Agencia de Tecnología
y Certificación Electrónica

Certification Practices and Policies for website authentication certificates

Date: 03/06/2025	**Version**4.0.17
Status: APPROVED	**No. of pages**112
OID: 1.3.6.1.1.4.1.8149.2.4 .0	**Classification: PUBLIC**
Archivo:ACCV-CPS-CP-V4.0.17-EN-2025.docx	

Changes

Version	Author	Date	Remarks
4.0.1	ACCV	20/05/2017	No change
4.0.2	ACCV	03/09/2018	CAB/Forum Modification
4.0.3	ACCV	03/02/2019	OCSP Extension
4.0.4	ACCV	19/07/2019	RFC364 Corrections. Modifications in the treatment of mail
4.0.5	ACCV	29/07/2019	Modification of the serial number
4.0.6	ACCV	15/01/2020	RFC3647 minor corrections .
4.0.7	ACCV	24/02/2020	Minor changes in the Law. RFC3647 Corrections
4.0.8	ACCV	20/03/2021	Change in the address of the headquarters. Proof of key compromise
4.0.9	ACCV	20/04/2022	Revision and correction
4.0.10	ACCV	02/12/2022	Video identification is included
4.0.11	ACCV	16/03/2023	Revision and minor changes
4.0.12	ACCV	10/09/2023	Adaptation to CAB/Forum Policy 2.0.0.0
4.0.13	ACCV	02/04/2024	Review
4.0.14	ACCV	10/06/2024	New TLS hierarchy and revision
4.0.15	ACCV	13/01/2025	Elimination of new hierarchy
4.0.16	ACCV	12/02/2025	New TLS hierarchy and revision
4.0.17	ACCV	03/06/2025	Consolidation of CPS and CP. Profile change.

Table of Contents

1. INTRODUCTION 13

1.1. Overview 13

1.2. Document Name and Identification 13

1.3. PKI Participants 14

1.3.1. Certification Authorities 14

1.3.1.1. Root Certification Authorities 14

1.3.1.1.1. ACCVRAIZ1 14

1.3.1.1.2. ACCV ROOT ECC TLS 2024 15

1.3.1.1.3. ACCV ROOT RSA TLS 2024 15

1.3.1.2. Subordinate Certification Authorities 15

1.3.2. Registration Authorities 17

1.3.3. Subscribers 18

1.3.4. Relying parties 18

1.3.5. Other participants 18

1.3.5.1. Applicants 18

1.4. Certificate Usage 18

1.4.1. Appropriate Certificate Uses 18

1.4.2. Prohibited Certificates Uses 19

1.5. ACCV Policy Administration 19

1.5.1. Organization Administering the Document 19

1.5.2. Contact Person 19

1.5.2.1. Problem Reporting Address 19

1.5.3. Person determining CPS suitability for the policy 19

1.5.4. CPS approval procedures 19

1.6. Definitions and Acronyms 20

1.6.1. Definitions 20

1.6.2. Acronyms 23

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES 24

2.1. Certificate repository 24

2.2. Publication 25

2.3. Time or Frequency of Publication 26

2.4. Access Controls on Repositories 26

3. IDENTIFICATION AND AUTHENTICATION 27

3.1. Naming 27

3.1.1. Types of names 27

3.1.2. Need for Names to be Meaningful 27

3.1.3. Anonymity or Pseudonymity of Subscribers 27

3.1.4. Rules for Interpreting Various Name Forms....27
3.1.5. Uniqueness of names....27
3.1.6. Recognition, Authentication, and Role of Trademarks....27
3.2. Initial Identity Validation....28
3.2.1. Method to Prove Possession of Private Key....28
3.2.2. Authentication of Organization Identity....28
3.2.3. Authentication of Individual Identity....30
3.2.4. Non-Verified Subscriber Information....31
3.2.5. Validation of Authority....31
3.2.6. Criteria for interoperation....31
3.3. Identification and Authentication for Re-Key Requests....31
3.3.1. Identification and Authentication for Routine Re-Key....31
3.3.2. Identification and Authentication for Re-Key after Revocation - Uncompromised key....32
3.4. Identification and Authentication for Revocation Request....32

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS....33

4.1. Certificate Application....33
4.1.1. Who can submit a certificate request....33
4.1.2. Enrollment Process and Responsibilities....33
4.2. Certificate Application Processing....33
4.2.1. Performing identification and authentication functions....33
4.2.2. Approval or Rejection of Certificate Applications....34
4.2.3. Time to Process Certificate Applications....34
4.3. Certificate Issuance....34
4.3.1. CA Actions during Certificate Issuance....34
4.3.2. Notification to Subscriber by the CA of Issuance of Certificate....35
4.3.3. Refusal to Issue a Certificate....35
4.4. Certificate Acceptance....35
4.4.1. Conduct Constituting Certificate Acceptance....35
4.4.2. Publication of the Certificate by the CA....35
4.4.3. Notification of Certificate Issuance by the CA to Other Entities....35
4.5. Key Pair and Certificate Usage....36
4.5.1. Subscriber Private Key and Certificate Usage....36
4.5.2. Relying Party Public Key and Certificate Usage....36
4.6. Certificate Renewal....36
4.6.1. Circumstances for certificate renewal....36
4.6.2. Who May Request Renewal....36
4.6.3. Processing Certificate Renewal Requests....36
4.6.4. Notification of New Certificate Issuance to Subscriber....36
4.6.5. Conduct Constituting Acceptance of a Renewal Certificate....37

4.6.6. Publication of the renewal certificate by the Certification Authority 37

4.6.7. Notification of Certificate Issuance by the CA to Other Entities 37

4.7. CERTIFICATE RE-KEY 37

4.7.1. Circumstances for Certificate Re-Key 37

4.7.2. Who May Request certification of a new public key 37

4.7.3. Processing Certificate Rekeying Requests 37

4.7.4. Notification of new certificate issuance to Subscriber 37

4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate 37

4.7.6. Publication of the Re-Keyed Certificate by the CA 37

4.7.7. Notification of Certificate Issuance by the CA to Other Entities 37

4.8. CERTIFICATE MODIFICATION 37

4.8.1. Circumstance for Certificate Modification 37

4.8.2. Who May Request Certificate Modification 37

4.8.3. Processing Certificate Modification Requests 38

4.8.4. Notification of New Certificate Issuance to Subscriber 38

4.8.5. Conduct Constituting Acceptance of Modified Certificate 38

4.8.6. Publication of the Modified Certificate by the CA 38

4.8.7. Notification of Certificate Issuance by the CA to Other Entities 38

4.9. CERTIFICATE REVOCATION AND SUSPENSION 38

4.9.1. Circumstances for revocation 38

4.9.1.1. Reasons to revoke a user certificate 38

4.9.1.2. Reasons to revoke a subordinate (intermediate) CA certificate 39

4.9.2. Who Can Request Revocation 39

4.9.3. Procedure for Revocation Request 40

4.9.3.1. Interactive telematics 40

4.9.3.2. Telematic ACME 40

4.9.3.3. Telephone 40

4.9.4. Revocation Request Grace Period 40

4.9.5. Time Within which CA Must Process the Revocation Request 40

4.9.6. Revocation Checking Requirement for Relying Parties 40

4.9.7. CRL Issuance Frequency 40

4.9.8. Maximum Latency for CRLs 41

4.9.9. On-Line Revocation/Status Checking Availability 41

4.9.10. On-Line Revocation Checking Requirements 41

4.9.11. Other Forms of Revocation Advertisements Available 41

4.9.12. Special Requirements for Key Compromise 41

4.9.13. Circumstances for suspension 42

4.9.14. Who can Request Suspension 42

4.9.15. Procedure for Suspension Request 42

4.9.16. Limits on Suspension Period 42

4.10. Certificate Status Services....42
4.10.1. Operational characteristics....42
4.10.2. Service availability....43
4.10.3. Optional features....43
4.11. End of subscription....43
4.12. Key Escrow and Recovery....43
4.12.1. Key Escrow and Recovery Policy and Practices....43
4.12.2. Session Key Encapsulation and Recovery Policy and Practices....43
4.13. Expiration of CA certificate keys....43
5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS....44
5.1. Physical Security Controls....44
5.1.1. Site Location and Construction....44
5.1.2. Physical access....44
5.1.3. Power and air conditioning....44
5.1.4. Water Exposure....44
5.1.5. Fire Protection and Prevention....44
5.1.6. Media Storage....44
5.1.7. Waste Disposal....44
5.1.8. Off-Site Backup....44
5.2. Procedural controls....45
5.2.1. Reliable papers....45
5.2.1.1. Management....45
5.2.1.2. Systems Administrator....45
5.2.1.3. PRU Administrator....46
5.2.1.4. Security Administrator....46
5.2.1.5. Certification Authority Operator....46
5.2.1.6. User Registration Point Operator....47
5.2.1.7. Training, Support and Communications Manager....47
5.2.1.8. Security Manager....47
5.2.1.9. Auditor....48
5.2.1.10. Legal Expert....48
5.2.1.11. Documentation Manager....48
5.2.1.12. Deployment Support Manager....48
5.2.1.13. Certification Authority Coordinator....49
5.2.2. Number of persons required per task....49
5.2.3. Identification and authentication for each role....49
5.2.4. Roles requiring segregation of duties....49
5.3. Personnel security controls....49
5.3.1. Qualifications, Experience, and Clearance Requirements....50
5.3.2. Background check procedures....50

5.3.3. Training requirements *50*

5.3.4. Retraining Frequency and Requirements *50*

5.3.5. Job Rotation Frequency and Sequence *50*

5.3.6. Sanctions for Unauthorized Actions *50*

5.3.7. Independent Contractor Requirements *51*

5.3.8. Documentation Supplied to Personnel *51*

5.3.9. Periodic compliance checks *51*

5.3.10. Termination of contracts *51*

5.3.10.1. Access to organizational locations 51

5.3.10.2. Access to Information Systems 52

5.3.10.3. Access to documentation 52

5.3.10.4. Information to the rest of the organization 52

5.3.10.5. Information to suppliers and collaborating entities 52

5.3.10.6. Return of material 52

5.3.10.7. Suspension as PRU Operator 52

5.4. AUDIT LOGGING PROCEDURES 53

5.4.1. Types of events recorded *53*

5.4.2. Frequency of Processing Log *53*

5.4.3. Retention Period for Audit Log *53*

5.4.4. Protection of Audit Log *54*

5.4.5. Audit log backup procedures *54*

5.4.6. Audit information collection system (internal vs. external) *54*

5.4.7. Notification to the subject causing the event *54*

5.4.8. Vulnerability Assessments *54*

5.5. RECORDS ARCHIVAL 54

5.5.1. Types of Records Archived *54*

5.5.2. Retention Period for Archive *55*

5.5.3. Protection of Archive *55*

5.5.4. Archive Backup Procedures *55*

5.5.5. Requirements for Time-Stamping of Records *55*

5.5.6. Archive Collection System (Internal or External) *55*

5.5.7. Procedures to Obtain and Verify Archive Information *55*

5.6. KEY CHANGEOVER 55

5.7. COMPROMISE AND DISASTER RECOVERY 55

5.7.1. Incident and Compromise Handling Procedures *55*

5.7.2. Computing Resources, Software, and/or Data are corrupted *56*

5.7.3. Entity Private Key Compromise Procedures *56*

5.7.4. Business Continuity Capabilities after a Disaster *56*

5.8. CA OR RA TERMINATION 56

6. TECHNICAL SECURITY CONTROLS 58

6.1. KEY PAIR GENERATION AND INSTALLATION 58
6.1.1. Key pair generation 58
6.1.1.1. CA Key Pair Generation 58
6.1.1.2. RA Key Pair Generation 58
6.1.1.3. Subscriber Key Pair Generation 58
6.1.1.3.1. Qualified Website Authentication Certificates 58
6.1.1.3.2. Electronic Administrative Headquarters Certificates in Hardware Secure Module 58
6.1.1.3.3. Electronic Administrative Headquarters Certificates based on software 59
6.1.1.3.4. Server Authentication Certificates 59
6.1.2. Private Key Delivery to Subscriber 59
6.1.3. Public Key Delivery to Certificate Issuer 59
6.1.4. CA Public Key Delivery to Relying Parties 59
6.1.5. Key Sizes 59
6.1.6. Public Key Parameters Generation and Quality Checking 59
6.1.7. Key Usage Purposes (as per X.509 v3 key usage field) 60
6.1.8. Key generation hardware/software 60
6.1.8.1. CA Keys 60
6.1.8.2. Qualified Website Authentication Certificates 60
6.1.8.3. Electronic Administrative Headquarters Certificates in Hardware Secure Module 61
6.1.8.4. Electronic Administrative Headquarters Certificates based on software 61
6.1.8.5. Server Authentication Certificates 61
6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS 61
6.2.1. Cryptographic Module Standards and Controls 61
6.2.1.1. CA Keys 61
6.2.1.2. Qualified Website Authentication Certificates 61
6.2.1.3. Electronic Administrative Headquarters Certificates in Hardware Secure Module 61
6.2.1.4. Electronic Administrative Headquarters Certificates based on software 62
6.2.1.5. Server Authentication Certificates 62
6.2.2. Private Key (n out of m) Multi-Person Control 62
6.2.3. Private Key Escrow 62
6.2.4. Private Key Backup 62
6.2.5. Private Key Archival 62
6.2.6. Private Key Transfer into or from a Cryptographic Module 62
6.2.6.1. CA Keys 62
6.2.6.2. Qualified Website Authentication Certificates 62
6.2.6.3. Electronic Administrative Headquarters Certificates in Hardware Secure Module 63
6.2.6.4. Electronic Administrative Headquarters Certificates based on software 63
6.2.6.5. Server Authentication Certificates 63
6.2.7. Storage of the private key in the cryptographic module 63
6.2.7.1. CA Keys 63
6.2.7.2. Qualified Website Authentication Certificates 63
6.2.7.3. Electronic Administrative Headquarters Certificates in Hardware Secure Module 63

6.2.7.4. Electronic Administrative Headquarters Certificates based on software 63
6.2.7.5. Server Authentication Certificates 63
6.2.8. Method of Activating Private Key 63
6.2.8.1. CA Keys 63
6.2.8.2. Qualified Website Authentication Certificates 63
6.2.8.3. Electronic Administrative Headquarters Certificates in Hardware Secure Module 64
6.2.8.4. Electronic Administrative Headquarters Certificates based on software 64
6.2.8.5. Server Authentication Certificates 64
6.2.9. Method of Deactivating Private Key 64
6.2.9.1. CA Keys 64
6.2.9.2. Qualified Website Authentication Certificates 64
6.2.9.3. Electronic Administrative Headquarters Certificates in Hardware Secure Module 64
6.2.9.4. Electronic Administrative Headquarters Certificates based on software 64
6.2.9.5. Server Authentication Certificates 64
6.2.10. Method of Destroying Private Key 64
6.2.10.1. Cryptographic hardware 64
6.2.10.2. Cryptographic cards 65
6.2.10.3. Qualified Website Authentication Certificates 65
6.2.10.4. Electronic Administrative Headquarters Certificates in Hardware Secure Module 65
6.2.10.5. Electronic Administrative Headquarters Certificates based on software 65
6.2.10.6. Server Authentication Certificates 65
6.2.11. Cryptographic Module Rating 65
6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT 65
6.3.1. Public Key Archival 65
6.3.2. Certificate Operational Periods and Key Pair Usage Periods 65
6.4. ACTIVATION DATA 66
6.4.1. Activation Data Generation and Installation 66
6.4.1.1. Certification Authorities 66
6.4.1.2. Qualified Website Authentication Certificates 66
6.4.1.3. Electronic Administrative Headquarters Certificates in Hardware Secure Module 66
6.4.1.4. Electronic Administrative Headquarters Certificates based on software 66
6.4.1.5. Server Authentication Certificates 66
6.4.2. Activation Data Protection 66
6.4.2.1. Certification Authorities 66
6.4.2.2. Qualified Website Authentication Certificates 66
6.4.2.3. Electronic Administrative Headquarters Certificates in Hardware Secure Module 66
6.4.2.4. Electronic Administrative Headquarters Certificates based on software 66
6.4.2.5. Server Authentication Certificates 66
6.4.3. Other Aspects of Activation Data 66
6.5. COMPUTER SECURITY CONTROLS 67
6.5.1. Specific Computer Security Technical Requirements 67
6.5.2. Computer Security Rating 67

6.6. LIFECYCLE TECHNICAL CONTROLS....67

6.6.1. System Development Controls....67

6.6.2. Security Management Controls....68

6.6.3. Lifecycle Security Controls....68

6.7. NETWORK SECURITY CONTROLS....68

6.8. TIME-STAMPING....69

7. CERTIFICATE, CRL AND OCSP PROFILES....70

7.1. CERTIFICATE PROFILE....70

7.1.1. Version number....70

7.1.2. Certificate Extensions; implementation of RFC 5280....70

7.1.2.1. Root CAs....70

7.1.2.2. Subordinate Cas....71

7.1.2.3. Subscriber Certificates....72

7.1.2.3.1. Qualified Website Authentication Certificates....72

7.1.2.3.2. Electronic Administrative Headquarters Certificates in Hardware Secure Module....74

7.1.2.3.3. Electronic Administrative Headquarters Certificates based on software....76

7.1.2.3.4. Server Authentication Certificates....78

7.1.3. Object Identifiers (OID) of the algorithms....80

7.1.3.1. SubjectPublicKeyInfo....80

7.1.3.1.1. RSA....80

7.1.3.1.2. ECDSA....81

7.1.3.2. Signature algorithm identifier....81

7.1.3.2.1. RSA....81

7.1.3.2.2. ECDSA....82

7.1.4. Name Forms....82

7.1.4.1. Name Encoding....84

7.1.5. Name Constraints....84

7.1.6. Certification Policy Object Identifier (OID)....84

7.1.6.1. Qualified Website Authentication Certificates....84

7.1.6.2. Electronic Administrative Headquarters Certificates in Hardware Secure Module....85

7.1.6.3. Electronic Administrative Headquarters Certificates based on software....85

7.1.6.4. Server Authentication Certificates....86

7.1.7. Usage of Policy Constraints Extension....86

7.1.8. Policy Qualifiers Syntax and Semantics....86

7.1.9. Processing Semantics for the Critical Certificate Policies Extension....86

7.1.10. Signed Certificate Timestamp (SCT) List....86

7.2. CRL PROFILE....87

7.2.1. Version number....87

7.2.2. CRL and extensions....87

7.3. OCSP PROFILE....88

7.3.1. Version number....88

7.3.2. OCSP extensions *88*

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS 89

8.1. Frequency or Circumstances of Assessment 89

8.2. Identity/Qualifications of Assessor 89

8.3. Assessor's Relationship to Assessed Entity 89

8.4. Topics Covered by Assessment 90

8.5. Actions Taken as a Result of Deficiency 90

8.6. Communication of Results 90

8.7. Self-Audits 91

9. OTHER BUSINESS AND LEGAL MATTERS 92

9.1. Fees 92

9.1.1. Certificate Issuance or Renewal Fees *92*

9.1.2. Certificate Access Fees *92*

9.1.3. Revocation or Status Information Access Fees *92*

9.1.4. Fees for Other Services *92*

9.1.5. Refund Policy *92*

9.2. Financial Responsibility 92

9.2.1. Insurance Coverage *92*

9.2.2. Other assets *92*

9.2.3. Insurance or Warranty Coverage for end-entities *92*

9.3. Confidentiality of Business Information 92

9.3.1. Scope of Confidential Information *92*

9.3.2. Information Not Within the Scope of Confidential Information *93*

9.3.3. Responsibility to Protect Confidential Information *93*

9.4. Privacy of Personal Information 93

9.4.1. Privacy Plan *93*

9.4.2. Information Treated as Private *94*

9.4.3. Information not Deemed Private *95*

9.4.4. Responsibility to Protect Private Information *95*

9.4.5. Notice and Consent to Use Private Information *95*

9.4.6. Disclosure Pursuant to Judicial or Administrative Process *95*

9.4.7. Other Information Disclosure Circumstances *96*

9.5. Intellectual Property Rights 96

9.6. Representations and Warranties 96

9.6.1. CA Representations and Warranties *96*

9.6.2. RA Representations and Warranties *98*

9.6.3. Subscriber Representations and Warranties *99*

9.6.4. Relying Party Representations and Warranties *99*

9.6.5. Representations and Warranties of other Participants *100*

9.7. Disclaimer of Warranties 100

9.8. Limitations of Liability 100

9.9. Indemnities 101

9.10. Term and Termination 101

9.10.1. Term *101*

9.10.2. Termination *101*

9.10.3. Effect of Termination and Survival *101*

9.11. Individual Notices and Communications with Participants 102

9.12. Amendments 102

9.12.1. Procedure for Amendment *102*

9.12.2. Notification Mechanism and Period *102*

9.12.3. Circumstances Under Which OID Must be Changed *102*

9.13. Dispute Resolution Provisions 102

9.14. Governing Law 103

9.15. Compliance with Applicable Law 103

9.16. Miscellaneous Provisions 103

9.16.1. Entire Agreement *103*

9.16.2. Assignment *104*

9.16.3. Severability *104*

9.16.4. Enforcement (Attorneys' Fees and Waiver of Rights) *104*

9.16.5. Force Majeure *104*

9.17. Other Provisions 104

10. ANNEX I **105**

10.1. Qualified Website Authentication Certificates 105

10.2. Electronic Administrative Headquarters Certificates in Hardware Secure Module 107

10.3. Electronic Administrative Headquarters Certificates based on software 109

10.4. Server Authentication Certificates 111

1. INTRODUCTION

1.1. Overview

This document contains the *Declaration of Certification Practices and Policies (CPS)* of Agencia de Tecnología y Certificación Electrónica in the issuance of website authentication certificates.

Agencia de Tecnología y Certificación Electrónica (ACCV) is part of Infraestructures i Serveis de Telecomunicacions i Certificació, SAU (ISTEC), public law entity with its own legal personality and full capacity to fulfill its purposes, which is governed by its Statutes.

