement (CPS) of ACCV.

9.4.5. Notice and consent to use private information
As specified in the Certification Practices Statement (CPS) of ACCV.

9.4.6. Disclosure pursuant to judicial or administrative process
As specified in the Certification Practices Statement (CPS) of ACCV.

9.4.7. Other information disclosure circumstances
As specified in the Certification Practices Statement (CPS) of ACCV.

9.5. Intellectual property rights
As specified in the Certification Practices Statement (CPS) of ACCV.

9.6. Representations and warranties

9.6.1. CA representations and warranties
As specified in the Certification Practices Statement (CPS) of ACCV.

9.6.2. RA representations and warranties
As specified in the Certification Practices Statement (CPS) of ACCV.

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

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

9.6.5. Repository obligations

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

9.7. Disclaimers of warranties

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

9.8. Limitations of liability

9.8.1. Warranty and warranty limitations

As 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

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

9.8.3. Loss limitations

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

9.9. Indemnities

9.9.1. Indemnification by CAs.

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

9.10. Term and termination

9.10.1. Term.

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

9.10.2. Termination.

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

9.10.3. Effect of termination and survival.

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

9.11. Individual notices and communications with participants.

As 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

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

9.12.1. Procedure for amendment

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

9.12.2. Notification mechanism and period

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

9.12.3. Procedures of Certification Practices Statement approval

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

9.13. Dispute resolution provisions

9.13.1. Off-court conflict resolution

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

9.13.2. Competent jurisdiction

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

9.14. Governing law

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

9.15. Compliance with the applicable law

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

9.16. Miscellaneous clauses

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

9.16.1. Entire Agreement

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

9.16.2. Assignment

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

9.16.3. Severability

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

10. Annex I

CERTIFICATION CONTRACT – OID 1.3.6.1.4.1.8149.3.3
Section 1 – Subscribers data *Surname*: *Name*: NIF: Tel.: Position or occupation: Administration-Organization: Organization CIF: *Email address*: Mailing Address:
Section2 – Domain data Qualified name: Alias: Contact email address:
Section 3 – *Date and Signature* *I subscribe the current certification contract associated to the Certification Policy of Qualified Certificates of Websites Authentication with OID 1.3.6.1.4.1.8149.3.3, issued by the la 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*:

CERTIFICATION CONTRACT – OID 1.3.6.1.4.1.8149.3.3

Certificate usage conditions

1. The certificates associated to the Certification Policy of Qualified Certificates of Websites Authentication, 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 or 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 certificates 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 acocmplishment of the European, Spanish and Valencian legislation, when is referred to the Electronic Signature. Therefore, it is the responsible for the accomplishment of the specified at the Certification Practices Statement of the Agencia de Tecnología y Certificación 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.

11. In accordance to the law 15/1.999, of 13th December, of Personal Data Protection, the applicant is informed about a computerized file with personal data created under the responsibility of the 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 access rights, rectification or cancellation over his/her personal data, sending a letter to the Agencia de Tecnología y Certificación Electrónica, through any Entry Register of the Generalitat Valenciana and indicating clearly his/her will.

14. La 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.