In accordance with the above, in compliance with current legislation and aligned with Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC and its amendment in Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) n.° 910/2014 regarding the establishment of the European digital identity framework, this Declaration of Certification Practices and Policies (CPS) details the rules and general conditions of the certification services provided by the Agencia de Tecnología y Certificación Electrónica, in relation to the management of signature creation and verification data and electronic certificates, the conditions applicable to the request, issuance, use, suspension and termination of the validity of the certificates, the technical and organizational security measures, profiles and information mechanisms on the validity of the certificates and, where appropriate, the existence of coordination procedures with the corresponding public registries that allow the immediate exchange of information on the validity of the powers of attorney indicated in the certificates and that must be registered in these registries, always in the scope of website authentication certificates.

Thus, this Certification Practices Statement is the compendium of standards applicable to the certification activity of the Agencia de Tecnología y Certificación Electrónica (ACCV) as a Qualified Trust Service Provider in the issuance of website authentication certificates.

It should also be noted that this Certification Policy and Practices Statement is drafted following the specifications of RFC 3647 *"Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*" proposed by the *Network Working Group* for this type of documents.

Finally, it should be noted that the Agencia de Tecnología y Certificación Electrónica (ACCV) follows the current version of the document "*Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates*" published in https://wwww.cabforum.org/. In the case of any incompatibility between this document and the CAB Forum requirements, these requirements will prevail.

ACCV will NOT issue official certificates signed by Certification Authorities that have not passed the necessary audits and certifications in each case.

1.2. Document Name and Identification

Name of document	Certification Practices and Policies for website authentication certificates
Document version	4.0.17
Document status	APPROVED
CPS/ OID (Object Identifier) Reference	1.3.6.1.4.1.1.8149.2.4.0
Date of issue	03/06/2025
Expiration date	Not applicable.
Location	This CPS can be found at http://www.accv.es/pdf-politicas

Website Authentication Certificate is a type of certificate used to confirm the identity of the website to which users connect, using public key cryptography techniques and by using well-established protocols that provide data encryption and authentication between applications and servers (TLS/SSL).

The following types of certificates are issued under this CPS:

Name	OID owner
Qualified Website Authentication Certificates	1.3.6.1.4.1.8149.3.3.5.0
Qualified Certificates of electronic administrative headquarter in hardware secure module -HSM-.	1.3.6.1.4.1.8149.3.14.6.0
Qualified Certificates of electronic administrative headquarters based on software	1.3.6.1.4.1.8149.3.15.6.0
Server Authentication Certificates	1.3.6.1.4.1.8149.3.36.2.0

All certificates issued under this CPS are OV (Organization Validated), which means that they follow at least the OVCP issuance and management requirements as described in

https://cabforum.org/working-groups/server/baseline-requirements/documents/

1.3. PKI Participants

1.3.1. Certification Authorities

In this Certification Practice Statement, the acronym "ACCV" will be used to designate the Certification Authorities that make up the Agencia de Tecnología y Certificación Electrónica.

The Certification Authorities that make up ACCV are structured in several certification hierarchies, composed of several root and subordinate Certification Authorities.

The hierarchies under the scope of application of this CPS are made up of the following certification authorities

1.3.1.1. Root Certification Authorities

First level Certification Authority. Its function is to establish the root of the new trust model of the Public Key Infrastructure or PKI. This CA does not issue certificates for end entities. This first level Certification Authority is self-signed, issuing a certificate whose signer is the Certification Authority itself, and which contains the public key (or signature verification data) signed with the signature creation data (private key).

1.3.1.1.1. ACCVRAIZ1

- ○ C=EN,O=ACCV,OU=PKIACCV,CN=ACCVRAIZ1
- ○ Fingerprint (HASH) SHA1:
- **93057A8815C64FCE882FFA9116522878BC536417**
- ○ Fingerprint (HASH) SHA256:
- **9A6EC012E1A7DA9DBE34194D478AD7C0DB1822FB071DF12981496ED104384113**

Valid from May 5, 2011 to December 31, 2030.

Key type: RSA 4096 bits - SHA1

1.3.1.1.2. ACCV ROOT ECC TLS 2024

  - CN=ACCV ROOT ECC TLS 2024,2.5.4.97=VATES-A40573396,O=ISTEC,L=BURJASSOT,ST=VALENCIA,C=ES
  - Fingerprint (HASH) SHA1:
- **2E529E361D817B33E1FE095E91A4EB969458B3F4**
  - Fingerprint (HASH) SHA256:
- **79CD55455296ADFB55CDF0DBE9176985A0B503C544276C5A9305F2EC9B66693A**

Valid from February 27, 2024 to January 26, 2049.

Key type: ECDSA P384 SHA384

1.3.1.1.3. ACCV ROOT RSA TLS 2024

  - CN=ACCV ROOT RSA TLS 2024,2.5.4.97=VATES-A40573396,O=ISTEC,L=BURJASSOT,ST=VALENCIA,C=ES
  - Fingerprint (HASH) SHA1:
- **970ABA25EC3D78649B305BA75F8C914C275D8654**
  - Fingerprint (HASH) SHA256:
- **B40BFA8880A02F93025643C6DBBD39DF194A2854D076E167A2BD8467CF9E2C34**

Valid from February 27, 2024 to January 26, 2049.

Key type: RSA 4096 SHA512

1.3.1.2. Subordinate Certification Authorities

- ACCVRAIZ1 root

- "ACCVCA-110"

Valid from May 7, 2015 until January 1, 2027.

SHA256 Fingerprint:

E9327A347CBE1CB94CDC9AA54CB31B6E43D68968D17D09CE326A091BFC2F0B11

SHA1 Fingerprint:

677CDF63B95E9EAEAE696F44506718FE0D2F6E41

Key type: RSA 4096 bits - SHA256

- "ACCVCA-120.

Valid from January 27, 2015 to January 01, 2027.

SHA256 Fingerprint:

2DE620F2D1200AA90B16C3CCF670FD7ED14379AB06FA8B031CFEF8DA051EA5A2

SHA1 Fingerprint:

4872A4C3DF174CEF34D77FE6A3B4E7BE7DF2D25D

Key type: RSA 4096 bits - SHA256

- "ACCVCA-130"

Valid from January 15, 2015 to January 1, 2027.

SHA256 Fingerprint:

572BF899FD774362DC19219625ECC157BB55434EA5166D5758DC4B4F890D6653

SHA1 Fingerprint:

0055B77F432B54245406068CC8F77805C325DCF5

Key type: RSA 4096 bits - SHA256

- ACCV ROOT root **ECC TLS 2024**

- "ACCV ECC1 TLS"

Valid from February 27, 2024 to February 23, 2039.

SHA256 Fingerprint:

93C087AB9331B74C0FCCCE11BC61FB9FA6D432077D8F1018194FA4CCA664D781

SHA1 Fingerprint:

4F35E0547A8E74D9D3EC1B260F0F9AD4809246E3

Key type: ECDSA P384 SHA384

- ACCV ROOT RSA TLS 2024 ACCV ROOT RSA TLS 2024 Root

- "ACCV RSA1 TLS"

Valid from February 27, 2024 to February 23, 2039.

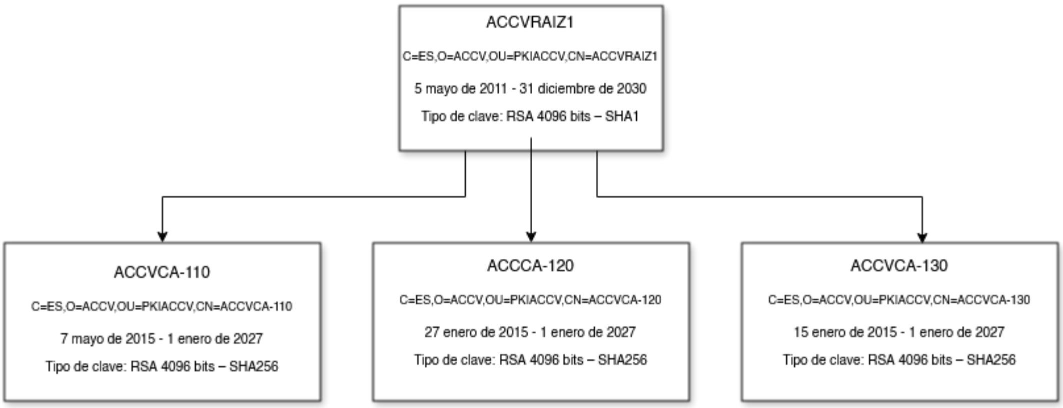
SHA256 Fingerprint:

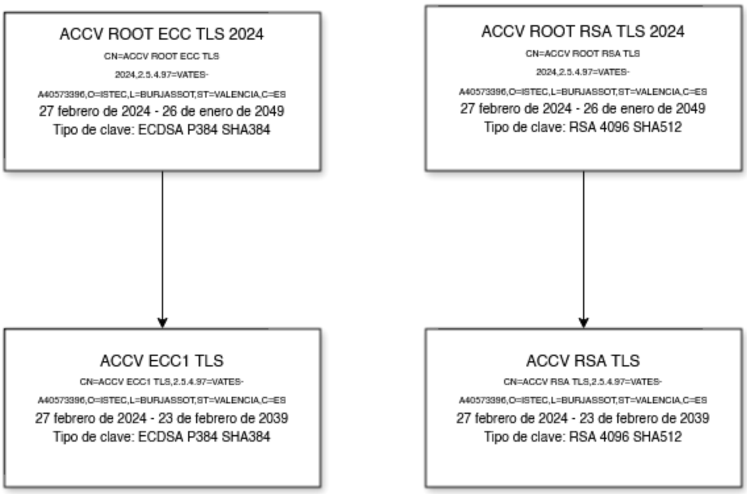
346440CF7674A529305545563322FCFB38F5A4B3F1E7E852DFF8A4B7A5EF72D1

SHA1 Fingerprint:

D9698B1190136DAE3C3B0164329D050AB84D416D

Key type: RSA 4096 SHA512


ACCVRAIZ1
C=ES,O=ACCV,OU=PKIACCV,CN=ACCVRAIZ1
5 mayo de 2011 - 31 diciembre de 2030
Tipo de clave: RSA 4096 bits – SHA1
ACCVCA-110
C=ES,O=ACCV,OU=PKIACCV,CN=ACCVCA-110
7 mayo de 2015 - 1 enero de 2027
Tipo de clave: RSA 4096 bits – SHA256
ACCCA-120
C=ES,O=ACCV,OU=PKIACCV,CN=ACCVCA-120
27 enero de 2015 - 1 enero de 2027
Tipo de clave: RSA 4096 bits – SHA256
ACCVCA-130
C=ES,O=ACCV,OU=PKIACCV,CN=ACCVCA-130
15 enero de 2015 - 1 enero de 2027
Tipo de clave: RSA 4096 bits – SHA256


ACCV ROOT ECC TLS 2024
CN=ACCV ROOT ECC TLS 2024,2.5.4.97=VATES-A40573396,O=ISTEC,L=BURJASSOT,ST=VALENCIA,C=ES
27 febrero de 2024 - 26 de enero de 2049
Tipo de clave: ECDSA P384 SHA384
ACCV ROOT RSA TLS 2024
CN=ACCV ROOT RSA TLS 2024,2.5.4.97=VATES-A40573396,O=ISTEC,L=BURJASSOT,ST=VALENCIA,C=ES
27 febrero de 2024 - 26 de enero de 2049
Tipo de clave: RSA 4096 SHA512
ACCV ECC1 TLS
CN=ACCV ECC1 TLS,2.5.4.97=VATES-A40573396,O=ISTEC,L=BURJASSOT,ST=VALENCIA,C=ES
27 febrero de 2024 - 23 de febrero de 2039
Tipo de clave: ECDSA P384 SHA384
ACCV RSA TLS
CN=ACCV RSA TLS,2.5.4.97=VATES-A40573396,O=ISTEC,L=BURJASSOT,ST=VALENCIA,C=ES
27 febrero de 2024 - 23 de febrero de 2039
Tipo de clave: RSA 4096 SHA512

1.3.2. Registration Authorities

The only Registration Authority for website authentication certificates is ACCV, and performs the identification and verification of the applicant and verification of all data included in the certificate, with special emphasis on the verifications necessary to verify the possession of the domain or domains by the certificate applicant. To this end, the Registration Authority will ensure that the certificate application contains truthful and complete information, and that it complies with the requirements of the corresponding Policy.

The basic functions of the Registration Authority extend to:

- Verify the identity and any personal circumstances of certificate applicants relevant to the purpose of the certificate.
- Prior to the issuance of the certificate, inform the person requesting it of the precise conditions for the use of the certificate and its limitations of use.
- Verify that the information contained in the certificate is accurate and that it includes all the information prescribed for a certificate of the type in question.
- Ensure that the signatory is in possession of the signature creation data corresponding to the verification data contained in the certificate.

- Verify by the established and accepted methods for this type of certificates the possession of the domain or domains by the applicant.

1.3.3. Subscribers

The group of users that can request certificates defined by this policy is made up of those responsible for public or private entities, in a position to represent the requesting entity.

In the case of public entities, requests can be made by Heads of Service or equivalent organizational positions in any type of Public Administration (European, state, regional and local), who are ultimately responsible for their use within the different projects or information systems. These (or to whom they explicitly delegate) are the only subscribers authorized to request e-Office certificates.

In the case of private entities, the certificates may be requested by those persons with the capacity to represent the entity or who have been authorized to manage this type of certificates.

The right to request certificates defined in this Certification Policy is limited to individuals. Certification requests made by legal persons, entities or organizations will not be accepted without a natural person identified as the applicant.

1.3.4. Relying parties

The right to rely on certificates issued in accordance with these practices and policies is limited to:

1. Users of application clients in the area of identity verification of the websites they connect to and encryption of the channel of data transmitted between them.
2. Applications and services with SSL and/or TLS support capabilities, in the field of verification of the identity of the websites to which they connect, and of the encryption of the channel of the data transmitted between them.

1.3.5. Other participants

1.3.5.1. Applicants

An Applicant is the natural person who, in his own name or as representative of a third party, and after identification, requests the issuance of a Certificate.
In the case of Certificate Applicants whose Subscriber is a legal entity, such natural person may only be a legal or voluntary representative or an administrator with sufficient powers for this purpose of the legal entity that will be the subscriber of the certificate.

1.4. Certificate Usage

The Certification Policies corresponding to each type of certificate issued by ACCV are the documents that determine the uses and limitations of each certificate. This CPS establishes the uses and limitations for certificates issued for website authentication..

1.4.1. Appropriate Certificate Uses

Certificates issued by ACCV under this CPS can be used to provide websites with SSL/TLS capabilities. Also, and as long as the uses allow it, they can be used as a mechanism to identify these sites unequivocally to services and software applications.

The Certificates of Electronic Administrative Headquarters are a subset of Website Authentication Certificates, which are issued as identification systems of an Electronic Administrative Headquarters that guarantees secure communication with it, in the terms defined in Law 40/2015, of October 1, on the Legal Regime of the Public Sector and in Law 18/2011, of July 5, regulating the use of information and communication technologies in the Administration of Justice.

1.4.2. Prohibited Certificates Uses

Certificates issued by ACCV for website authentication will be used only in accordance with the function and purpose established in this Certification Practices and Policies Statement, and in accordance with current regulations.

1.5. ACCV Policy Administration

1.5.1. Organization Administering the Document

Name	*Agencia de Tecnología y Certificación Electrónica*
E-mail address	*accv@accv.es*
Address	*Pol. Ademuz, s/n.- 46100 Burjassot (Spain)*
Telephone number	*+34 963 866 014*

1.5.2. Contact Person

Name	*Agencia de Tecnología y Certificación Electrónica*
E-mail address	*accv@accv.es*
Address	*Pol. Ademuz, s/n. - 46100 Burjassot (Spain)*
Telephone number	*+34 963 866 014*

1.5.2.1. Problem Reporting Address

The user can provide information regarding compromised keys or incorrect certificates by using the form https://www.accv.es/contacta/.
In the form the user can paste the certificate or keys in PEM format, including the BEGIN and END lines.
You can also use directly the address for sending detected problems problem_reporting@accv.es (the form sends a copy to that address).
In the case of ACME certificates, the account owner can use the mechanism enabled following the protocol for revocation:

https://npsc.accv.es:8450/npsc/acme/revoke-cert

1.5.3. Person determining CPS suitability for the policy

The competent entity to determine the adequacy of this CPS is Infraestructures i Serveis de Telecomunicacions i Certificació, SA (ISTEC) in accordance with its bylaws.

1.5.4. CPS approval procedures

ISTEC approves the CPS and its possible modifications. Modifications are made by updating the entire CPS or by publishing an addendum. ISTEC determines whether a modification to this CPS requires a notification or an OID change.

ISTEC will review its certification policies and practices and update this Certification Policy and Practice Statement annually to keep it in line with the latest version of the requirements defined in "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates", published at https://www.cabforum.org/, increasing the version number and adding a dated changelog entry, even if no other changes were made to the document.

1.6. Definitions and Acronyms

1.6.1. Definitions

For the purpose of determining the scope of the concepts that are used in this Certification Practices Statement, it shall be understood as follows:

- Certification Authority: is the natural or legal person that, in accordance with the legislation on electronic signatures, issues electronic certificates, and may also provide other services related to electronic signatures. For the purposes of this Certification Practices Statement, Certification Authorities are all those defined as such.
- Registration Authority: natural or legal person that ACCV designates to verify the identity of applicants and subscribers of certificates, and if applicable, the validity of the powers of representatives and subsistence of legal personality or voluntary representation. In ACCV they are also called User Registration Points or PRU.
- Bastioning: is the process by which a specific security policy is implemented on an operating system installation. The bastioning of a computer is intended to reduce the level of exposure of a computer and, therefore, the risks and vulnerabilities associated with it.
- Certification chain: list of certificates containing at least one certificate and ACCV root certificate.
- Certificate: electronic document electronically signed by a Certification Service Provider that binds the subscriber to signature verification data and confirms the identity of the subscriber. In this Certification Practices Statement, when reference is made to a certificate, it means a Certificate issued by ACCV.
- Root certificate: Certificate whose subscriber is ACCV and belongs to the hierarchy of ACCV as Certification Service Provider, and contains the signature verification data of the Certification Service Provider, signed with the signature creation data of ACCV as Certification Service Provider.
- Qualified certificate: certificate issued by a Trusted Service Provider that meets the requirements established in Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 regarding the verification of the identity and other circumstances of the applicants and the reliability and guarantees of the certification services they provide. To be considered as a qualified certificate it must appear on the trusted list (TSL) referred to in Article 22(1) of that Regulation.
- Websites Authentication Certificate: A Certificate that authenticates a website and links the website to the natural or legal person to whom the Certificate has been issued.
- OV Certificate: Web site authentication certificate issued according to the Organization Validation Policy (OVCP), guaranteeing the user that the owner of the web site he/she is accessing is the same as the Organization identified by the OV Certificate.
- Electronic Headquarters Certificate: Certificate of authentication of websites that identifies an Electronic Headquarters, guaranteeing secure communication with the same in the terms defined in Law 40/2015, of October 1, 2015, of the Public Sector Legal Regime.
- Key: sequence of symbols.
- Signature creation data (Private Key): unique data, such as codes or private cryptographic keys, used by the subscriber to create the electronic signature.
- Signature verification data (Public Key): data, such as codes or public cryptographic keys, used to verify the electronic signature.
- Certification Practices Statement: ACCV's statement made available to the public electronically and free of charge by the Certification Service Provider in compliance with the provisions of the Law.

- Secure Signature Creation Device: instrument used to apply signature creation data complying with the requirements set forth in Regulation (EU) No 910/2014 (Annex II Requirements for Qualified Electronic Signature Creation Devices).
- Certificate Directory: repository of information that follows the ITU-T X.500 standard.
- Electronic document: information of any nature in electronic form, stored in an electronic support according to a specific format, and susceptible of identification and differentiated treatment.
- Register of Activities: document required by Regulation (EU) 2016/679 whose purpose is to establish the security measures implemented, for the purposes of this document, by ACCV as Certification Service Provider, for the protection of personal data contained in the files of the certification activity that contain personal data (hereinafter the Files).
- Data Processor: the natural or legal person, public authority, service or any other body that processes personal data on behalf of the controller of the files.
- Qualified electronic signature: an advanced electronic signature based on a qualified certificate and generated by means of a qualified signature creation device.
- Advanced electronic signature: is an electronic signature that allows to establish the personal identity of the subscriber with respect to the signed data and to verify the integrity of the same, since it is exclusively linked to the subscriber and to the data to which it refers, and because it has been created by means that are under the subscriber's exclusive control.
- Electronic signature: is the set of data in electronic form, consigned together or associated with others, which can be used as a means of personal identification.
- Hash function: is an operation performed on a set of data of any size, so that the result obtained is another set of data of fixed size, regardless of the original size, and which has the property of being uniquely associated to the initial data, i.e., it is impossible to find two different messages that generate the same result when applying the hash function.
- Hash or Fingerprint: a fixed-size result obtained after applying a hash function to a message and which has the property of being uniquely associated with the initial data.
- Public Key Infrastructure (PKI): infrastructure that supports the issuance and management of keys and certificates for authentication, encryption, integrity, or non-repudiation services.
- Certificate Revocation Lists or Revoked Certificates Lists: list containing only the lists of revoked or suspended certificates (not expired ones).
- Cryptographic Security Hardware Module: hardware module used to perform cryptographic functions and store keys in secure mode.
- Certificate Serial Number: a unique integer value that is unequivocally associated with a certificate issued by CA.
- Multi-Perspective Issuance Corroboration: A process by which the determinations made during domain validation and CAA checking by the Primary Network Perspective are corroborated by other Network Perspectives before Certificate issuance.
- OCSP (Online Certificate Status Protocol): computer protocol that allows the status of a certificate to be checked at the time it is used.
- OCSP Responder: computer server that responds, following the OCSP protocol, to OCSP requests with the status of the certificate being queried.
- OID (Object Identifier): value of hierarchical nature and comprising a sequence of variable components, but always consisting of non-negative integers separated by a dot, which can be assigned to registered objects and which have the property of being unique among the rest of the OIDs.
- OCSP Request: request for a certificate status query to OCSP Responder following the OCSP protocol.

- PIN: (Personal Identification Number) specific number only known by the person who has to access a resource that is protected by this mechanism.
- Certification Service Provider: is a natural or legal person who, in accordance with the legislation on electronic signatures, issues electronic certificates, and may also provide other services related to electronic signatures. In this Certification Practices Statement will correspond to the Certification Authorities belonging to ACCV hierarchy.
- Certification Policy: document that completes the Certification Practices Statement, establishing the conditions of use and procedures followed by ACCV to issue Certificates.
- PKCS#10 (Certification Request Syntax Standard): standard developed by RSA Labs, and accepted internationally as a standard, which defines the syntax of a certificate request.
- Pre-certificate: Signed data structure that can be sent to a Certificate Tramsparency log, as defined in RFC 6962.
- PUK: (Personal Unblocking Key) a specific number or key known only to the person who has to access a resource that is used to unlock access to that resource.
- CAA records: DNS (Domain Name System) Certification Authority Authorization (CAA) resource record. It allows a DNS domain name holder to specify the Certification Authorities (CAs) authorized to issue certificates for that domain. The publication of CAA resource records allows a domain name registrant to implement additional controls to reduce the risk of unauthorized issuance.
- File Manager (or File Processor): the person who decides on the purpose, content and use of the processing of the Files.
- Security Manager: in charge of coordinating and controlling the measures imposed by the security document regarding the files.
- Electronic headquarters: Electronic address, available to citizens through telecommunications networks, whose ownership corresponds to a Public Administration, or to one or more public bodies or Public Law entities in the exercise of their competences.
- SHA Secure Hash Algorithm. A family of encryption hash functions published by the National Institute of Standards and Technology (NIST). The first version of the algorithm was created in 1993 under the name SHA, although it is now known as SHA-0 to avoid confusion with later versions. The second version of the system, published under the name SHA-1, was released two years later. Subsequently, SHA-2 has been published in 2001 (consisting of several functions: SHA-224, SHA-256, SHA-384, and SHA-512) and the most recent, SHA-3, which was selected in a hash function competition held by NIST in 2012). The algorithm consists of taking messages of less than 264 bits and generating a fixed-length digest. The probability of finding two different messages that produce the same digest is practically zero. For this reason it is used to ensure the integrity of documents during the electronic signature process.
- Time-Stamping: The date and time stamping of an electronic document by means of indelible cryptographic procedures, based on the specifications Request For Comments: 3161 - "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)", which enables the document to be objectively dated.
- Applicant: natural person who requests the issuance of a certificate.
- Subscriber (or Subject): the certificate holder or signer. The person whose personal identity is linked to the electronically signed data, through a public key certified by the Certification Service Provider. The concept of subscriber will be referred to in the certificates and in the software applications related to their issuance as Subject, for strict reasons of international standardization.
- Cryptographic card: card used by the subscriber to store private signature and decryption keys, to generate electronic signatures and decrypt data messages. It is considered a secure signature creation device in accordance with the Electronic Signature Law and allows the generation of recognized electronic signatures.

- Relying third parties or trusting parties: those persons who place their trust in an ACCV certificate, verifying the validity and validity of the certificate as described in this Certification Practices Statement and in the Certification Policies associated with each type of certificate.
- X.500: standard developed by the ITU that defines the directory recommendations. It corresponds to the ISO/IEC 9594-1: 1993 standard. It gives rise to the following series of recommendations: X.501, X.509, X.511, X.518, X.519, X.520, X.521 and X.525.
- X.509: standard developed by the ITU, which defines the basic electronic format for electronic certificates.

1.6.2. Acronyms

ACCV	Agencia de Tecnología y Certificación Electrónica
CA	Certification Authority
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DGTIC GVA	Directorate General of Information and Communication Technologies Generalitat Valenciana
FIPS	Federal Information Processing Standard
IETF	Internet Engineering Task Force
IVF	Valencian Institute of Finance
ISTEC	Telecommunication Infrastructures and Services and Certification
OID	Object identifier
OCSP	On-line Certificate Status Protocol
OPRU	Registration Point Operator
OV	Organization Validated
PKI	Public Key Infrastructure
PKIGVA	ACCV PKI
PRU	User Registration Point
RA	Registration Authority
RFC	Request For Comment
SSL	Secure Sockets Layer
Sub CA	Subordinate Certification Authority
TLS	Transport Security Layer

2. Publication and Repository Responsibilities

2.1. Certificate repository

The certificate repository service will be available 24 hours a day, 7 days a week, and in case of interruption due to force majeure, the service will be restored as soon as possible.

ACCV repository is composed of:

OCSP server according to RFC-6960 accessible at: http://ocsp.accv.es

URL for access to certificates with high availability

ACCVRAIZ1: https://www.accv.es/fileadmin/Archivos/certificados/ACCVRAIZ1.crt

ACCVCA-110: https://www.accv.es/fileadmin/Archivos/certificados/ACCVCA110SHA2.cacert.crt

ACCVCA-120: https://www.accv.es/fileadmin/Archivos/certificados/ACCVCA120.crt

ACCVCA-130: https://www.accv.es/fileadmin/Archivos/certificados/ACCVCA130SHA2.cacert.crt

ACCV ROOT RSA TLS 2024: http://www.accv.es/gestcert/accv_root_rsa_tls_2024.crt

ACCV RSA1 TLS: http://www.accv.es/gestcert/accv_rsa1_tls.crt

ACCV ROOT ECC TLS 2024: http://www.accv.es/gestcert/accv_root_ecc_tls_2024.crt

ACCV ECC1 TLS: http://www.accv.es/gestcert/accv_ecc1_tls.crt

URL of access to CRLs with high availability

ACCVRAIZ1: http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1_der.crl

ACCVCA-110: http://www.accv.es/fileadmin/Archivos/certificados/accvca110_der.crl

ACCVCA-120: http://www.accv.es/fileadmin/Archivos/certificados/accvca120_der.crl

ACCVCA-130: http://www.accv.es/fileadmin/Archivos/certificados/accvca130_der.crl

ACCV ROOT RSA TLS 2024: http://www.accv.es/gestcert/accv_root_rsa_tls_2024.crl

ACCV RSA1 TLS: http://www.accv.es/gestcert/accv_rsa1_tls.crl

ACCV ROOT ECC TLS 2024: http://www.accv.es/gestcert/accv_root_ecc_tls_2024.crl

ACCV ECC1 TLS: http://www.accv.es/gestcert/accv_ecc1_tls.crl

ACCV repository does not contain any information of a confidential nature and no other repository operated by any other organization is used.

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, the latter shall take precedence over this document.

Among the conditions established is the obligation to revoke the certificates if it is detected that the issuance or operation does not comply with that defined in the regulations. **This revocation must be made within a maximum period of between one (1) and five (5) calendar days (depending on the type of non-compliance) and no postponement of any kind is possible. If it is not possible to comply with this condition, certificates issued under this regulation should never be used.**

2.2. Publication

It is the obligation of the CAs belonging to ACCV trust hierarchy to publish information regarding their practices, their certificates and the updated status of such certificates.

This CPD is public and is available on ACCV website http://www.accv.es/fileadmin/Archivos/Practicas_de_certificacion/ACCV-CPS-CP-V4.0.17-EN-2025.pdf, in PDF format.

ACCV Certification Policies are public and are available on ACCV website http://www.accv.es/pdf-politicas, in PDF format.

ACCV CA certificate is public and is available in ACCV repository, in X.509 v3 format. It is also available at http://www.accv.es.

The certificates issued by ACCV are public and are available in ACCV repository, in X.509 v3 format.

The list of certificates revoked by ACCV is public and is available, in CRL v2 format, in ACCV repository.

ACCV provides test web pages that allow application software vendors to test their software with subscriber certificates that are chained to each publicly trusted root certificate.

- ACCVCA-120

  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 RSA1 TLS

  VALID

  https://activonjrsa.accv.es/test/hola.html

  REVOKED

  https://revocadonjrsa.accv.es:442/test/hola.html

  EXPIRED

  https://caducadonjrsa.accv.es:444/test/hola.html

- ACCV ECC1 TLS

  VALID

  https://activonjecc.accv.es/test/hola.html

  REVOKED

  https://revocadonjecc.accv.es:442/test/hola.html

  EXPIRED

  https://caducadonjecc.accv.es:444/test/hola.html

Within the scope of the Certificate Transparency project, in the case of TLS certificates (such as those issued under this CPS), pre-certificates will be published in the CT Log service of qualified log server providers to meet project requirements.

2.3. Time or Frequency of Publication

This CPS shall be published each time it is modified, carrying out an annual review to verify compliance and adaptation to new directives and technical standards. This revision shall be indicated by changing the minor version number.

Certificates issued by the CA will be published immediately after issuance.

The CA shall add the revoked certificates to the relevant CRL within the time period stipulated in section 4.4.9 *Frequency of issuance of CRLs*.

2.4. Access Controls on Repositories

Access to read the information in ACCV repository and on its website is free of charge.

Only ACCV is authorized to modify, replace or delete information from its repository and website. In this regard, ACCV uses appropriate means of control in order to restrict the ability to write or modify these elements.

3. Identification and Authentication

3.1. Naming

3.1.1. Types of names

All certificate subscribers require a non-null distinguished name compliant with the X.500 standard.

TLS Certificates in general include entries in the subjectAlternativeName (SAN) extension which are intended to be relied upon by relying parties.

3.1.2. Need for Names to be Meaningful

In all cases the distinguished name must make sense. This CPS describes the attributes used for the distinguished name in the points in 7.1.2 and 7.1.4. The names in the certificates identify the subject and the issuer respectively.

The subject name in CA Certificates MUST match the issuer name in Certificates issued by the

CA, as required by the RFC5280.

3.1.3. Anonymity or Pseudonymity of Subscribers

ACCV does not issue pseudonym certificates for server authentication.

3.1.4. Rules for Interpreting Various Name Forms

The rules used by ACCV to interpret the distinguished names of the certificates it issues are those contained in ISO/IEC 9594 (X.500) Distinguished Name (DN) and RFC-2253.

3.1.5. Uniqueness of names

Distinctive names must identify the subscriber and shall be unambiguous.

ACCV does not enforce uniqueness of distinguished names. As a difference, the assigned serial numbers included in the certificates are unique. ACCV generates serial numbers of at least 64 bits. These numbers are the result of a CSPRNG. It is verified that the serial numbers are never reused.

In the case of TLS certificates the CN may be missing or optionally one of the names included in the Subject Alternative Name extension may be used. The second option is not recommended.

3.1.6. Recognition, Authentication, and Role of Trademarks

The inclusion of a name in a certificate does not imply the existence of any right over it and is without prejudice to the best rights that third parties may have.

ACCV does not act as arbitrator or mediator, nor does it resolve any disputes concerning ownership of names of persons or organizations, domain names, trademarks or trade names, etc.

ACCV reserves the right to refuse an application for a certificate because of a name conflict.

The Spanish Patent and Trademark Office of the Ministry of Industry, Commerce and Tourism has granted the following trademarks owned by ISTEC.

- “Autoritat de Certificació de la Comunitat Valenciana", mixed trademark nº 2.591.232, granted on September 15, 2004, published in the Official Bulletin of Industrial Property of October 16, 2004.

Autoritat de Certificació
de la Comunitat Valenciana

- “ACCV", trademark nº 2.591.037, granted on May 19, 2005, published in the Spanish Official Industrial Property Gazette on June 16, 2005.

- "Agencia de Tecnología y Certificación Electrónica", trademark nº 2.943.180, applied for at the Spanish Official Industrial Property Office on August 13, 2010.

ACCV deliberately prohibits the use of a name whose right of use is not owned by the subscriber. However, it is not required to seek proof of trademark ownership before issuing certificates.

3.2. Initial Identity Validation

3.2.1. Method to Prove Possession of Private Key

In the event that the key pair is generated by the final entity (subscriber) externally to the tools and applications provided by ACCV, the subscriber must prove possession of the private key corresponding to the public key requested to be certified by sending the certification request signed by the private key associated with the public key provided.

3.2.2. Authentication of Organization Identity

ACCV makes no commitments in the issuance of certificates regarding the use of a trademark or trade name, deliberately not allowing the use of a name whose right of use is not owned by the Subscriber. In case of dispute, ACCV may refuse the application or revoke any certificate without liability. ACCV will use the tools indicated in this point to perform the corresponding searches and confirm the rights of use.

ACCV uses the mechanisms established by the technical regulations in force, specifically Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on the establishment of minimum technical specifications and procedures for the security levels of electronic identification methods, as provided for in Article 8(3) of Regulation (EU) No. 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

The right to request certificates as defined in this CPS is limited to subscribers identified as natural persons. Certification requests made by subscribers identified as legal persons, entities or organizations will not be accepted.

The applicant's identity is authenticated by using his or her qualified personal certificate, signing with it the request for the website authentication certificate when identifying himself or herself in the application that ACCV makes available to users for this function (NPSC https://npsc.accv.es:8450/npsc).

The applicant must submit the necessary documentation as determined by

Data relating to the entity such as inclusion in the corresponding commercial register, domicile, locality, state or province, country, operating codes, etc.

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

Possession of the domain

This presentation must be made using the sources and applications that ACCV makes available to users for this purpose.

ACCV will check the data provided (including the applicant's country) using the information available at:

Official gazettes

https://boe.es/diario_boe/

https://dogv.gva.es/va/inici/

Data Protection Agencies

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

Public Administration Registries

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

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

https://www.pap.hacienda.gob.es/invente2/pagMenuPrincipalV2.aspx

Commercial registries

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

Patent and Trademark Offices

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

Identity Verification and Consultation Services

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

requesting from the applicant any corrections or additional documents it may consider necessary.

All agencies and records used are official and highly reliable, providing traceable evidence of all searches.

ACCV retains this information for audit purposes, allowing it to be reused for a period of no more than 13 months from its last verification.

Domain verification

ACCV will verify that the domain of the certificates and their associated addresses belong to the applicant's data using the information available from the personal and domain registries, requiring from the applicant any additional explanations or documents it may consider necessary and including in the process technically reliable verification mechanisms approved by the industry.

ACCV retains domain check information for audit purposes but does not reuse it, verifying the domain for each request independently. ACCV will not issue certificates for IP addresses or private domain names, and entries in the dNSName must be in the "preferred name syntax" as specified in RFC 5280, and therefore must not contain underscore characters ("_"). For gTLDs, certificates will only be issued with approved gTLD names, and will only be issued to subscribers who have control of the gTLD, as listed in ICANN/IANA.

Specifically:

- Verification that the applicant, whose identity has been verified beyond doubt, is one of the owners of the domain. For this verification, ACCV must use one or more of the following methods:

  Contact by mail, sending a unique random number in the mail to one or more addresses created using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at sign ("@"), followed by a domain name to authorize, including a random value in the email, and receiving a confirmation reply using the same random value as the initial email. ACCV must wait no longer than 30 days for the response and must confirm that the response includes the same random number.

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

  Confirm the presence of a random value included in the contents of a file under the "/.well-known/pki-validation" directory in the domain name to be authorized. This URL must be accessible by the CA via HTTP/HTTPS over an Authorized Port. Once the value has been communicated to the applicant, it will only be valid for 30 days. In the URL, the content of the file does not appear in any case and only 200 is considered as the correct HTTP response value (re-addresses are not allowed). Multiple network perspectives (at least two) will be used to verify the random value in the HTTP/HTTPS connection. This method is NOT allowed to validate wildcard domain names.

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

Confirmation of the requester's control over an FQDN by validating control of the FQDN domain using the ACME HTTP Challenge method defined in section 8.3 of RFC 8555.

ACCV MUST receive a successful HTTP response from the request (which means that an HTTP 2xx status code should be received).
a 2xx HTTP status code must be received).

The token (as defined in RFC 8555, Section 8.3) once the value is communicated to the requester, will only be valid for 30 days. In the URL, the content of the file does not appear in any case and only 200 is considered as the correct HTTP response value (re-addresses are not allowed). Multiple network perspectives (at least two) will be used to verify the random value in the HTTP/HTTPS connection. This method is NOT allowed to validate wildcard domain names.

The data necessary to establish communication using ACME with ACCV can be obtained from the account associated with the agency in the NPSC application provided by ACCV.

In order to carry out the automatic generation and renewal of certificates, it is essential that all subscriber and organization documents are validated and valid. For this purpose, reminders are sent to registered users with ACME certificates indicating that the documents or credentials are about to expire. These reminders begin 30 days before expiration and are repeated daily.

(CAB/Forum BR 3.2.2.4.19 Agreed-Upon Change to Website - ACME)

Confirm the presence of a random value in a DNS CNAME, TXT or CAA record for 1) an Authoritative Domain Name; or 2) an Authoritative Domain Name that is prefixed with a tag beginning with an underscore character. Once the value is communicated to the applicant, it will only be valid for 30 days. Multiple network perspectives (at least two) will be used to perform the verification.

(CAB/Forum BR 3.2.2.4.7 DNS Change)

ACCV will check for the existence of CAA records just before issuing the certificate, acting as defined in RFC 8659 and in the CAB/Forum documents if the record is present. Multiple network perspectives (at least two) shall be used to perform the CAA record verification.

The identifier associated with ACCV as CAA *issue* and *issuewild* records is "accv.es".

Connection tests to 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 requesting application (NPSC) only allows the character to be placed in a valid position (never allowed in a first position to the left of a "registry-controlled" label or public suffix). The wildcard character (*) is not allowed in the electronic headquarters certificates.

In the event of any irregularity, the applicant for the certificate will be notified by ACCV and its issuance will be suspended until it is corrected. If such correction is not made within one month, the application will be denied.

3.2.3. Authentication of Individual Identity

ACCV uses the mechanisms established by the technical regulations in force, specifically Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on the establishment of minimum technical specifications and procedures for the security levels of electronic identification methods, as provided for in Article 8(3) of Regulation (EU) No. 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. See the relevant Policy.

Authentication of the identity of a certificate applicant shall be performed by using his or her personal qualified certificate supported for signing the application for the qualified website certificate.

The applicant must also submit the necessary documentation that determines the capacity to represent the entity that owns the domain to which it refers and the possession of the domain itself. This presentation will be made telematically using the means and applications that ACCV makes available to the users ( ).3.2.2

ACCV will check the data provided (including the applicant's country) using the information available at:

Official gazettes

https://boe.es/diario_boe/

https://dogv.gva.es/va/inici/

Data Protection Agencies

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

Public Administration Registries

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

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

https://www.pap.hacienda.gob.es/invente2/pagMenuPrincipalV2.aspx

Commercial registries

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

Patent and Trademark Offices

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

Identity Verification and Consultation Services

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

requesting from the applicant any corrections or additional documents it may consider necessary.

All agencies and records used are official and highly reliable, providing traceable evidence of all searches.

ACCV retains this information for audit purposes, allowing it to be reused for a period of no more than 13 months from its last verification.

3.2.4. Non-Verified Subscriber Information

All information provided is verified.

3.2.5. Validation of Authority

The authority of certificate applicants to request certificates on behalf of someone else is verified during the validation of the applicant's identity. As established by law, a specific power of attorney is required for this operation.

3.2.6. Criteria for interoperation

ACCV neither interoperates nor has cross-certificates with other Certification Authorities.

3.3. Identification and Authentication for Re-Key Requests

3.3.1. Identification and Authentication for Routine Re-Key

Identification and authentication for certificate renewal can be performed using the techniques for initial authentication and identification (described in sections 3.2.2 *Authentication of the identity of an organization* and 3.2.3 *Authentication of the identity of an individual,* of this CPS). ACCV can reuse information stored in previous verifications if no more than 13 months have passed since the last verification of the data, except for domain verification information, which is not reused, and the associated keys, which must be supplied again. There are, therefore, mechanisms for renewal:

- Web forms in the Non-Personal Certificate Management Area, available at https://npsc.accv.es:8450/npsc.
- Automation via ACME (with the corresponding documentation in force)

For further information see section 4.6 of this document.

3.3.2. Identification and Authentication for Re-Key after Revocation - Uncompromised key

The identification and authentication policy for the renewal of a certificate after an uncommitted revocation of the key will be the same as for the initial registration, being able to reuse the information in possession of ACCV if no more than 13 months have passed since the last verification of the data, except for the domain verification information, which is not reused, and the associated keys, which must be supplied again.

ACCV, for technical reasons and detailing all the steps, may use some electronic method that reliably and unequivocally guarantees the identity of the applicant and the authenticity of the application.

3.4. Identification and Authentication for Revocation Request

The identification policy for revocation requests may be the same as for initial registration. The authentication policy shall accept revocation requests digitally signed by the certificate subscriber.

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

- By means of a revocation form (located in the Non-Personal Certificate Management Area https://npsc.accv.es:8450/npsc) accessed by the certificate applicant or the person responsible for the certificate on the date of the revocation request by means of a qualified personal certificate.
- Using ACME's revocation mechanism

ACCV or any of its member entities may request ex officio the revocation of a certificate if they have knowledge or suspicion of the compromise of the subscriber's private key, or any other fact that would recommend such action.

For further information see section 4.9 of this document.

4. Certificate Life-Cycle Operational Requirements

4.1. Certificate Application

4.1.1. Who can submit a certificate request

This type of certificate request is the responsibility of private or public entities. A certificate request can be submitted by the subject of the certificate or by an authorized representative of the same, and that have proven to have control over the domain name to be included in the Certificate. In the case of electronic headquarters certificates, only public entities can apply for them.

4.1.2. Enrollment Process and Responsibilities

The process begins by accessing the Non-Personal Certificate Management Area (NPSC) located at https://npsc.accv.es:8450/npsc. The connection to the system is always encrypted and only client identification with qualified personal certificates is accepted.

If the website authentication certificate associated with an entity is requested for the first time, the user must attach the document that accredits him/her as qualified to make the request (document of taking office in the position or official journal where the corresponding appointment is recorded, powers of attorney and registration in the corresponding registries), in electronically signed pdf format. If the access has been made with a certificate that accredits the necessary capacity to manage the website authentication certificates, the Organization, Organizational Unit and Position data of that certificate will be used.

ACCV will check the application data and accredit the applicant for the application of website authentication certificates, for 13 months from the approval without the need to provide additional documentation, except for the domain verification information that is not reused. In the case of identification with a public employee certificate, there is no time limitation as long as the certificate is in force.

In addition to checking the credentials associated with the entity, ACCV will check in the authorized registries the possession of the domain or domains that appear in the certificate request, so that there is no doubt of such possession. ACCV will keep a record of these searches and verifications so that they can be reproduced in all the steps. For this verification ACCV will use the data provided in the registration process, being necessary a direct link between this data and the domains included in the application.

For domain verification and if the type of certificate allows it, the ACME services provided by ACCV can be used, automating the registration and generation process if the validation documentation of the organization is valid and in force. To register an ACME account it is necessary to register the user and the organization. From the registration you can obtain the necessary data for the application.

4.2. Certificate Application Processing

The identifier associated with ACCV as CAA issue and issuewild records is "accv.es".

4.2.1. Performing identification and authentication functions

The applicant identifies himself with a qualified personal certificate in the Non-Personal Certificate Management Area (NPSC) located at https://npsc.accv.es:8450/npsc, using the certificate data to perform the identification and authentication functions. In case of using ACME the request is completed in an automated way through the communication mechanisms described in the protocol since the identification is performed with the data provided when activating the ACME account.

Once the certificate application is received in electronic format through the platform by the authorized persons and once the economic proposal is accepted (if applicable), ACCV proceeds to review the application. In the case of using automation by ACME, the application will only be accepted if the required documentation is current and valid.

ACCV verifies the application data and accredits the applicant of the Web site authentication certificate application, for 13 months from the approval without the need to submit any additional documentation. In the case of identification with a public employee or representative certificate, there is no time limit as long as the certificate is valid.

In addition to checking the credentials associated with the entity, ACCV verifies in the authorized registries the possession of the domain or domains that appear in the certificate request, so that 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 that they can be reproduced at each step. For this check ACCV uses the data that was submitted in the registration process, being necessary a direct connection between this 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 the available mechanisms and lists.

4.2.2. Approval or Rejection of Certificate Applications

In case of acceptance, the Registration Authority will notify the applicant via a digitally signed email to the email address provided in the application. In the case of using ACME services the application is automatically approved if the domain requirements are met and the credentials of the agency and subscriber are current and valid.

In case of rejection, the Registration Authority will notify the applicant by means of a digitally signed e-mail to the e-mail address given in the application. The application is cancelled 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 member of ACCV different from the one responsible for performing the data verification. The differentiation of functions is performed using the capabilities established in the management application. In the case of ACME services all processes at this point are carried out in an automated manner.

ACCV will use this information to decide on new applications.

4.2.3. Time to Process Certificate Applications

The maximum time for processing certificate requests is five (5) business days. This time includes the processing time by ACCV and does not include the time used by the user to provide the necessary information and documentation.

4.3. Certificate Issuance

ACCV is not responsible for monitoring, investigating or confirming the accuracy of the information contained in the certificate subsequent to its issuance. In the event of receiving information about the inaccuracy or current non-applicability of the information contained in the certificate, the certificate may be revoked.

4.3.1. CA Actions during Certificate Issuance

The issuance of the certificate takes place once the Registration Authority has performed the necessary checks to validate the application. The mechanism that determines the nature and manner of these checks is this CPS.

When the applicant receives the approval email, they must log back into NPSC, identifying themselves with a qualified personal certificate to generate and download the certificate. This does not apply if ACME is used, where the application, verification of documentation and domain possession, and generation is done in a single step.

The organization responsible for the authentication certificate of the websites may request ACCV to add other users with the ability to perform the transactions that are associated with the lifecycle of the certificates. The Registration Authority will check the credential request and notify the applicant of the authorization or denial of permission, via a signed email.

ACCV may perform this authorization ex officio in the event that the person in charge of the organization loses its management capacity and there is no other authorized person.

When ACCV CA issues a certificate in accordance with a valid certification request, it will send one copy of the certificate to the Registration Authority that issued the request and another to ACCV repository.

ACCV checks that the certificates conform to the accepted profiles using different validators that are run before the CA signs the applications (they are signed by a generic non-recognized key). Specifically, the following are used:

- zlint

- pkilint

If any of these validators return an error, the issuance is stopped and the applicant and the CA operators are notified.

ACCV will perform frequent reviews of samples of website authentication certificates to ensure the accuracy of the data and the format of the certificates by the validators used in the issuance. If in the course of these samplings a change of data is confirmed that may imply the loss of domain ownership, ACCV will revoke the certificates involved. In case of inaccuracy of the data contained in the certificate or its inapplicability, the same process will be followed. ACCV will leave a documentary record of all these reviews and actions.

In the case of certificates issued by a root CA, a person authorized by ACCV is required to intervene manually in order for the root CA to perform a certificate signing operation.

4.3.2. Notification to Subscriber by the CA of Issuance of Certificate

ACCV notifies the subscriber of the issuance of the certificate, through an e-mail to the e-mail address provided in the application process.

4.3.3. Refusal to Issue a Certificate

ACCV reserves its right to refuse to issue a Certificate to any party as it sees fit, without incurring any liability or responsibility for any loss or expenses arising out of such refusal.

ACCV reserves the right not to disclose reasons for such a refusal.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

The acceptance of the certificates by the signatories occurs at the time of signing the certification contract associated with each Certification Policy. The acceptance of the contract implies knowledge and acceptance by the subscriber of the associated Certification Policy.

The user must accept the contract before the certificate is issued.

4.4.2. Publication of the Certificate by the CA

Once the certificate has been accepted by the subscriber and generated, the certificate will be published in ACCV repository and made available to authorized users.

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

Prior to the issuance of Website Authentication Certificates, a pre-certificate is sent to the Certificate Transparency Service Logs (CT LOG) following the requirements established in the application policies. The number of operators to which the pre-certificate is sent and the format of the extensions is indicated at .7.1.10

There are no further notifications.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Usage

ACCV does not generate or store the Private Keys associated with website authentication Certificates (although it provides tools to facilitate this). The custody and control of the private keys corresponds to the subscriber or its Representatives who have accredited to have control over the domain name to be included in the Certificate.

The intended scope of use for a private key shall be specified through certificate extensions, including key usage and extended key usage extensions, in the associated certificate.

Certificates can be used to identify the server to whose domain the certificate is issued in a secure manner, and to establish secure communication channels (including encryption) using the mechanisms available in each case.

In the case of electronic headquarters certificates, they are used to identify an electronic headquarter of a public body.

4.5.2. Relying Party Public Key and Certificate Usage

The relying parties undertake to:

- The uses of the certificates correspond to the scope of application.

- The provisions of the CPS are complied with

- Check the status of the certificate and verify the status of the hierarchical chain before establishing trust.

- Not to compromise or use the services offered in a malicious manner.

- Report any anomalies or problems detected using the appropriate channels.

4.6. Certificate Renewal

The renewal of certificates must be carried out using the same procedures and identification methods as those established for the initial application.

ACCV does not renew Certificates maintaining the public Key of the same, but, in any case, the renewal of Certificates is always done by providing Keys.

4.6.1. Circumstances for certificate renewal

The certificate renewal period begins 30 days before the expiration date of the certificate, when the subscriber receives an email notifying him/her of the steps to follow to proceed with the certificate renewal. In the case of using ACME the renewal process can be initiated automatically if this option has been configured and the documents required for the validation of the organization are current and valid.

4.6.2. Who May Request Renewal

Any subscriber may request the renewal of its certificate. To do so, the same requirements must be met as for the initial application. ACCV does not automatically renew Certificates.

4.6.3. Processing Certificate Renewal Requests

The same process will be followed as described for the initial issuance.

4.6.4. Notification of New Certificate Issuance to Subscriber

It is the responsibility of the Registration Authority to notify the subscriber of the issuance of the certificate and to deliver a copy to the subscriber or, failing that, to inform the subscriber how to obtain a copy.

The same process will be followed as described for the initial issuance.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

The same process will be followed as described for the initial issuance.

4.6.6. Publication of the renewal certificate by the Certification Authority

The same process will be followed as described for the initial issuance.

4.6.7. Notification of Certificate Issuance by the CA to Other Entities

The same process will be followed as described for the initial issuance.

4.7. Certificate Re-key

Key renewal necessarily implies certificate renewal and cannot be carried out as separate processes.

4.7.1. Circumstances for Certificate Re-Key

Key renewal necessarily implies certificate renewal and cannot be carried out as separate processes.

4.7.2. Who May Request certification of a new public key

Key renewal necessarily implies certificate renewal and cannot be carried out as separate processes.

ACCV can regenerate the keys of the certificates of the CAs, according to the document of the corresponding generation ceremony. ACCV can regenerate the keys of OCSP and TSA services certificates in accordance with the corresponding internal procedure.

4.7.3. Processing Certificate Rekeying Requests

Key renewal necessarily implies certificate renewal and cannot be carried out as separate processes.

4.7.4. Notification of new certificate issuance to Subscriber

Key renewal necessarily implies certificate renewal and cannot be carried out as separate processes.

4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate

Key renewal necessarily implies certificate renewal and cannot be carried out as separate processes.

4.7.6. Publication of the Re-Keyed Certificate by the CA

Key renewal necessarily implies certificate renewal and cannot be carried out as separate processes.

4.7.7. Notification of Certificate Issuance by the CA to Other Entities

Key renewal necessarily implies certificate renewal and cannot be carried out as separate processes.

4.8. Certificate Modification

Modification of certificate fields is not allowed. When it is necessary to modify any information in the certificate, ACCV will revoke the certificate and issue a new one following the established processes.

4.8.1. Circumstance for Certificate Modification

Modification of certificate fields is not allowed. When it is necessary to modify any information in the certificate, ACCV will revoke the certificate and issue a new one following the established processes.

4.8.2. Who May Request Certificate Modification

Modification of certificate fields is not allowed. When it is necessary to modify any information in the certificate, ACCV will revoke the certificate and issue a new one following the established processes.

4.8.3. Processing Certificate Modification Requests

Modification of certificate fields is not allowed. When it is necessary to modify any information in the certificate, ACCV will revoke the certificate and issue a new one following the established processes.

4.8.4. Notification of New Certificate Issuance to Subscriber

Modification of certificate fields is not allowed. When it is necessary to modify any information in the certificate, ACCV will revoke the certificate and issue a new one following the established processes.

4.8.5. Conduct Constituting Acceptance of Modified Certificate

Modification of certificate fields is not allowed. When it is necessary to modify any information in the certificate, ACCV will revoke the certificate and issue a new one following the established processes.

4.8.6. Publication of the Modified Certificate by the CA

Modification of certificate fields is not allowed. When it is necessary to modify any information in the certificate, ACCV will revoke the certificate and issue a new one following the established processes.

4.8.7. Notification of Certificate Issuance by the CA to Other Entities

Modification of certificate fields is not allowed. When it is necessary to modify any information in the certificate, ACCV will revoke the certificate and issue a new one following the established processes.

4.9. Certificate Revocation and Suspension

ACCV specifies the revocation reasons for the certificates that have been revoked. For subscriber's certificates only if the subscriber has provided the revocation reason, otherwise this will be unspecified.

4.9.1. Circumstances for revocation

4.9.1.1. Reasons to revoke a user certificate

A certificate is revoked in a period not exceeding 24 hours when:

- A valid revocation request is received from the subscriber.
- A valid request for revocation is received from an authorized third party, for example by means of a court order.
- The certificate subscriber or its keys or the keys of its certificates have been compromised by:
  - The theft, loss, disclosure, modification, or other compromise or suspected compromise of the user's private key.
  - Deliberate misuse of keys and certificates, or failure to observe the operational requirements of the Subscriber Agreement, or this CPS.
- The key pair generated by the subscriber is revealed as "weak".
- The certificate of a higher RA or CA in the certificate trust hierarchy is revoked.
- ACCV is aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed.

A certificate must be revoked in a period not exceeding five days, being advisable to revoke in a period not exceeding 24 hours when:

- A prerequisite necessary for the issuance of the certificate has not been met.
- A fundamental factor of the certificate is known to be false or reasonably believed to be false.
- An error occurred while entering or processing the data.
- The information contained in a certificate becomes inaccurate, for example, when the owner of a certificate changes its name.
- ACCV is aware of any circumstances indicating that the use of a domain name in the certificate is no longer legally permitted (for example, if a court or similar body has revoked the domain name owner's right to use the domain name, if a relevant license or service agreement between the domain name owner and the certificate applicant has been terminated, or if the domain name owner has not renewed the certificate).
- ACCV is aware that a Wildcard Certificate has been used to fraudulently authenticate a subordinate domain name.
- The Certificate has not been issued in accordance with the policies set out in this document

4.9.1.2. Reasons to revoke a subordinate (intermediate) CA certificate

An intermediate (subordinate) CA certificate is revoked when:

- ACCV obtains evidence that the private key of the subordinate CA corresponding to the certificate's public key has been compromised.
- ACCV obtains evidence of misuse.
- ACCV has knowledge that the certificate has not been issued in accordance with this CPS, the Certification Policy or the applicable Certification Practices Statement, or that the subordinate CA has not complied with them.
- ACCV determines that any information appearing on the Certificate is inaccurate or misleading.
- ACCV ceases to operate for any reason and has not arranged for another CA to provide revocation support for the Certificate.
- ACCV's right to issue certificates under these requirements expires, is revoked or lapses, unless the issuing CA has taken steps to continue to maintain the CRL/OCSP repository.
- Revocation is required by ACCV Certificate Policy and/or the Certification Practices Statement.
- The technical content or format of the certificate presents an unacceptable risk to application software vendors or relying parties.

The revocation must be made within a period not exceeding 7 days from the time ACCV becomes aware of the fulfillment of these conditions.

4.9.2. Who Can Request Revocation

The revocation of a certificate can be requested both by the subscriber of the certificate and by ACCV, as well as by any person who has reliable knowledge that the data associated with the certificate has become inaccurate or incorrect or that any of the circumstances established for revocation have been incurred.

Certificate subscribers may request revocation for any reason and must request revocation under the conditions specified in the following section.

4.9.3. Procedure for Revocation Request

ACCV accepts requests for revocation of Web site authentication certificates by the following procedures

4.9.3.1. Interactive telematics

By accessing the Non-Personal Certificate Management Area (NPSC) located at https://npsc.accv.es:8450/npsc the user can revoke the certificates he/she has requested or for which he/she has permission to do so.

It can also be revoked through the contact form at https://www.accv.es/# where the user must paste the private key in PEM format, including the BEGIN and END lines.

4.9.3.2. Telematic ACME

Using the automation service through ACME, from the account for which the certificate was issued.

https://npsc.accv.es:8450/npsc/acme/revoke-cert

4.9.3.3. Telephone

Using the 24x7 contact telephone number 963 866 014.

Subscribers, relying parties, application software vendors and other third parties may report suspected private key compromise, certificate misuse or other types of fraud, compromise, misuse, misconduct or any other certificate-related issues at the URL https://www.accv.es/contacto/. The support email and contact telephone numbers are located at this URL.

4.9.4. Revocation Request Grace Period

In the event that a Grace Period is not defined in the Subscriber Agreement, Subscribers are required to request revocation within 24 hours of detecting any problem that invalidates the use of the certificate (loss or compromise of the Private Key, etc.).

4.9.5. Time Within which CA Must Process the Revocation Request

ACCV will handle revocation requests in accordance with sections 4.9.1.1 and 4.9.5 of the BR/TLS, always ensuring that within 24 hours of receipt of a CPR a preliminary study and initial report has been carried out. ACCV will inform the subscriber and the entity has reported the problem.

4.9.6. Revocation Checking Requirement for Relying Parties

Third parties that trust and accept the use of Certificates issued by ACCV are obliged to verify the status of the certificates (revocation and expiration) throughout the certification chain and at each use of the same against the relevant CRL published or using the OCSP server.
ACCV makes available to its users several revocation checking services for the certificates it issues (CRL, OCSP, others...). Relying parties must use at least OCSP (preferably) or CRL.

4.9.7. CRL Issuance Frequency

ACCV will publish a new end-entity CRL in its repository at maximum intervals of 5 hours, even if no CRL modifications (certificate status changes) have occurred during the mentioned period. The nextUpdate field has a maximum value of 4 days.

ACCV shall publish a new root CRL in its repository with a maximum periodicity of 6 months, even if there have been no changes in the CRL. In case of revocation of an intermediate certification authority, the CRL shall be published within no more than 12 hours.

The OCSP is updated prior to the CRL. The most recent information will be the one provided by the OCSP.

The CRL does not contain expired certificates. To inquire about the status of an expired certificate the valid information will be the one provided by the OCSP.

4.9.8. Maximum Latency for CRLs

The maximum time between the generation of the CRLs and their publication in the repository is 30 minutes.

4.9.9. On-Line Revocation/Status Checking Availability

ACCV provides an OCSP server for online certificate status verification at: ocsp.accv.es:80 according to RFC 6960 and RFC 5019.

OCSP responses are signed by an OCSP server whose certificate is signed by the CA that issued the certificate we are checking, and which has the specific key usages for it.

ACCV maintains the certificate status information indefinitely, guaranteeing this information for at least 15 years.

4.9.10. On-Line Revocation Checking Requirements

The OCSP server is freely accessible and there are no requirements for its use, except for those derived from the use of the OCSP protocol according to the provisions of RFC 6960.

OCSP supports calls to the service using the GET method (in addition to the POST method).

For the status of subscriber certificates:

- ACCV updates the information provided through OCSP within 3 hours.

- OCSP responses for this service have a maximum expiration time of 3 days.

- An authorized OCSP response (i.e., the OCSP service MUST NOT respond with "unknown" status) must be available within 15 minutes of the certificate first being published or made available.

For the status of subordinate CA certificates:

- ACCV updates the information provided via OCSP within 6 months and within 12 hours of revocation of an intermediate CA certificate.

ACCV OCSP service provides definitive responses on "reserved" certificate serial numbers, as if there is a corresponding certificate that matches the pre-certificate, as indicated in RFC 6962. A certificate serial number within an OCSP request is in one of the following three options:

- 1 . "assigned" if the issuing CA has issued a certificate with that serial number.
- 2 "reserved" if a Precertificate [RFC6962] with that serial number has been issued by the issuing CA.
- 3 "not used" if none of the above conditions are met.

If the OCSP server receives a status request for a certificate that has not been issued ("not used"), then it responds with a "revoked" status, with reason certificateHold(6) and revocationTime January 1, 1970. ACCV monitors the response to such requests as part of its security response procedures.

ACCV also provides web services to consult the validity status of issued certificates.

4.9.11. Other Forms of Revocation Advertisements Available

Not defined

4.9.12. Special Requirements for Key Compromise

There will be no variation in the above clauses in the event that the revocation is due to the compromise of the private key.

The user can provide the compromised private key using the support form at the following URL: https://www.accv.es/ayuda/certificates-revocation/how-revoke-certificate/.

In the form you must paste this key in PEM format, including the BEGIN and END lines.

4.9.13. Circumstances for suspension

Suspension renders the certificate invalid for the entire time it is suspended.

ACCV does not allow the suspension of certificates.

4.9.14. Who can Request Suspension

ACCV does not allow the suspension of certificates.

4.9.15. Procedure for Suspension Request

ACCV does not allow the suspension of certificates.

4.9.16. Limits on Suspension Period

ACCV does not allow the suspension of certificates.

4.10. Certificate Status Services

The information related to the verification of the revocation status of the electronic Certificates issued by ACCV can be consulted through CRLs and/or the Certificate Status Information and Consultation Service through the OCSP protocol, and are accessible through the following means indicated in our web page:

https://www.accv.es/servicios/validacion/

CRL:

CRL ACCVRAIZ1 https://www.accv.es/fileadmin/Archivos/certificados/raizaccv1_der.crl

CRL ACCVCA110 https://www.accv.es/fileadmin/Archivos/certificados/accvca110_der.crl

CRL ACCVCA120 https://www.accv.es/fileadmin/Archivos/certificados/accvca120_der.crl

CRL ACCVCA130 https://www.accv.es/fileadmin/Archivos/certificados/accvca130_der.crl

CRL ACCV ROOT RSA TLS 2024 http://www.accv.es/gestcert/accv_root_rsa_tls_2024.crl

CRL ACCV RSA1 TLS http://www.accv.es/gestcert/accv_rsa1_tls.crl

CRL ACCV ROOT ECC TLS 2024 http://www.accv.es/gestcert/accv_root_ecc_tls_2024.crl

CRL ACCV ECC1 TLS http://www.accv.es/gestcert/accv_ecc1_tls.crl

OCSP (all hierarchy): http://ocsp.accv.es

4.10.1. Operational characteristics

Revoked certificates remain in the CRL until they reach their expiration date.

Once this is reached, they are removed from the list of revoked certificates.

OCSP sets a limit of 180 months, which allows checking the status of the certificate beyond the expiration date.

The Certificate Status Information and Query Service via OCSP protocol supports the GET method to retrieve the validation information of issued certificates, in accordance with the requirements of RFC6960 and those established by the CA/Browser Forum entity (which can be consulted at https://cabforum.org/baseline-requirements-documents/). OCSP responses have a validity interval of 3 days and the information is constantly updated by directly accessing the database. The OCSP server will not respond "good" to a query about the status of a certificate that has not been issued.

4.10.2. Service availability

CRL systems and Online Certificate Status Query Systems (OCSP) will be available 24 hours a day, 7 days a week.

The OCSP response time should be kept below 1s and the CRL download time should be kept below 10s.

4.10.3. Optional features

There are no access or query restrictions for OCSP and CRL.

4.11. End of subscription.

The subscription ends with:

ACCV cease of operation

the expiration or revocation of the certificate without a renewal.

ACCV will inform the person responsible for the website authentication certificate, by e-mail, at a time prior to the publication of the certificate in the List of Revoked Certificates, about the suspension or revocation of the certificates in which he/she appears as subscriber or responsible, specifying the reasons, date and time when his/her certificate will become invalid, and informing him/her that he/she should not continue to use it.

4.12. Key Escrow and Recovery

4.12.1. Key Escrow and Recovery Policy and Practices

ACCV does not deposit keys of any kind associated with this type of certificate.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

Session key recovery is not supported.

4.13. Expiration of CA certificate keys.

ACCV will avoid generating website authentication certificates that expire later than the CA certificates. For this purpose, website authentication certificates whose validity period exceeds that of the CA certificate in question will not be issued and will be generated with the new CA certificate, in order to avoid notifying subscribers to renew their certificate, in the event that the CA certificate expires earlier.

5. Facility, Management, and Operational Controls

5.1. Physical Security Controls

5.1.1. Site Location and Construction

The information systems of ACCV are located in Data Processing Centers (DPC) with appropriate levels of protection, external walls of the sites are of solid construction, and surveillance 24 hours a day, 7 days a week. Physical barriers are used to segregate secure areas within DPCs and are constructed so as to extend from real floor to real ceiling to prevent unauthorized entry.

5.1.2. Physical access

ACCV Data Processing Centers have different security perimeters, with different security requirements and authorizations. The equipment that protects the security perimeters includes combination-based physical access control systems, video surveillance and recording, and intrusion detection systems, among other equipment.

In order to access the most protected areas, duality of access and an extensive period of time working for the company is required.

5.1.3. Power and air conditioning

The installations are equipped with uninterruptible power supply systems with sufficient power to autonomously power the electrical network during controlled system power cuts and to protect equipment from electrical fluctuations that could damage it.

The equipment shall only be switched off in the event of failure of the autonomous power generation systems.

The air conditioning system consists of various independent pieces of equipment with the capacity to maintain temperature and humidity levels within the systems' optimum margins of operation.

5.1.4. Water Exposure

ACCV Data Processing Centers are equipped with flood detectors and alarm systems appropriate to the environment.

5.1.5. Fire Protection and Prevention

ACCV' Data Processing Centers have automated systems for fire detection and extinguishing.

5.1.6. Media Storage

Sensitive data media is stored securely in fireproof cabinets and safes in accordance with the type of medium and the classification of the information contained in them.

These cabinets are located in different buildings to remove risks associated with a single location.

Access to these media is restricted to authorized personnel.

5.1.7. Waste Disposal

The disposal of magnetic and optical media and information on paper is carried out securely following procedures stipulated for this purpose, using processes of demagnetization, sterilization, destruction or shredding, depending on the type of medium to be processed.

5.1.8. Off-Site Backup

Encrypted remote backup copies are made on a daily basis and are stored in premises located close to the back-up Data Processing Center, where ACCV operations would continue in the event of a serious incident or collapse of the main Data Processing Center.

5.2. Procedural controls

ACCV information systems and services are operated securely, following pre-established procedures.

For security reasons, information regarding procedural controls is considered confidential and is only explained in summary form.

5.2.1. Reliable papers

The roles identified for the control and management of the services are:

a. Management
b. Systems Administrator
c. Point of User Registration (PRU) Manager
d. Security Administrator
e. Certification Authority Operator
f. PRU Operator
g. Responsible for training, support and communication
h. Security Manager
i. Auditor
j. Jurist
k. Documentation Manager
l. Application Development Assistance and Deployment Support
m. Certification Authority Coordinator

5.2.1.1. Management

At the head of ACCV's staff and under the control of ISTEC's Board of Directors, he is the person responsible for the economic and financial management and the technical and administrative control of ACCV's activities.

Corresponds to the position of Manager of Infraestructures i Serveis de Telecomunicacions i Certificació, SAU (ISTEC).

5.2.1.2. Systems Administrator

He/she is responsible for operating systems and software products installation and configuration, and maintaining and updating the installed products and programs.

He/she is entrusted with the establishment and documentation of systems and provided services monitoring procedures, as well as tasks carried out by the Certification Authority Operators monitoring.

He/she must ensure that services are provided with the appropriate level of quality and reliability, in accordance with the critical level of these services.

He/she is responsible for the correct implementation of the Backup Policy, and in particular, for maintaining sufficient information which permits the effective restoration of any system. Along with the Certification Authority Operator and, in exceptional cases, the PRU Administrator, is responsible for making the local backup copies.

He/she must maintain the inventory of servers and equipment comprising ACCV certification platform group.

He/she must not have access to aspects relating to system or network security (registrations/removals of users, management of firewall rules, management and maintenance of intrusion detection systems, etc.).

He/she must collaborate with the Auditors in relation to everything that is required of him/her.

5.2.1.3. PRU Administrator.

This profile is similar to Systems Administrator but dedicated to the tasks related to installation, maintenance and control of the systems that comprising the User Registration Points.

He/she is responsible for administrative tasks relating to PRU Operators' authorizations, confidentiality agreements, etc.

He/she must maintain the inventory of PRUs and equipment used for PRU operations.

In exceptional cases, he/she may work with the Systems Administrator and Certification Authority Operator to carry out local backups of the PKI systems.

In the same way as for Systems Administrators, he/she must not have access to aspects relating to the security of systems, or of the network, etc. (registrations/removals of users, management of firewall rules, management and maintenance of intrusion detection systems, etc.).

He/she must collaborate with the Auditors in relation to everything that is required of him/her.

5.2.1.4. Security Administrator.

He/she must comply with and ensure compliance with ACCV's security policies, and must be responsible for any matter relating to the security of ACCV: physical security, security of applications, of the network, etc.

He/she is the individual responsible for managing the perimeter protection systems and specifically managing firewall rules, according to the security rules and in compliance with the Security Responsible.

He/she is responsible for installation, configuration and management of the intrusion detection systems (IDS) and the tools associated with these.

He/she is responsible for resolving or ensuring the resolution of security incidents that have occurred, eliminating vulnerabilities detected, etc. recording always all the incidences that have occurred and all his/her actions.

He/she is responsible for maintaining updated the documents concerned with security devices and, generally, all its tasks.

He/she will notify the Security Responsible of the incoherence between the Security Policy, the Certification Practices Statement, etc. and the real practices.

He/she will control that companies which provide collocation services operate and maintain correctly the physical security systems of DPCs.

In a coordinated manner with the Security Responsible, he/she must take charge of explaining all security mechanisms to the personnel that should know it, raising awareness among ACCV staff and enforcing standards and security policies.

He/she must collaborate with the Auditors in relation to everything that is required of him/her.

5.2.1.5. Certification Authority Operator

He/she assists the Systems Administrators and PRU Administrators in technical or administrative matters that do not require access to the DPC.

He/she must assist the Training, Support and Communications Manager in any tasks instructed.

He/she must collaborate in accordance with the requests of PRU Administrators, with regard to inventory roles, assistance in the installation of systems comprising the PRUs, documentation preparation, collaboration in the training and support of PRU Operators, etc.

He/she works with the Documentation Manager to monitor existing documents, to monitor the documentation file (hard copy) and to revise certificates and contracts.

He/she works with the Security Manager on administrative tasks, inventory tasks and, in general, technical or administrative tasks.

Along with the Systems Administrator and, in exceptional cases, the PRU Administrator, he/she is responsible for making the local backup copies. This is the only task that the Certification Authority Operator carries out within the DPC.

He/she must collaborate with the Auditors in relation to everything that is required of him/her.

5.2.1.6. User Registration Point Operator

He/she is responsible for functions relating to the identification of certificate applicants, the processing of digital certificates, the revocation of digital certificates and the unblocking of cryptography cards, all while exclusively using the tools and applications provided by the PRU Administrators, and strictly following the approved procedures.

He/she must collaborate with the Auditors in relation to everything that is required of him/her.

5.2.1.7. Training, Support and Communications Manager

He/she is responsible for the maintenance of content of the website of the Agencia de Tecnología y Certificación Electrónica (www.accv.es).

He/she is entrusted with communication and updating duties in relation to ACCV's website.

He/she is responsible for defining the training plan for end users, Call Center agents and personnel involved directly in the operation and administration of ACCV's certification platform. In addition, he/she works with the PRU Administrator in preparing training for PRU Operators.

The Training, Support and Communications Manager is responsible for preparation of the contents of the courses taught on the e-learning corporate platform.

He/she must revise the Call Centre incident and response files on a monthly basis, and revise the Call Center agents' scripts.

He/she must coordinate the actions of microcomputing personnel and provide the tools and necessary material for them to carry out their duties correctly.

The Training, Support and Communications Manager may receive the collaboration of the Certification Authority Operators for those tasks that he/she deems appropriate.

5.2.1.8. Security Manager

He/she must comply with and ensure compliance with ACCV's security policies, and must be responsible for any matter relating to the security of ACCV: physical security, security of applications, of the network, etc.

He/she is the individual responsible for managing the perimeter protection systems and specifically managing firewall rules.

He/she is responsible for installation, configuration and management of the intrusion detection systems (IDS) and the tools associated with these.

He/she is responsible for resolving or ensuring the resolution of security incidents that have occurred, eliminating vulnerabilities detected, etc.

He/she is responsible for management and control of the DPC physical security systems, the access control systems, the air conditioning and power supply systems.

He/she is responsible for explaining the security systems to personnel that must know about them, ensuring the awareness of all ACCV personnel and ensuring compliance with security regulations and policies.

He/she must establish schedules for carrying out the analysis of vulnerabilities, trials and tests of service continuity plans and information systems audits.

He/she must collaborate with the Auditors in relation to everything that is required of him/her.

5.2.1.9. Auditor

The auditor profile corresponds to an internal position, without prejudice to the personnel responsible for external audits.

The Auditor is responsible for:

- Verifying the existence of all the required and listed documentation
- Verifying the consistency of the documentation with procedures, inventoried assets, etc.
- Verifying the monitoring of incidents and events
- Verifying the protection of systems (exploitation of vulnerabilities, access logs, users, etc.).
- Verifying alarms and physical security elements
- Verifying compliance with regulations and legislation
- Verifying knowledge of procedures among the personnel involved

In short, the auditor must verify all aspects mentioned in the security policy, copies policies, certification practices, Certification Policies, etc. in the group of ACCV systems and within ACCV personnel, as well as in the PRUs.

5.2.1.10. Legal Expert

He/she is responsible for the legal aspects of the provision of certification services and the formalization of the provision of these services to other entities, with which a certification agreement has to be set up.

He/she is entrusted with processing the approval and publication of Certification Policies, modifications to the Certification Practice Statement document and, in general, to any government regulations which affect the Certification Authority's certification platform and services.

He/she ensures compliance with the electronic signature legislation currently in force, analyzing the existing Certification Policies and Certification Practice Statement and those which are subject to approval, and notifying the inconsistencies or problems that he/she detects.

He/she must collaborate with the Auditors in relation to everything that is required of him/her.

5.2.1.11. Documentation Manager

He/she is responsible for maintaining ACCV's electronic documentation repository and hard-copy documentation files.

He/she checks that documents are updated when required and by the persons that the Documentation Manager appoints, and may even exceed specified requirements for documents to be updated or maintained.

He/she is responsible for keeping the document index file up to date and is the only individual authorized to store, delete or modify documents in ACCV's documentation repository.

He/she may receive the collaboration of the Certification Authority Operators in carrying out documentary control or inventory tasks.

He/she must guarantee that any certificate issued is associated with a certification contract drawn up in hard copy.

He/she must collaborate with the Auditors in relation to everything that is required of him/her.

5.2.1.12. Deployment Support Manager

He/she is responsible for maintaining contact with development teams of IT applications of user organizations and entities of ACCV's services, in order to provide the necessary support and assistance for the development and deployment of data transmission applications and services which use digital certification and electronic signatures.

He/she is responsible for redirecting technical IT or legal queries that he/she cannot resolve to the appropriate personnel.

He/she must gather sufficient information (projects information template) in order to be able to provide an optimum level of assistance and advice.

He/she must provide guidance on development possibilities, techniques and tools, taking into account the corporate information systems, security policy, applicable legislation, etc.

The Deployment Support Manager must provide guidance on existing technical and administrative regulations, the role of creation of PRUs by organizations and entities that offer electronic transmission services, the operating method of these, etc. Must collaborate with ministries or entities with which a certification agreement has been set up, in order to analyze methods of distribution of certificates, creation of PRUs, etc.

He/she must collaborate with the Auditors in relation to everything that is required of him/her.

5.2.1.13. Certification Authority Coordinator

He/she is responsible for monitoring and controlling the performance of the roles attributed to each job profile described above, and for the distribution of new tasks among the profiles.

He/she is responsible for constituting a means of communication between the personnel appointed to each of the profiles and the Certification Authority management body. In the same way, he/she is responsible for serving as a link with other departments of the Autonomous Government of Valencia.

He/she is responsible for presenting strategic decisions to the Certification Authority management body and for approving tactical decisions.

He/she advises ACCV personnel on training to be taken, retraining courses, etc. and facilitates the implementation of these courses and training plans.

He/she must collaborate with the Auditors in relation to everything that is required of him/her.

5.2.2. Number of persons required per task

Two persons are required for key activation of cryptographic hardware key generation and storage devices. Modification of cryptographic hardware configuration parameters requires authentication by at least two authorized persons with sufficient privileges.

5.2.3. Identification and authentication for each role

All authorized ACCV users are identified by digital certificates issued by ACCV itself and are authenticated by cryptographic smart-cards and/or biometric devices.

Authentication is complemented with the corresponding authorizations to access certain information assets or ACCV systems.

5.2.4. Roles requiring segregation of duties

No identity is authorized to assume both a System Administrator and a Security Manager role;

No identity is authorized to assume both a System Administrator and an Auditor role;

No identity is authorized to assume both a Security Manager and an Auditor role;

5.3. Personnel security controls

This section reflects the contents of ACCV *Personnel Security Controls* document.

5.3.1. Qualifications, Experience, and Clearance Requirements

ACCV requires all personnel who carry out duties in its installations to have sufficient qualifications and experience in environments relating to the provision of certification services.

All personnel must comply with the organization's security requirements and must possess:

- Knowledge and training in digital certification environments.
- Basic training in information systems security.
- Specific training for their post.
- Academic qualification or experience in the equivalent industry

Before new personnel begin performing any task or work for ACCV, their identity and trust issues will be verified with official records.

5.3.2. Background check procedures

By checking the Curriculum Vitae of the personnel.

5.3.3. Training requirements

The personnel of ACCV are subject to a specific training plan for carrying out their role within the organization:

This training plan includes the following aspects:

1. Training in the basic legal aspects relating to the provision of certification services.
2. Training in information systems security.
3. Services provided by ACCV.
4. Basic concepts of PKI.
5. Certification Practice Statement and the relevant Certification Policies.
6. Incident management

ACCV maintains records of such training and ensure that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily.

ACCV documents that each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task.

ACCV requires all Validation Specialists to pass an examination provided by the CA on the information verification requirements outlined in the “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates”.

5.3.4. Retraining Frequency and Requirements

Prior to technological changes in the environment, the introduction of new tools or the modification of operating procedures, the appropriate training will be carried out for the personnel affected.

Training sessions will be carried out prior to changes in the Certification Practice Statement, Certification Policies or other relevant documents.

5.3.5. Job Rotation Frequency and Sequence

No rotation plan has been defined for the personnel Agencia de Tecnología y Certificación Electrónica in the assignment of its tasks.

5.3.6. Sanctions for Unauthorized Actions

In the event that an unauthorized action is carried out regarding to the operations of the Certification Authority, disciplinary measures shall be taken. Actions which contravene the Certification Practice

Statement or the relevant Certification Policies in a negligent or malicious way shall be considered to be unauthorized actions.

If any infringement occurs, the Certification Authority shall suspend the access of the persons involved to all the Certification Authority information systems, as soon as it becomes aware of the infringement.

In addition, and according to the seriousness of the infringements, the sanctions provided for in the Civil Service Act, the company collective agreement, or the Workers' Statute shall be applied in accordance with the employment situation of the infringing party.

5.3.7. Independent Contractor Requirements

The external personnel that is involved in the issuance of certificates receives the necessary technical and legal training to carry out their tasks with due diligence (at least the detailed training on section 5.3.3).

All personnel are subject to a secrecy obligation by virtue of signing the confidentiality agreement begin working for ACCV. In this agreement, they also undertake to carry out their duties in accordance with this Certification Practice Statement, ACCV Information Security Policy and the approved procedures of ACCV.

5.3.8. Documentation Supplied to Personnel

Personnel joining the Certification Authority are provided with access to the following documentation:

- Certification Practice Statement
- Certification Policies
- Privacy policy
- Information Security Policy
- Organization chart and roles of personnel

Access is provided to documentation relating to regulations and security plans, emergency procedures and all technical documentation necessary for personnel to carry out their roles.

5.3.9. Periodic compliance checks

The check that personnel possess the necessary knowledge is carried out at the end of the training sessions and on a discretionary basis, by the training staff responsible for teaching these courses and, as a last resort, by the Training, Support and Communications Manager.

The verification of the existence of the documentation that employees must be familiar with and sign is carried out annually by the Documentation Manager.

The Security Manager carries out an annual review of the compliance of the authorizations granted with the actual privileges given to employees.

5.3.10. Termination of contracts

In the event of termination of the employment relationship of personnel performing their duties at ACCV, the Security Manager shall proceed to carry out the actions or checks detailed in the following points, either directly or by instructing the appropriate personnel to do so.

5.3.10.1. Access to organizational locations

The individual's access privileges to the organization's facilities to which access is restricted shall be removed. This involves, at a minimum, the removal of access authorization to the following locations

- ○ Suppression of privilege access to the main CPS
- ○ Suppression of privilege access to the secondary CPS

- Suppression of privileged access to computer rooms and facilities and dependencies of Polígono Ademuz S/N in Burjassot (Valencia).

5.3.10.2. Access to Information Systems

The individual's access privileges to the organization's Information Systems should be removed, with special attention to administration privileges and remote access privileges.

- User deletion on servers
- User deletion in ACCV Document Repository (RD-ACCV)
- User deletion in Incident Control System
- Change known passwords
  - Root / Server Administrator
  - FW
  - Network electronics (switches, balancers, routers,...)
  - IDS

5.3.10.3. Access to documentation

Suppression of access to all information, with the exception of information considered PUBLIC.

Removal of access to the Secure Developer Zone on ACCV website.

5.3.10.4. Information to the rest of the organization

The rest of the organization should be clearly informed of the individual's departure and loss of privileges. This is to minimize the possibility of "social engineering" attacks by the individual.

5.3.10.5. Information to suppliers and collaborating entities

Suppliers and entities collaborating with ACCV must also be informed of the departure of the individual and that he/she no longer represents ACCV.

5.3.10.6. Return of material

The return of material provided by ACCV should be verified. For example:

- PC and monitor / laptop
- Office furniture keys
- Cell phone
- etc

5.3.10.7. Suspension as PRU Operator

The need for the employee to maintain their ability to operate as a PRU Operator after leaving the organization should be reviewed. If this need does not exist, the employee's permission to access the ARCA .system should be revoked

5.4. Audit Logging Procedures

5.4.1. Types of events recorded

ACCV records all events relating to:

- Successful or failed attempts to change the security parameters of the operating system.
- Start-up and stoppage of applications.
- Successful or failed attempts to start or end a session.
- Successful or failed attempts to create, modify or delete system accounts.
- Successful or failed attempts to create, modify or delete authorized system users.
- Successful or failed attempts to request, generate, sign, issue or revoke keys and certificates.
- Successful or failed attempts to generate, sign or issue a CRL.
- Successful or failed attempts to create, modify or delete certificate holder information.
- Successful or failed attempts to access installations by authorized or unauthorized personnel.
- Successful and unsuccessful login attempts to routers and firewalls
- Logging of all administrative actions performed on routers and firewalls, including configuration changes, firmware updates, and access control modification
- Logging of all changes made to firewall rules, including additions, modifications, and deletions
- Logging of all system events and errors, including hardware failures, software crashes, and system restarts
- Backup, file and restoration.
- Changes to system configuration.
- Software and hardware updates.
- System maintenance.
- Changes of personnel

All these records are centralized at several points:

- The incident management system (change management, tracking of non-personal certificates, etc...).
- The centralized log system (centralizes via syslog the events of the core systems)
- The Active Directory log for the organization's LAN.

5.4.2. Frequency of Processing Log

Two levels of audits are established for the control of event records with a weekly and monthly frequency, respectively.

5.4.3. Retention Period for Audit Log

ACCV shall retain all the relevant audit records generated by the system for a minimum period from the date of their creation of two (2) years for those relating to daily audits, five (5) years for those relating to monthly audits and fifteen (15) years for those relating to annual audits.

5.4.4. Protection of Audit Log

Each audit log contained in these records is encrypted using the public key of a certificate that is issued for ACCV audit function. The backup copies of these records are stored in a fireproof file locked within the secure ACCV installations.

The destruction of an audit file can only be carried out with the authorization of the System Administrator, the Security Manager and ACCV Auditor. This destruction can be begun on the written recommendation of any of these three parties or of the Administrator of the audited service.

5.4.5. Audit log backup procedures

Incremental local and remote copies are generated on a daily basis, in accordance with ACCV's Backup Copies Policy.

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

The audit gathering system on ACCV information systems is a combination of automatic and manual processes carried out by the operating systems, ACCV applications, and the personnel that operates them.

5.4.7. Notification to the subject causing the event

There is no provision for notification regarding the subject giving rise to the log.

5.4.8. Vulnerability Assessments

At least one yearly analysis is carried out of vulnerabilities and perimeter security.

It is the responsibility of the analysis team coordinators to inform ACCV, via the Security Manager, of any problem preventing the performance of the audits, or the delivery of the resulting documentation. It is the responsibility of ACCV to inform the audit teams of the suspension of analyses.

The security analyses involve the initiation of the specific tasks to correct the vulnerabilities detected and the issue of a counter-report by ACCV.

5.5. Records Archival

5.5.1. Types of Records Archived

The information and events recorded are as follows:

- The audit records specified in point 5.4 of this Certification Practice Statement.

- The backup supports of the servers that comprising ACCV infrastructure.

- Documentation relating to the certificates' life cycles, including:

- Certification contract
- Copy of the identification documentation provided by the certificate requester
- Location of the User Registration Point -PRU- where the certificate was issued
- Identity of the Operator of the PRU where the certificate was issued
- Date of the last in-person identification of the subscriber

- Confidentiality agreements

- Agreements signed by ACCV

- Authorizations for Access to Information Systems (including User Registration Point Operator authorization).

5.5.2. Retention Period for Archive

All information and documentation related to the life cycle of the certificates issued by ACCV is retained for a period of 15 years.

5.5.3. Protection of Archive

Access to the archive is restricted to authorized personnel.

Likewise, the events related to the certificates issued by ACCV are cryptographically protected to guarantee the detection of manipulations in their content.

5.5.4. Archive Backup Procedures.

Two daily copies are made of the files that comprising the archives to be retained.

One copy is made locally and is stored in a fireproof safe in ACCV main Data Processing Center.

The second copy of the data is made in encrypted and remote manner and is stored in the continuity/backup Data Processing Center located in a building other than ACCV main DPC building.

5.5.5. Requirements for Time-Stamping of Records

ACCV systems record the time that the archives are made. The systems time is provided by a reliable time source. All ACCV systems synchronize their time with this source.

5.5.6. Archive Collection System (Internal or External)

The information collection system is an internal ACCV system.

5.5.7. Procedures to Obtain and Verify Archive Information

Only authorized personnel have access to physical backup and IT files in order to carry out integrity verification or other kinds of checks.

Integrity validation of electronic archives (backups) are carried out automatically at time of their generation and an incident is created in the event of errors or unexpected events.

5.6. Key Changeover

ACCV CA's private signing key is changed periodically. ACCV will stop issuing certificates associated and will proceed to sign or issue new certificates from the corresponding Certification Authority before the end of the validity period is reached, in accordance with the provisions of section 6.3.2. The prior key will continue to sign and publish CRLs until the end of its useful life. The key change or the issuance of a new certificate for the signing of the subscriber certificates will be carried out in such a way that the impact on the subscribers and trusted parties is minimal. All affected entities will be notified prior to a planned key change.

5.7. Compromise and Disaster Recovery

5.7.1. Incident and Compromise Handling Procedures

The Incident Response Plan and the Disaster Recovery Plan describe all the actions carried out and the material and human resources to solve a specific incident.

These documents detail the actions to:

Notify users, evaluate the incident, activate safeguards

At this point, if necessary, the different actors of the WebPKI ecosystem will be notified using the available and commonly used tools (Bugzilla, distribution lists, etc.) as stipulated in the different recognition policies.

Recover affected services to provide adequate levels

Restore regular operations and processes to normal levels

In the event of the unavailability of the installations of the Certification Authority for a period greater than six hours, ACCV's Incident Response Plan and a Disaster Recovery Plan shall be activated.

The Disaster Recovery Plan guarantees that services identified as critical due to their availability requirement will be available in the Continuity DPC in less than 12 hours following activation of the Plan.

ACCV annually test, review, and update these procedures.

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

If hardware, software and/or data resources are altered or are suspected of having been altered, the operation of ACCV's services shall be suspended until a secure environment is re-established with the incorporation of new components of creditable effectiveness. In parallel, an audit shall be carried out to identify the cause of the alteration and ensure the non-reoccurrence of the alteration.

In the event of issued certificates being affected, the certificate subscribers shall be notified of this and re-certification shall take place.

All these actions are included in the incident response plan.

5.7.3. Entity Private Key Compromise Procedures

In the event of the compromise of an entity's key, it shall immediately be revoked and this shall be notified to the rest of the entities that are part of ACCV whether they are dependent or not on the affected entity. The corresponding CRL shall be generated and published, the entity operations shall be suspended and the process of generation, certification and start-up of a new entity with the same name as the withdrawn one and with a new key pair will begin.

In the event that the affected entity is a CA, the entity's revoked certificate shall remain accessible in ACCV repository for the purpose of continuing to permit the verification of the certificates issued during the entity's period of operation.

The entities comprising ACCV that are dependent on the renewed entity shall be informed about the fact and ordered to request their re-certification due to the entity having been renewed.

Certificates signed by entities dependent on the compromised entity during the period between compromise of the key and revocation of the corresponding certificate, shall in turn be revoked, and their subscribers informed and re-certified.

5.7.4. Business Continuity Capabilities after a Disaster

In the event of a natural disaster affecting the installations of ACCV's main Data Processing Center and, therefore, the services provided from this location, the Service Continuity Plan shall be activated, guaranteeing that the services identified as critical due to their availability requirement, shall be available in the Continuity DPC in less than 12 hours following the Plan activation, and the remaining essential services shall be available within reasonable and appropriate periods to their level of necessity and critical nature.

5.8. CA or RA Termination

The causes that can lead to the termination of the Certification Authority operations are as follows:

- Compromise of the CA private key
- Political decision by the Autonomous Government of Valencia

In the event of termination of its activity as Certification Services Provider, ACCV shall carry out the following actions with a minimum notice period of two months:

- To duly inform about their intentions to terminate their activity to all the subscribers of their certificates, as well as to third parties with whom it has signed a contract / agreement or who may be affected.

- To finalize any contract / agreement that allows acting on your behalf in the procedure of issuing certificates.

- With the consent of the subscribers, transfer to another Qualified Trust Service Provider those certificates that remain valid on the effective date of cessation of activity. If this transfer is not accepted or not possible, the certificates will be revoked.

- To communicate to the Ministry that at that moment it has the competences in the matter, the cessation of its activity and the destination that it will give to the certificates, as well as any other relevant circumstance related to the cessation of activity.

- To send to the Ministry competent in the matter all the information related to the revoked certificates so that the latter takes care of their custody to the pertinent effects.

6. Technical Security Controls

6.1. Key Pair Generation and Installation

6.1.1. Key pair generation

6.1.1.1. CA Key Pair Generation

Following this procedure, ACCV will prepare and follow a Key Generation Script, have a Qualified Auditor witness the CA Key Pair generation process, and have a Qualified Auditor issue a report opining that the CA followed its key ceremony during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair.

This procedure describes the following:

- roles participating in the ceremony;
- functions to be performed by every role and in which phases;
- responsibilities during and after the ceremony; and
- requirements of evidence to be collected of the ceremony.

The procedure of issuing, signing and distributing of new CA Certificate, specifying that before the expiration of the Certificate a new one is generated, thus avoiding possible interruptions in the operations from any entity that can trust the Certificate.

For reasons of security and quality, the Keys that ACCV needs to carry out its activities as a Trust Service Provider will be generated by the Entity itself inside its own infrastructures, in a physically secure environment and by at least two authorised persons.

Key pairs for all ACCV internal components are generated on cryptography hardware modules with FIPS 140-1 Level 4 certification. In the case of components of CA type, there is audited documentation of the creation ceremony, which includes the steps followed, the personnel involved and the distribution of the activation mechanisms. All these steps are carried out and recorded in the presence of a qualified auditor and in a secured environment.

Key algorithms and lengths employed are based on standards that are broadly recognised for the purpose for which they are generated.

The technical components necessary to create Keys are designed so that a Key is only generated once and so that a Private Key cannot be calculated using its Public Key.

6.1.1.2. RA Key Pair Generation

Not stipulated

6.1.1.3. Subscriber Key Pair Generation

6.1.1.3.1. Qualified Website Authentication Certificates

The key pair for certificates issued under this policy is generated in software by the certificate subscriber.

6.1.1.3.2. Electronic Administrative Headquarters Certificates in Hardware Secure Module

The key pair for certificates issued under this policy is generated in the user's HSM and never leaves it.

6.1.1.3.3. Electronic Administrative Headquarters Certificates based on software

The key pair for certificates issued under this policy is generated in software by the certificate subscriber.

6.1.1.3.4. Server Authentication Certificates

The key pair for certificates issued under this policy is generated in software by the certificate subscriber.

6.1.2. Private Key Delivery to Subscriber

The private key is generated by the subscriber, therefore, it is not necessary to deliver it to the subscriber.

6.1.3. Public Key Delivery to Certificate Issuer

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

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

6.1.4. CA Public Key Delivery to Relying Parties

The public keys of all CAs belonging to ACCV trust hierarchy can be downloaded from the website http://www.accv.es.

6.1.5. Key Sizes

The keys of ACCVRAIZ1 root and the certificate authorities that are in the same hierarchy are RSA keys of 4096 bits in length.

The keys of ACCV ROOT RSA TLS 2024 root ACCV ROOT and certificate authorities that are in the same hierarchy are RSA keys of 4096 bits in length.

The keys of ACCV ROOT ECC TLS 2024 root ACCV ROOT and certification authorities that are in the same hierarchy are 384-bit long ECC keys.

The key size for end-entity certificates issued under the scope of this Certification Policy is:

- For RSA keys of at least 2048 bits.
- For ECDSA keys of at least NIST ECC P-256.

6.1.6. Public Key Parameters Generation and Quality Checking

Keys for ACCVRAIZ1 and CAs of the same hierarchy are created with the RSA algorithm.

Keys for ACCV ROOT RSA TLS 2024 and CAs of the same hierarchy are created with the RSA algorithm.

Keys for ACCV ROOT ECC TLS 2024 and CAs of the same hierarchy are created with the ECC algorithm.

For end-entity certificates, the parameters defined in ETSI TS 119 312 "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites" are used.

The parameters used are as follows:

Signature Suite	Hash Function	Padding Method	Signature algorithm
sha256-with-rsa	sha256	emsa-pkcs1-v1.5	rsa
sha2-with-ecdsa	SHA-256, SHA-384 or SHA-512		ecdsa

ACCV performs the validation of RSA and ECC keys following the procedures defined in NIST SP 800-89 and NIST SP 800-56A: Revision 3

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

All subscriber certificates issued by ACCV contain the KEY USAGE and EXTENDED KEY extensions.

USAGE defined by the X.509 v3 standard for the definition and limitation of these purposes.

The private keys corresponding to the root certificates are not used to sign certificates, except in the following cases

Self-signed certificates to represent the Root CA itself.

Certificates for SubCAs, and, if applicable, Cross Certificates.

Certificates for infrastructure purposes (administrative function certificates, internal CA operating device certificates)

Certificates for OCSP response verification

The keys defined by this policy will be used for the purposes described in 1.3 User Community and Scope of Application.

The detailed definition of the certificate profile and the uses of the keys can be found in section 7 of this document *"Certificate, CRL and OCSP Profiles"*.

6.1.8. Key generation hardware/software

6.1.8.1. CA Keys

Keys for PKI entities are generated on cryptographic HSM devices with FIPS 140-1 Level 4 certification.

The devices used are:

- Thales Nshield 500e F2, with EAL-4+ certification and FIPS 140-2 Level3
- AEP Keyper Enterprise Model 9720, with FIPS-140-2 Level4 certification.
- Thales Luna PCIe HSM A700 with FIPS 140-2 Level3 Certification
- Thales Luna Network HSM A790 with certification FIPS 140-2 Level3

6.1.8.2. Qualified Website Authentication Certificates

Key generation is performed in software by the certificate subscriber.

6.1.8.3. Electronic Administrative Headquarters Certificates in Hardware Secure Module

Key generation is performed in HSM.

The minimum requirements for these devices are those specified by the corresponding competent Ministry, and in accordance with European technical standards.

6.1.8.4. Electronic Administrative Headquarters Certificates based on software

Key generation is performed in software by the certificate subscriber.

6.1.8.5. Server Authentication Certificates

Key generation is performed in software by the certificate subscriber.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

ACCV will protect its Private Key(s) in accordance with the provisions of this CPS and in compliance with the CA/Browser Forum Baseline Requirements.

6.2.1. Cryptographic Module Standards and Controls

6.2.1.1. CA Keys

It is mandatory that the modules used for the creation of keys used by all CAs integrated in the trust hierarchies comply with a security certification appropriate to their functionality and the security required.

A hardware security module (HSM) is a security device that generates and protects cryptographic keys. Therefore, these products must meet, at a minimum, FIPS 140-2 level 3, or Common Criteria EAL 4+ criteria for the corresponding protection profile. ACCV has procedures and policies in place to verify that an HSM has not been tampered with during transport and storage.

Cryptographic devices with qualified electronic signature certificates, suitable as qualified signature creation devices (DSCF), meet the requirements of the CC EAL4+ security level, although certifications that meet a minimum of ITSEC E3, FIPS 140-2 Level 2 or equivalent security criteria are also acceptable. The European reference standard for the devices used is Commission Implementing Decision (EU) 2016/650 of 25 April 2016.

6.2.1.2. Qualified Website Authentication Certificates

The cryptographic modules are located in software on the subscriber's device.

6.2.1.3. Electronic Administrative Headquarters Certificates in Hardware Secure Module

HSM devices used in the issuance of these certificates must be ITSEC E5 high, FIPS 140-2 level 3 or equivalent certified and support PKCS#11 and CSP standards.

HSMs certified by the nationally accredited agency (OC-CCN https://oc.ccn.cni.es/index.php/es/) are also accepted.

Key generation is performed in the HSMs.

The minimum requirements for these devices are those specified by the relevant competent authority and in accordance with European technical standards.

These HSMs must be accredited as Secure Signature Creation Device/Secure Seal Creation Device according to eIDAS (QsigCD/QsealCD) regulations.

6.2.1.4. Electronic Administrative Headquarters Certificates based on software

The cryptographic modules are located in software on the subscriber's device.

6.2.1.5. Server Authentication Certificates

The cryptographic modules are located in software on the subscriber's device.

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

The private keys used by the certification authorities that make up both hierarchies are under multi-person control. All of them are divided into several fragments and a minimum of two of these fragments is necessary to access the key.

Not applicable in the case of end-entity/subscriber private keys.

6.2.3. Private Key Escrow

Subscriber private signature keys are not stored.

Private keys of the Certification Authorities and Registration Authorities that are part of ACCV are stored in cryptography hardware devices with FIPS 140-2 level 3 certification.

The rest of the private keys of entities comprising ACCV are contained on cryptography smartcards in the possession of the Administrators of each entity.

6.2.4. Private Key Backup

The CA private signature keys SHALL be backed up under the same multi-person control as the original signature key.

There is a procedure for activating the keys of the cryptographic backup module of the CA (root or subordinate) that can be applied in the event of a contingency.

All private keys of ACCV entities are under the exclusive control of ACCV.

The private keys of the subscribers of the certificates defined by this policy are not stored or backed up.

6.2.5. Private Key Archival.

Backups of expired private keys of ACCV entities are stored in encrypted form in a fireproof safe, which can only be accessed by authorized personnel with at least dual access.

All private keys of ACCV entities are under the exclusive control of ACCV.

The private keys of the subscribers of the certificates defined by this policy are not archived.

6.2.6. Private Key Transfer into or from a Cryptographic Module

6.2.6.1. CA Keys

Private keys are created on the cryptography module at the time of the creation of each ACCV entity that use these modules, fulfilling the requirements defined in section 6.2.1.

6.2.6.2. Qualified Website Authentication Certificates

Not applicable within the scope of this CPS.

6.2.6.3. Electronic Administrative Headquarters Certificates in Hardware Secure Module

The generation of the keys that are associated to the certificate is carried out inside the HSM and never leaves it.

6.2.6.4. Electronic Administrative Headquarters Certificates based on software

Not applicable within the scope of this CPS.

6.2.6.5. Server Authentication Certificates

Not applicable within the scope of this CPS.

6.2.7. Storage of the private key in the cryptographic module

6.2.7.1. CA Keys

Private keys are created in the cryptographic module at the time of the creation of each of ACCV entities that make use of these modules, complying with the requirements defined in the section "Private keys". 6.2.1

6.2.7.2. Qualified Website Authentication Certificates

Not applicable within the scope of this CPS.

6.2.7.3. Electronic Administrative Headquarters Certificates in Hardware Secure Module

The private key is generated by the applicant and is never in possession of Agencia de Tecnología y Certificación Electrónica. The storage of the private key will depend on the mechanisms of the HSM chosen to generate and store the keys.

6.2.7.4. Electronic Administrative Headquarters Certificates based on software

Not applicable within the scope of this CPS.

6.2.7.5. Server Authentication Certificates

Not applicable within the scope of this CPS.

6.2.8. Method of Activating Private Key

6.2.8.1. CA Keys

The private keys of each of the CAs that conform trust hierarchies are activated by means of the initialization of the CA software and the activation of the cryptography hardware that contains the keys.

Once the CA system has been activated, a threshold number of shareholders SHALL be required to supply their activation data in order to activate a CA's Private Key, as defined in 6.2.2. Once the Private Key is activated, the Private Key MAY be active for an indefinite period until it is deactivated when the CA goes offline.

6.2.8.2. Qualified Website Authentication Certificates

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

6.2.8.3. Electronic Administrative Headquarters Certificates in Hardware Secure Module

The private key is generated by the applicant and is never in possession of ACCV. The activation will depend on the mechanisms of the HSM chosen to generate and store the keys.

6.2.8.4. Electronic Administrative Headquarters Certificates based on software

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

6.2.8.5. Server Authentication Certificates

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

6.2.9. Method of Deactivating Private Key

6.2.9.1. CA Keys

An Administrator can proceed to deactivate ACCV Certification Authorities key by stopping the CA software.

6.2.9.2. Qualified Website Authentication Certificates

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

6.2.9.3. Electronic Administrative Headquarters Certificates in Hardware Secure Module

The private key is generated by the applicant and is never in possession of Agencia de Tecnología y Certificación Electrónica. The deactivation will depend on the mechanisms of the HSM chosen to generate and store the keys.

6.2.9.4. Electronic Administrative Headquarters Certificates based on software

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

6.2.9.5. Server Authentication Certificates

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

6.2.10. Method of Destroying Private Key

The destruction of a token can be done for the following reasons:

- Cessation of the use of the keys contained
- Deterioration such that it does not allow efficient use of the token, but does not totally prevent its use.
- Recovery of a lost token or stolen.

Destruction must always be preceded by a revocation of the certificate associated with the token, if it is still valid. Private Keys are destroyed in accordance with NIST SP 800-88.

6.2.10.1. Cryptographic hardware

HSM destruction is not contemplated, due to its high cost. Instead, initialization tasks will be carried out. During the transition from the "operational" to the "initialization" state, the keys contained therein are securely deleted.

6.2.10.2. Cryptographic cards

The destruction of the token can be done when the information printed on the token becomes invalid and a new card must be issued.

The task to be performed consists of a **Secure Destruction** of the Token at the physical level.

6.2.10.3. Qualified Website Authentication Certificates

The private key is generated by the applicant and is never in the possession of ACCV. It can be destroyed by deleting it following the instructions of the application that hosts it.

6.2.10.4. Electronic Administrative Headquarters Certificates in Hardware Secure Module

The private key is generated by the applicant and is never in possession of Agencia de Tecnología y Certificación Electrónica. Destruction will depend on the mechanisms of the HSM chosen to generate and store the keys.

6.2.10.5. Electronic Administrative Headquarters Certificates based on software

The private key is generated by the applicant and is never in the possession of ACCV. It can be destroyed by deleting it following the instructions of the application that hosts it.

6.2.10.6. Server Authentication Certificates

The private key is generated by the applicant and is never in the possession of ACCV. It can be destroyed by deleting it following the instructions of the application that hosts it.

6.2.11. Cryptographic Module Rating

See6.2.1 section of this document.

6.3. Other Aspects of Key Pair Management.

6.3.1. Public Key Archival

ACCV maintains an archive of all certificates issued for a period of fifteen (15) years.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

ACCVRAIZ1 root CA certificate is valid until 12/31/2030 and the CAs belonging to its hierarchy are valid for 4 years less than the root CA.

ACCV ROOT RSA TLS 2024 Root CA certificate is valid until Saturday, January 26, 2049 and the CAs belonging to its hierarchy are valid until February 23, 2039.

ACCV ROOT ECC TLS 2024 Root CA certificate is valid until Saturday, January 26, 2049 and the CAs belonging to its hierarchy are valid until February 23, 2039.

Registration Authorities and other ACCV entities have a maximum term of three (3) years.

Certificates issued under this policy are valid for a maximum of 12 months.

The key used for the issuance of certificates is provided for each issuance, and therefore they are also valid for a maximum of 12 months. This is the maximum validity date allowed in the application for certificates issued under this policy.

ACCVCA-120 certificate is valid from January 27, 2015 through January 1, 2027.

ACCV RSA1 TLS certificate is valid from February 27, 2024 to February 23, 2039.

ACCV ECC1 TLS certificate is valid from February 27, 2024 to February 23, 2039.

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

6.4.1.1. Certification Authorities

The activation data of ACCV Certification Authorities are generated and stored in secure devices in possession of authorized personnel.

6.4.1.2. Qualified Website Authentication Certificates

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

6.4.1.3. Electronic Administrative Headquarters Certificates in Hardware Secure Module

The private key is generated by the applicant and is never in possession of ACCV. The activation data will depend on the mechanisms of the HSM chosen to generate and store the keys.

6.4.1.4. Electronic Administrative Headquarters Certificates based on software

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

6.4.1.5. Server Authentication Certificates

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

6.4.2. Activation Data Protection

Only authorized personnel know the PINs and passwords to access the activation data.

6.4.2.1. Certification Authorities

Only authorized personnel know the PINs and passwords to access the activation data.

6.4.2.2. Qualified Website Authentication Certificates

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

6.4.2.3. Electronic Administrative Headquarters Certificates in Hardware Secure Module

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

6.4.2.4. Electronic Administrative Headquarters Certificates based on software

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

6.4.2.5. Server Authentication Certificates

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

6.4.3. Other Aspects of Activation Data

There are no other aspects to consider.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

ACCV implements an Information Security Management System (ISMS) based on the **ISO-27001** standard and establishes controls and procedures for its correct compliance.

- - Operational controls
    - - User procedures documented
    - - Safe delete procedures for storage and removable media, so obsolete equipment.
    - - Contingency and Continuity plans
    - - Antivirus and Antimalware
    - - Strict policy on which types of software users may install
- - Security data exchanges
    - - Transmission with CA and RA
    - - Transmission with CA and RA Databases
    - - User data
- - Access control
    - - Dual factor based authentication for CA and RA operators
    - - Use the principle of least privilege
    - - Unique and nominal user IDs
    - - Periodic audits of the privileges applied
    - - Strict provisioning procedures
    - - Enforcement guides for passwords and security tokens.

ACCV has a security policy and procedures to guarantee security.

6.5.2. Computer Security Rating

ACCV implements an Information Security Management System (ISMS) based on the **ISO-27001** standard and establishes controls and procedures for its correct compliance.

During the continuous evaluation of the ISMS, impact and risk analyses are performed to assess IT security.

6.6. Lifecycle Technical Controls

6.6.1. System Development Controls

ACCV implements an Information Security Management System (ISMS) based in standard **ISO-27001** and establishes controls and procedures for its correct compliance.

There are several procedures and guidelines from ACCV associated with development control:

- Development and Testing Policy

- ACCV Development Best Practices Guidelines

- Change Control Procedure

- Capacity Management

- Business Continuity Plan

All these procedures have the corresponding documentary support in the ACCV document manager.

The characteristics of the ACCV development system:

Continuous integration process

Tools to analyze and detect anomalies in the code

Strict separation between the development and test platform and the working platform

The test and real data are independent

Test and development never work with real data

The production process is carried out after an exhaustive approval process, following the change control procedure, always warranting the roll-back.

6.6.2. Security Management Controls

ACCV implements an Information Security Management System (ISMS) based in standard **ISO-27001** and establishes controls and procedures for its correct compliance.

There are several procedures and guidelines from ACCV associated with security control:

- Staff Security Functions and Controls
- Asset Inventory
- Procedure for the safe use of devices and media
- Business Continuity Plan
- Change Control Procedure
- Incident Management Procedure
- Vulnerability Management Procedure

All these procedures have the corresponding documentary support in the ACCV document manager.

Certificate subscribers can contact the ACCV to report any incident using the channels specified in:

https://www.accv.es/contacto/

and as indicated in 1.5.2

ACCV keeps a detailed record of all incidents, as well as the solutions implemented in its resolution, as specified in the ISMS.

6.6.3. Lifecycle Security Controls

ACCV periodically performs security and vulnerability tests in the different phases of the software life cycle (SDL).

- Threat modeling to avoid errors in the design phase
- Automatic code review tools for detecting bugs, vulnerabilities and code defects (Sonarqube)
- Vulnerability scanning and penetration testing.

6.7. Network Security Controls

ACCV protects physical access to network management devices and has an architecture that distributes traffic according to its security characteristics, creating clearly defined network sections. These sections are divided by multi-level zoning, using multiple redundant firewalls. Sensitive information transferred over insecure networks is encrypted using SSL protocols. ACCV conforms with the latest version of the CAB Forum Network and Certificate System Security Requirements.

6.8. Time-Stamping

ACCV has a qualified Time Stamping Authority (TSA).

The rules and procedures governing the TSA can be found in its respective policy at https://www.accv.es/quienes-somos/practicas-y-politicas-de-certificacion/politicas-de-certificacion/.

The anonymous access URL is at:

http://tss.accv.es:8318/tsa

7. Certificate, CRL and OCSP Profiles

7.1. Certificate Profile

ACCV generates serial numbers with 127 bits of entropy. The main application forces this behavior. It implements a singleton serial number generator using SecureRandom. This generator generates random serial numbers of 16 octets (128 bits).

7.1.1. Version number

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

X.509 is a standard developed by the International Telecommunication Union (international organization of the United Nations for the coordination of telecommunications network services between governments and companies) for Public Key Infrastructures and digital certificates.

7.1.2. Certificate Extensions; implementation of RFC 5280

Certificate extensions, their criticality and cryptographic algorithm object identifiers are provisioned according to IETF RFC 5280 standards and comply with CAB Forum Baseline Requirements.

7.1.2.1. Root CAs

The extensions used generically in the certificates are:

- Key Usage. Marked as critical in all cases
  - KeyCertSign CRLSign
- Basic Constraint
  - Present and marked as critical
  - Field CA TRUE
- Certification policies
  - ACCVRAIZ1: Present and marked non-critical
  - ACCV ROOT RSA TLS 2024: Not Present
  - ACCV ROOT ECC TLS 2024: Not present
- SubjectAlternativeName.
  - ACCVRAIZ1: Present and marked non-critical
  - ACCV ROOT RSA TLS 2024: Not Present
  - ACCV ROOT ECC TLS 2024: Not present
- CRL Distribution Point.
  - ACCVRAIZ1: Present and marked non-critical
  - ACCV ROOT RSA TLS 2024: Not Present
  - ACCV ROOT ECC TLS 2024: Not present
- extKeyUsage
  - Not present
- authorityInformationAccess
  - ACCVRAIZ1: Present and marked non-critical
  - ACCV ROOT RSA TLS 2024: Not Present

  - ACCV ROOT ECC TLS 2024: Not present
- nameConstraints: Not present

7.1.2.2. Subordinate Cas

The extensions used generically in the certificates are:

- Key Usage. Marked as critical in all cases
  - KeyCertSign CRLSign
- Basic Constraint
  - Present and marked as critical
  - Field CA TRUE
- Certification policies
  - Present and marked as non-critical
- SubjectAlternativeName.
  - ACCVCA-110: Present and marked non-critical
  - ACCVCA-120: Present and marked non-critical
  - ACCVCA-130: Present and marked non-critical
  - ACCV RSA1 TLS: Not Present
  - ACCV ECC1 TLS: Not present
- CRL Distribution Point.
  - ACCVCA-110: Present and marked non-critical
  - ACCVCA-120: Present and marked non-critical
  - ACCVCA-130: Present and marked non-critical
  - ACCV RSA1 TLS: Present and marked as non-critical
  - ACCV ECC1 TLS: Present and marked as non-critical
- extKeyUsage
  - ACCVCA-110: Not present
  - ACCVCA-120: Not present
  - ACCVCA-130: Not present
  - ACCV RSA1 TLS: Client authentication, Server authentication
  - ACCV ECC1 TLS: Client authentication, Server authentication
- authorityInformationAccess
  - Present and marked as non-critical
- nameConstraints: Not present

7.1.2.3. Subscriber Certificates

7.1.2.3.1. Qualified Website Authentication Certificates

Field	**Value**
Subject	
SerialNumber	NIF of the Administration, organization or entity of public or private law subscriber of the certificate, to which the website is linked.
CommonName	Domain Name (DNS) where the certificate will reside. If it appears it must match a DNSName of the SAN. (OPTIONAL not recommended)
OrganizationIdentifier (2.5.4.97)	Tax ID number of the entity, as it appears in the official records. Encoded According to European Standard ETSI EN 319 412-1
Organization	Denomination ("official" name) of the Administration, organization or public law entity subscribing the certificate and owner of the domain.
Locality	City
State	Province
Country	ES (code ISO 3166-1)
Version	V3
SerialNumber	Unique identifier of the certificate. Less than 32 hexadecimal characters.
Signature algorithm	ACCVCA-120 sha256withRSAEncryption ACCV RSA1 TLS sha256withRSAEncryption ACCV ECC1 TLS ecdsa-with-SHA384
Issuer	DN of the CA issuing the certificate (see 7.1.4)
Valid from	Issuance Date
Valid until	Expiration Date
Public Key	Octet String containing the certificate public key
Extended Key Usage	Server Authentication Client Authentication (optional)
CRL Distribution Point	ACCVCA-120: http://www.accv.es/fileadmin/Archivos/certificados/accvca120_der.crl ACCV RSA1 TLS: http://www.accv.es/gestcert/accv_rsa1_tls.crl ACCV ECC1 TLS: http://www.accv.es/gestcert/accv_ecc1_tls.crl
SubjectAlternativeName	
	dnsName: DNS Domain Name 1 (if commonName is included it must have the same value)
Optional	dnsName: DNS Domain Name 2
Optional	dnsName: DNS Domain Name 3
Optional	dnsName: DNS Domain Name 4
Optional	dnsName: DNS Domain Name 5
Optional	dnsName: DNS Domain Name 6
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	QCP-w Qualified website certificate in accordance with EU Regulation 910/2014.
	itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112)
	policy-identifiers(1) qncp-web (5)

Policy OID	1.3.6.1.4.1.8149.3.3.5.0
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	ACCVCA-120: http://www.accv.es/gestcert/ACCVCA120SHA2.cacert.crt ACCV RSA1 TLS: http://www.accv.es/gestcert/accv_rsa1_tls.crt ACCV ECC1 TLS: http://www.accv.es/gestcert/accv_ecc1_tls.crt
Fingerprint issuer	Fingerprint of the certificate of the CA issuing the certificate
Hashing algorithm	RSA: SHA-256 ECC: SHA-384
KeyUsage (critical)	RSA: Digital Signature, Key Encipherment ECC: Digital Signature
SCT List 1.3.6.1.4.1.11129.2.4.2	Signed Certificate Timestamp List SCT Responses from Qualified Logs. At least three different responses.
QcStatement	**QC (Qualified Certificate) Fields**
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-V1.1-EN.pdf Location of PKI Disclosure Statement
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 *Province (optional)*
	registrationReference Registration reference assigned according to the identified registration scheme (CIF)

7.1.2.3.2. Electronic Administrative Headquarters Certificates in Hardware Secure Module

Field	Value
Subject	
SerialNumber	NIF of the Administration, organism or public law entity subscribing the certificate, to which the head office is linked.
CommonName	Domain Name (DNS) where the certificate will reside. If it appears it must match a DNSName of the SAN. (OPTIONAL not recommended)
OrganizationIdentifier (2.5.4.97)	Tax ID number of the entity, as it appears in the official records. Encoded According to European Standard ETSI EN 319 412-1
Organization	Denomination ("official" name) of the Administration, agency or public law entity subscribing the certificate, to which the site is linked.
Locality	City
State	Province
Country	ES State whose law governs the name, which will be "Spain" because they are public entities.
Version	V3
SerialNumber	Unique identifier of the certificate. Less than 32 hexadecimal characters.
Signature algorithm	ACCVCA-120 sha256withRSAEncryption ACCV RSA1 TLS sha256withRSAEncryption ACCV ECC1 TLS ecdsa-with-SHA384
Issuer	DN of the CA issuing the certificate (see 7.1.4)
Valid from	Issuance Date
Valid until	Expiration Date
Public Key	Octet String containing the public key of the host certificate
Extended Key Usage	Server Authentication Client Authentication (optional)
CRL Distribution Point	ACCVCA-120: http://www.accv.es/fileadmin/Archivos/certificados/accvca120_der.crl ACCV RSA1 TLS: http://www.accv.es/gestcert/accv_rsa1_tls.crl ACCV ECC1 TLS: http://www.accv.es/gestcert/accv_ecc1_tls.crl
SubjectAlternativeName	
	DnsName: DNS Domain Name of the Headquarters (if commonName is included it must have the same value)
Optional	DnsName: DNS Domain Name of the Head Office
Optional	DnsName: DNS Domain Name of the Head Office
Optional	DnsName: DNS Domain Name of the Head Office
Optional	DnsName: DNS Domain Name of the Head Office
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 website certificate in accordance with EU Regulation 910/2014.
	itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112)
	policy-identifiers(1) qncp-web (5)

Policy OID	1.3.6.1.4.1.8149.3.14.6.0
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	ACCVCA-120: http://www.accv.es/gestcert/ACCVCA120SHA2.cacert.crt ACCV RSA1 TLS: http://www.accv.es/gestcert/accv_rsa1_tls.crt ACCV ECC1 TLS: http://www.accv.es/gestcert/accv_ecc1_tls.crt
Fingerprint issuer	Fingerprint of the certificate of the CA issuing the certificate (see CPS)
Hashing algorithm	RSA: SHA-256 ECC: SHA-384
KeyUsage (critical)	RSA: Digital Signature, Key Encipherment ECC: Digital Signature
SCT List 1.3.6.1.4.4.1.11129.2.4.2	Signed Certificate Timestamp List
QcStatement	**QC (Qualified Certificate) Fields**
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-V1.1-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)*

7.1.2.3.3. Electronic Administrative Headquarters Certificates based on software

Field	**Value**
Subject	
SerialNumber	NIF of the Administration, organism or public law entity subscribing the certificate, to which the head office is linked.
CommonName	Domain Name (DNS) where the certificate will reside. If it appears it must match a DNSName of the SAN. (OPTIONAL not recommended)
OrganizationIdentifier (2.5.4.97)	Tax ID number of the entity, as it appears in the official records. Encoded According to European Standard ETSI EN 319 412-1
Organization	Denomination ("official" name) of the Administration, agency or public law entity subscribing the certificate, to which the site is linked.
Locality	City
State	Province
Country	ES State whose law governs the name, which will be "Spain" because they are public entities.
Version	V3
SerialNumber	Unique identifier of the certificate. Less than 32 hexadecimal characters.
Signature algorithm	ACCVCA-120 sha256withRSAEncryption ACCV RSA1 TLS sha256withRSAEncryption ACCV ECC1 TLS ecdsa-with-SHA384
Issuer	DN of the CA issuing the certificate (see 7.1.4)
Valid from	Issuance Date
Valid until	Expiration Date
Public Key	Octet String containing the public key of the host certificate
Extended Key Usage	
	Server Authentication Client Authentication (optional)
CRL Distribution Point	
	ACCVCA-120: http://www.accv.es/fileadmin/Archivos/certificados/accvca120_der.crl ACCV RSA1 TLS: http://www.accv.es/gestcert/accv_rsa1_tls.crl ACCV ECC1 TLS: http://www.accv.es/gestcert/accv_ecc1_tls.crl
SubjectAlternativeName	
	DnsName: DNS Domain Name of the Headquarters (if commonName is included it must have the same value)
Optional	DnsName: DNS Domain Name of the Head Office

Optional	DnsName: DNS Domain Name of the Head Office
Optional	DnsName: DNS Domain Name of the Head Office
Optional	DnsName: DNS Domain Name of the Head Office
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	2.16.724.1.3.5.5.2

Policy OID	QCP-w Qualified website certificate in accordance with EU Regulation 910/2014.
	itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112)
	policy-identifiers(1) qncp-web (5)
	0.4.0.194112.1.5

Policy OID	1.3.6.1.4.1.8149.3.15.6.0
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	ACCVCA-120: http://www.accv.es/gestcert/ACCVCA120SHA2.cacert.crt ACCV RSA1 TLS: http://www.accv.es/gestcert/accv_rsa1_tls.crt ACCV ECC1 TLS: http://www.accv.es/gestcert/accv_ecc1_tls.crt
Fingerprint issuer	Fingerprint of the certificate of the CA issuing the certificate (see CPS)
Hashing algorithm	RSA: SHA-256 ECC: SHA-384
KeyUsage (critical)	
	RSA: Digital Signature, Key Encipherment ECC: Digital Signature
SCT List 1.3.6.1.4.4.1.11129.2.4.2	Signed Certificate Timestamp List
QcStatement	**QC (Qualified Certificate) Fields**

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-V1.1-EN.pdf *Location of PKI Disclosure Statement*
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)*

7.1.2.3.4. Server Authentication Certificates

Field	**Value**
Subject	
SerialNumber	NIF of the Administration, organization or entity of public or private law subscriber of the certificate, to which the website is linked.
CommonName	Domain Name (DNS) where the certificate will reside. If it appears it must match a DNSName of the SAN. (OPTIONAL not recommended)
OrganizationIdentifier (2.5.4.97)	Tax ID number of the entity, as it appears in the official records. Encoded According to European Standard ETSI EN 319 412-1
Organization	Denomination ("official" name) of the Administration, organization or public law entity subscribing the certificate and owner of the domain.
Locality	City
State	Province
Country	ES (code ISO 3166-1)
Version	V3
SerialNumber	Unique identifier of the certificate. Less than 32 hexadecimal characters.
Signature algorithm	ACCVCA-120 sha256withRSAEncryption ACCV RSA1 TLS sha256withRSAEncryption ACCV ECC1 TLS ecdsa-with-SHA384
Issuer	DN of the CA issuing the certificate (see 7.1.4)
Valid from	Issuance Date
Valid until	Expiration Date
Public Key	Octet String containing the certificate public key

Extended Key Usage	
	Server Authentication Client Authentication (optional)
CRL Distribution Point	ACCVCA-120: http://www.accv.es/fileadmin/Archivos/certificados/accvca120_der.crl ACCV RSA1 TLS: http://www.accv.es/gestcert/accv_rsa1_tls.crl ACCV ECC1 TLS: http://www.accv.es/gestcert/accv_ecc1_tls.crl
SubjectAlternativeName	
	dnsName: DNS Domain Name (if commonName is included it must have the same value)
Optional	dnsName: DNS Domain Name 2
Optional	dnsName: DNS Domain Name 3
Optional	dnsName: DNS Domain Name 4
Optional	dnsName: DNS Domain Name 5
Certificate Policy Extensions	
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	1.3.6.1.4.1.8149.3.36.2.0
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	ACCVCA-120: http://www.accv.es/gestcert/ACCVCA120SHA2.cacert.crt ACCV RSA1 TLS: http://www.accv.es/gestcert/accv_rsa1_tls.crt ACCV ECC1 TLS: http://www.accv.es/gestcert/accv_ecc1_tls.crt
Fingerprint issuer	Fingerprint of the certificate of the CA issuing the certificate (see CPS)
Hashing algorithm	RSA: SHA-256 ECC: SHA-384
KeyUsage (critical)	
	RSA: Digital Signature, Key Encipherment ECC: Digital Signature
SCT List1.3.6.1.4.1.11129.2.4.2	Signed Certificate Timestamp List *SCT Responses from Qualified Logs. At least three different responses.*
CA/Browser Forum Organization	cabfOrganizationIdentifier (OID: 2.23.140.3.1)

Identifier Field	{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 *Province (optional)*
	registrationReference *Registration reference assigned according to the identified registration scheme (CIF)*

In all cases, the specifications and limits established in RFC-5280 shall be complied with.

In the case of pre-certificates (only applicable to certificates published in the Certificate Transparency logs) the profile is structurally identical to the final certificate, with the exception of a special extension marked as critical with the OID

1.3.6.1.4.1.11129.2.4.3

This extension ensures that the Precertificate will not be accepted as a Certificate by clients conforming to RFC 5280. The existence of a signed Precertificate can be treated as evidence of a corresponding Certificate also existing, as the signature represents a binding commitment by the CA that it may issue such a Certificate.

7.1.3. Object Identifiers (OID) of the algorithms

Object Identifier (OID) of Cryptographic algorithms:

- sha1withRSAEncryption (1.2.840.113549.1.1.5)
- sha256withRSAEncryption (1.2.840.113549.1.1.11)
- sha384WithRSAEncryption(1.2.840.113549.1.1.12)
- sha512withRSAEncryption (1.2.840.113549.1.1.13)
- rsaEncryption (1.2.840.113549.1.1.1)
- ECC P-256 secp256r1 (OID: 1.2.840.10045.3.1.7).
- ECC P-384 secp384r1 (OID: 1.3.132.0.34).
- ECC P-521 secp521r1 (OID: 1.3.132.0.35).
- ecdsa-with-SHA256 (1.2.840.10045.4.3.2)
- ecdsa-with-SHA384 (1.2.840.10045.4.3.3)

As of January 16, 2015, ACCV does not issue subscriber certificates using the SHA-1 algorithm with an expiration date greater than January 1, 2017.

7.1.3.1. SubjectPublicKeyInfo

The following requirements apply to the subjectPublicKeyInfo field of a certificate or Pre-Certificate. Pre-certificate. Other encodings are not allowed.

7.1.3.1.1. RSA

ACCV indicates an RSA key using the rsaEncryption algorithm identifier (OID: 1.2.840.113549.1.1.1.1). The parameters are present, and are an explicit NULL.

The AlgorithmIdentifier for RSA keys is identical byte by by byte with the following hexadecimal encoded bytes: **300d06092a864886f70d0101010500**

7.1.3.1.2. ECDSA

ACCV indicates the ECDSA key using the algorithm identifier id-ecPublicKey (OID: 1.2.840.10045.2.1). The namedCurve encoding is used for the parameters.

For P-256 keys, the namedCurve MUST be secp256r1 (OID: 1.2.840.10045.3.1.7).
For P-384 keys, the namedCurve MUST be secp384r1 (OID: 1.3.132.0.34).
For P-521 keys, the namedCurve MUST be secp521r1 (OID: 1.3.132.0.35).

When encrypted, the AlgorithmIdentifier for ECDSA keys is identical byte-for-byte with the following bytes hexadecimally encoded:

For P-256 keys, **301306072a8648ce3d020106082a8648ce3d030107**.
For P-384 keys, **301006072a8648ce3d02010606052b81040022**.
For P-521 keys, **301006072a8648ce3d02010606052b81040023**.

7.1.3.2. Signature algorithm identifier

All objects signed by ACCV meet these requirements on the use of the AlgorithmIdentifier or AlgorithmIdentifier-derived type in the context of signatures.

In particular, it applies to all of the following objects and fields:

- The signatureAlgorithm field of a certificate or pre-certificate.
- The signatureAlgorithm field of a TBSCertificate (e.g., the one used by a certificate or pre-certificate).
- The signatureAlgorithm field of a CertificateList.
- The signature field of a TBSCertList
- The signatureAlgorithm field of a BasicOCSPResponse.

No other coding is allowed for these fields.

7.1.3.2.1. RSA

ACCV uses one of the following algorithms and signature encodings. When encoded, the AlgorithmIdentifier MUST be identical byte-for-byte with the specified hexadecimal encoded bytes.

RSASSA-PKCS1-v1_5 with SHA-256:

Codificación: **300d06092a864886f70d01010b0500**.

RSASSA-PKCS1-v1_5 with SHA-384:

Codificación: **300d06092a864886f70d01010c0500**.

RSASSA-PKCS1-v1_5 with SHA-512:

Codificación: **300d06092a864886f70d01010d0500**.

RSASSA-PSS with SHA-256, MGF-1 with SHA-256 and a salt length of 32 bytes:

Encoding:

304106092a864886f70d01010a3034a00f300d06096086480165030402010500a11c301a06092a864886f70d010108300d06096086480165030402010500a203020120

RSASSA-PSS with SHA-384, MGF-1 with SHA-384 and a salt length of 48 bytes:

Encoding:

304106092a864886f70d01010a3034a00f300d06096086480165030402020500a11c301a06092a864886f70d010108300d06096086480165030402020500a203020130

RSASSA-PSS with SHA-512, MGF-1 with SHA-512 and a salt length of 64 bytes:

Encoding:

304106092a864886f70d01010a3034a00f300d06096086480165030402030500a11c301a06092a864886f70d010108300d06096086480165030402030500a203020140

7.1.3.2.2. ECDSA

ACCV uses the appropriate signature algorithm and encryption depending on the signing key used.

If the signing key is P-256, the signature MUST use ECDSA with SHA-256. When encrypted, the AlgorithmIdentifier MUST be identical byte-for-byte with the following hexadecimal encoded bytes: **300a06082a8648ce3d040302**.

If the signing key is P-384, the signature MUST use ECDSA with SHA-384. When encrypted, the AlgorithmIdentifier MUST be identical byte-for-byte with the following bytes hexadecimally encoded: **300a06082a8648ce3d040303**.

If the signing key is P-521, the signature MUST use ECDSA with SHA-512. When encrypted, the AlgorithmIdentifier MUST be identical byte-for-byte with the following hexadecimal encoded bytes: **300a06082a8648ce3d040304**.

7.1.4. Name Forms

The subject and sender names for all possible certification chains are identical byte by byte.

Certificates issued by ACCV contain the distinguished name X.500 of the issuer and the subscriber of the certificate in the issuer name and subject name fields respectively.

In the case of ACCVRAIZ1 RootCA or SubCAs

Issuer's name: cn=ACCVRAIZ1, ou=PKIACCV o=ACCV, c=ES

- Subject:
  - commonName (required). Must match the name of ACCV entity.
  - OrganizationalUnit (required) fixed string "PKIACCV".
  - Organization (required) fixed string "ACCV".
  - Country (required) Country code ISO 3166-1

In the case of ACCV ROOT RSA TLS 2024 RootCA and its SubCAs

Issuer Name: CN=ACCV ROOT RSA TLS 2024, organizationIdentifier=VATES-A40573396, O=ISTEC, L=BURJASSOT, ST=VALENCIA, C=EN

- Subject:
  - commonName (required). Must match the name of ACCV entity.
  - organizationIdentifier (required) fixed string **VATES-A40573396**
  - Organization (mandatory) **ISTEC** fixed chain
  - Locality (required): fixed chain **BURJASSOT**
  - State (required): fixed chain **VALENCIA**
  - Country (required) country code ISO 3166-1 **EN**

For ACCV ROOT ECC TLS 2024 RootCA and its SubCAs

Issuer Name: CN=ACCV ROOT ECC TLS 2024, organizationIdentifier=VATES-A40573396, O=ISTEC, L=BURJASSOT, ST=VALENCIA, C=ES

- Subject:
  - commonName (required). Must match the name of ACCV entity.
  - organizationIdentifier (required) fixed string **VATES-A40573396**
  - Organization (mandatory) **ISTEC** fixed chain
  - Locality (required): fixed chain **BURJASSOT**
  - State (required): fixed chain **VALENCIA**
  - Country (required) country code ISO 3166-1 **EN**

The Issuer names supported for end-entity certificates issued under this CPD are:

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

cn=ACCV RSA1 TLS,2.5.4.97=VATES-A40573396,o=ISTEC,l=BURJASSOT,s=VALENCIA,c=ES

cn=ACCV ECC1 TLS,2.5.4.97=VATES-A40573396,o=ISTEC,l=BURJASSOT,s=VALENCIA,c=ES

All the fields of the final entity certificate of the Subject and Subject Alternative Name, except those referring to DNS name or mailing addresses, must be completed in capital letters, without accents.

The subjectAlternativeName (SAN) field contains at least one entry. Each entry in the SAN field must be of type dNSName containing the full qualified name of a system.

Subject:

commonName (optional). If included, it must match one of the DNSName fields in the SAN.

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

OrganizationIdentifier (required) Entity identifier, following the format defined in the European standard ETSI EN 319 412-1.

Organization (required) Designation (official name) of the Administration, agency or entity on behalf of which the certificate subscriber and domain owner is acting.

locality (required) City

state (required) State or province

country (required) ISO 3166-1 country code

7.1.4.1. Name Encoding

Rules applied when coding a Name:

- Each Name contains one RDNSequence.
- Each RelativeDistinguishedName contains exactly one AttributeTypeAndValue.
- Each RelativeDistinguishedName, if present, is encoded within RDNSequence in the order in which it appears in Section 7.1.2. of the Certification Policy.
- Each Name contains no more than one instance of a given AttributeTypeAndValue in all RelativeDistinguishedNames.

7.1.5. Name Constraints

The names contained in the certificates are restricted to X.500 distinguished names (DN), distinguishable by subscriber and unambiguous.

There are no name restrictions defined in the SubCA certificates.

There are no restrictions defined by extension for certificates issued under this policy.

7.1.6. Certification Policy Object Identifier (OID)

ACCV has defined a policy for assigning OID's within its private numbering arc. The OID of all ACCV Certification Policies start with the prefix 1.3.6.1.1.4.1.8149.3.

For the root CA and intermediate Cas the policy is *anyPolicy* (2.5.29.32.0).

7.1.6.1. Qualified Website Authentication Certificates

The object identifier defined by ACCV to identify this policy is as follows:

1.3.6.1.4.1.8149.3.3.5.0

In this case an OID is added to identify the type of entity being represented according to ETSI EN 319 411-2.

0.4.0.194112.1.5 Certification policy for EU-qualified certificates issued to websites

In this case an OID is added to identify the type of entity being 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 to identify the type of entity being represented according to ETSI EN 319 411-1.

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

7.1.6.2. Electronic Administrative Headquarters Certificates in Hardware Secure Module

The object identifier defined by ACCV to identify this policy is as follows:

1.3.6.1.4.1.8149.3.14.6.0

In this case an OID is added to identify the type of entity that is represented according to the definition of the profiles by the General State Administration.

2.16.724.1.3.5.5.1 **High level Electronic Administrative Headquarters Certificates**

In this case an OID is added to identify the type of entity being represented according to ETSI EN 319 411-2.

0.4.0.194112.1.5 **Certification policy for EU-qualified certificates issued to websites**

In this case, an OID is added to identify the type of entity being represented according to 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 to identify the type of entity being represented according to the ETSI EN 319 411-1 standard.

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

7.1.6.3. Electronic Administrative Headquarters Certificates based on software

The object identifier defined by ACCV to identify this policy is as follows:

1.3.6.1.4.1.8149.3.15.6.0

In this case an OID is added to identify the type of entity that is represented according to the definition of the profiles by the General State Administration.

2.16.724.1.3.5.5.2 **Medium/substantial Electronic Administrative Headquarters Certificates**

In this case an OID is added to identify the type of entity being represented according to ETSI EN 319 411-2.

0.4.0.194112.1.5 **Certification policy for EU-qualified certificates issued to websites**

In this case, an OID is added to identify the type of entity being represented according to 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 to identify the type of entity being represented according to the ETSI EN 319 411-1 standard.

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

7.1.6.4. Server Authentication Certificates

The object identifier defined by ACCV to identify this policy is as follows:

1.3.6.1.4.1.8149.3.36.2.0

In this case an OID is added to identify the type of entity being 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**

7.1.7. Usage of Policy Constraints Extension

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

7.1.8. Policy Qualifiers Syntax and Semantics

The "Certificate Policy" extension can include a Policy Qualifier (optional):

- CPS Pointer: contains the URL where the Certification Policies are published.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

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

7.1.10. Signed Certificate Timestamp (SCT) List

Responses from well-known qualified registries, currently compliant with Chrome's certificate transparency policy.

OID extension: 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 is based on the lifetime of the certificate:

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 is based on the lifetime of the certificate:

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

The format of the CRLs used in this policy is as specified in version 2 (X509 v2).

The serial number of revoked certificates remains in the CRL until they expire.

7.2.2. CRL and extensions

This Certification Practice Statement supports and uses CRLs that comply with the X.509 standard and support the following fields:

Version: Set as v2

Signature Algorithm: Identifier of the algorithm used to sign the CRL.

Hash Algorithm: Identifier of the algorithm used to hash the CRL.

Issuer: The distinguished name of the issuing CA

This update: Time of CRL issuance

Next Update: Time of the next CRL update

CRL Number: Sequential CRL number

Issuer Key Identifier: Fingerprint of the CA issuer

Revoked Certificates: List of revoked certificates.

reasonCode (OID 2.5.29.21)

If present, this extension is not marked as critical.

If a CRL entry is for a root CA or subordinate CA certificate, this CRL entry extension is present. For subscriber certificates, their CRL entry extension is omitted when the CRLReason specified is not specified (0).

ACCV will make every effort to have the CRLReason indicate the most appropriate reason for revocation of the Certificate.

Only the following CRLReason can be present in the CRL reasonCode extension for subscriber certificates:

- keyCompromise (RFC 5280 CLR Reason #1): Indicates that it is known or suspected that the subscriber's private key has been compromised.
- affiliationChanged: (RFC 5280 CRL Reason #3): Indicates that the subject name or other subject identity information in the certificate has changed, but there is no reason to suspect that the certificate's private key has been compromised.

- superseded (RFC 5280 CRL Reason #4): Indicates that the Certificate is being replaced because: the Subscriber has requested a new Certificate.
- cessationOfOperation: (RFC 5280 CRL Reason #5): Indicates that the website with the Certificate is closed before the expiration of the Certificate, or if the Subscriber no longer owns or controls the Domain Name in the Certificate before the expiration of the Certificate.
- privilegeWithdrawn: (RFC 5280 CRL Reason #9): indicates that there has been a breach by the Subscriber that has not resulted in a Key Commitment, such as that the Certificate Subscriber provided misleading information in its Certificate Application or has failed to comply with its material obligations under the Subscriber Agreement. o Terms of Use.

ACCV will inform Subscribers of the revocation reason options listed above and provides an explanation of when to choose each option. The tools ACCV makes available to the Subscriber allow these options to be easily specified when the Subscriber requests revocation of their Certificate, with the default being that the reason for revocation is not indicated.

privilegeWithdrawn reason code is not available to the subscriber as a revocation reason option, because the use of this reason code is determined by the CA and not the subscriber.

7.3. OCSP Profile

ACCV also publishes certificate status information via the Online Certificate Status Protocol (OCSP). This OCSP service operates according to the standard defined in RFC 6960 and RFC 5019.

Specifically, it is guaranteed that if the OCSP responder receives a status request for a certificate that has not been issued, it will not respond with a "good" status. The response must be "revoked", with specification of the revocation reason certificateHold (6), and must specify the revocationTime January 1, 1970.

If the OCSP response is based on an OCSP input the code of the response revocation reason will be the same as the one obtained from the CRL.

ACCV provides its OCSP service at http://ocsp.accv.es, on a 24x7 basis.

7.3.1. Version number

The OCSP service operates according to the standard defined in RFC-6960 and RFC-5019. The certificates used in the service conform to the X509 version 3 standard.

7.3.2. OCSP extensions

The OCSP service provided by ACCV supports at least the following extensions:

- NONCE (optional)

- Archive Cutoff

- Extended Revoked Definition

The individual ACCV OCSP Response Extensions do not contain the ReasonCode extension (OID 2.5.29.21) of the CRL entries.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

ACCV carries out the necessary checks to ensure that

- Issues certificates and operates the services in accordance with all the legislation applicable to its activity

- Meets the established technical requirements

- Complies with the audit requirements set forth in this section.

8.1. Frequency or Circumstances of Assessment

A fully audit shall be carried out on ACCV at least once a year to guarantee the compliance of its running and operating procedures with the provisions included in this CPS.

Certificates capable of issuing new certificates and all their operations fall within the scope of the audit, these operations are divided into an unbroken sequence of audit periods. An audit period must not exceed one year in duration.

Other technical and security audits shall be carried out in accordance with the stipulations of ACCV's Audit Policy, which include an audit on compliance with personal data protection legislation

If ACCV does not have a valid Audit Report indicating compliance with one of the audit schemes listed in Section 8.4, then, before issuing Publicly-Trusted Certificates, we will successfully complete a point-in-time readiness assessment performed in accordance with applicable standards under one of the audit schemes listed in Section 8.4. The point-in-time readiness assessment will be completed no earlier than twelve (12) months prior to issuing Publicly-Trusted Certificates and will be followed by a complete audit under such scheme within ninety (90) days of issuing the first Publicly-Trusted Certificate.

8.2. Identity/Qualifications of Assessor

The auditor will be selected at the time of each audit.

The audit of the CA shall be performed by a Qualified Auditor. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills:

- Independence of the object of the audit;
- The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme (see Section 8.4);
- Employ individuals who are proficient in the examination of public key infrastructure technology, information security tools and techniques, information technology and security auditing, and the third party attestation function;
- For audits performed in accordance with the WebTrust standard: licensed by WebTrust;
- Required by law, government regulation or professional code of ethics; and
- Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage

8.3. Assessor's Relationship to Assessed Entity

Apart from the audit function, the auditor and the audited party (ACCV) shall not have any current or planned financial, legal or any other type of relationship that could lead to a conflict of interest.

In compliance with the provisions of the regulations in force in our legislation on the protection of personal data, and given that for the fulfillment, by the auditor, of the services regulated in the contract it will be necessary to access the personal data of the files owned by ACCV, the auditor will be considered a Data Processor, pursuant to the provisions of Article 4.8 of Regulation (EU) 2016/679 of 27 April 2016.

8.4. Topics Covered by Assessment

The audit shall determine the compliance of ACCV services with this CPS and the applicable CPs. It shall also determine the risks of non-fulfillment of compliance with the operating procedures defined by these documents.

The aspects covered by an audit shall include, but shall not be limited to:

- Security policy

- Physical security

- Technological evaluation

- Administration of the CA’s services

- Selection of personnel

- CPS and CPs in force

- Contracts

- Privacy policy

ACCV carries out at least one annual audit under these schemes:

- “WebTrust for CAs v2.1 or newer” and “WebTrust for CAs SSL Baseline with Network Security v2.3 or newer”.
- Regulation (EU) No. 910/2014 of the European Parliament and of the Council of July 23, 2014 (eIDAS) and Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024

In addition to the necessary audits established by the legislation in force and by the technical norms of application for the fulfillment of its functions.

ACCV incorporate periodic monitoring and/or accountability procedures to ensure that its audits continue to be conducted in accordance with the requirements of the scheme.

Audits will be conducted by a Qualified Auditor, as specified in 8.2.

8.5. Actions Taken as a Result of Deficiency

The identification of deficiencies in the audit will result in corrective actions being taken. ACCV, in collaboration with the Auditor, will be responsible for determining these corrective actions.

In case of serious deficiencies, ISTEC may decide to temporarily suspend operations until the deficiencies are remedied, revoke the entity's certificate, change personnel, etc.

8.6. Communication of Results

The auditor shall notify the results of the audit to ACCV Security Manager, and the managers of the various areas in which non-conformance is detected. The Audit Report shall state explicitly that it covers the relevant systems and processes used in the issuance of all Certificates that assert one or more of the policy identifiers listed in Section 7.1.6.1.

The Audit Report must contain at least the following clearly-labelled information:

- name of the organization being audited;
- name and address of the organization performing the audit;
- the SHA-256 fingerprint of all Roots and Subordinate CA Certificates, including Cross Certificates, that were in-scope of the audit;

- audit criteria, with version number(s), that were used to audit each of the certificates (and associated keys);
- a list of the CA policy documents, with version numbers, referenced during the audit;
- whether the audit assessed a period of time or a point in time;
- the start date and end date of the Audit Period, for those that cover a period of time;
- the point in time date, for those that are for a point in time;
- the date the report was issued, which will necessarily be after the end date or point in time date.

An authoritative English language version of the publicly available audit information must be provided by the Qualified Auditor and ACCV will keep public and accessible audit reports, ensuring that no more than three months will pass from the end of the previous audit period.

The Audit Report must be available as a PDF, and shall be text searchable for all information required. Each SHA-256 fingerprint within the Audit Report must be uppercase letters and must not contain colons, spaces, or line feeds.

8.7. Self-Audits

ACCV constantly monitors compliance with procedures and policies, establishing periodic controls of relevant indicators and performing self-audits. In the case of non-personal website and electronic headquarters certificates, at least quarterly on a randomly selected sample of three percent of the Certificates issued during the period immediately following the previous self-audit sample. In this quarterly analysis, ACCV uses linting tools to verify the technical accuracy of the certificates issued regardless of the reviews carried out in the issuance process.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. Fees

9.1.1. Certificate Issuance or Renewal Fees

The prices for the initial issuance and renewal of the certificates referred to in this CPS are included in the Price List of ACCV. This list is published on ACCV website www.accv.es

9.1.2. Certificate Access Fees

Access to the certificates issued, given their public nature, is free and free of charge and therefore there is no fee applied to them.

9.1.3. Revocation or Status Information Access Fees

Access to certificate status or revocation information is free of charge and therefore no fees will be charged.

9.1.4. Fees for Other Services

No fee shall be applied for the service of providing information on this CPS.

9.1.5. Refund Policy

No refunds will be made for amounts paid for this type of certificate.

9.2. Financial Responsibility

9.2.1. Insurance Coverage

ACCV offers a guarantee of sufficient coverage of civil liability as a public body and responsible as such for damages, as established in article 9, paragraph 3, subsection b) of Law 6/2020, of November 11, which regulates certain aspects of electronic trust services, which covers the risk of liability for damages that may be caused by the use of certificates issued by this Certification Authority.

9.2.2. Other assets

There are no other assets to consider.

9.2.3. Insurance or Warranty Coverage for end-entities

There are no additional insurances or coverages beyond those covered by the liability insurance defined in section .9.2.1

9.3. Confidentiality of Business Information

9.3.1. Scope of Confidential Information.

It is expressly declared as confidential information, which may not be disclosed to third parties, except in those cases provided by law:

- The private keys of the entities that make up ACCV.
- All information related to the operations carried out by ACCV.

- All information related to security parameters, control and audit procedures.
- All personal information provided to ACCV during the registration process of certificate subscribers, except as specified by the applicable Certification Policy and the certification contract.
- Business information provided by its suppliers and other persons with whom ACCV has a legal or contractual duty of confidentiality.
- Business continuity and emergency plans.
- Transaction records, including complete records and audit trails of transactions.
- All information classified as "CONFIDENTIAL" or "STRICTLY CONFIDENTIAL".

9.3.2. Information Not Within the Scope of Confidential Information

ACCV shall consider the following information to be for public access:

1. Information contained in the Certification Practice Statement approved by ACCV.
2. Information contained in the different Certification Policies approved by ACCV.
3. Issued certificates as well as the information contained in these.
4. Certificate Revocation List (CRL)
5. Any information qualified as "PUBLIC".

ACCV's CPS and CPs shall not include information qualified as confidential in point 9.3.1 of this document.

Information that is not considered as confidential access is permitted, without prejudice to the right of ACCV to establish the relevant security controls for the purpose of protecting the authenticity and integrity of documents that store information for public access, and thereby preventing unauthorized persons from being able to add to, modify or delete contents.

9.3.3. Responsibility to Protect Confidential Information

ACCV is responsible for the protection of confidential information generated or communicated during all operations.

In the case of end entities, certificate subscribers are responsible for protecting their own private key and all activation information required to access or use the private key.

ACCV shall have the right to disclose confidential information to the extent required by law. In particular, records certifying the reliability of the information included in the certificate will be disclosed if required as evidence in legal proceedings. In such cases, the consent of the certificate subscriber is not required.

Certificate revocation information is provided by the CRL on the web server that acts as ACCV repository.

This information is also available on ACCV OCSP validation server at ocsp.accv.es:80.

9.4. Privacy of Personal Information

ACCV has a Privacy Policy, published on the website of the entity, through which it complies with the provisions established in the legislation on protection of personal data in force and which informs about the policy of protection of personal data of ACCV.

9.4.1. Privacy Plan

In compliance with the requirements stipulated in each of the Certification Policies and according with Article 5 of Regulation (EU) 910/2014 (eIDAS), any information of a personal nature provided to ACCV by the subscribers of its certificates shall be handled in accordance with the terms of “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data” and “Organic Law 3/2018 of 5 December on the Protection of Personal Data and the Guarantee of Digital Rights”.

In this sense, ACCV appears before the Spanish Data Protection Agency as responsible for the mixed file "*Electronic Signature Users*" and its processing. This file was created and its attributes modified by means of the following regulations:

- Order of March 8, 2002, of the Regional Ministry of Innovation and Competitiveness, by which computerized files with personal data are created (vid. DOGV nº 4.221 of April 4, 2002 and correction of errors in the DOGV nº 4.304, of July 31, 2002).
- Order of May 26, 2004, of the Regional Ministry of Infrastructures and Transport, by which personal data files are created, modified and cancelled (DOGV 4.772, of June 10, 2004).
- Decree 149/2007, of September 7, 2007, of the Consell, which approves the Statute of Ente Prestador de Servicios de Certificación Electrónica de la Comunitat Valenciana (DOGV 5.596, of September 11, 2007).
- Law 5/2013, of December 23, 2013, on Fiscal Measures, Administrative and Financial Management, and Organization of the Generalitat (DOCV 7.181 of December 27, 2013).
- Decree 15/2014, of January 24, of the Consell, approving the Regulations of Organization and Operation of the Institut Valencià de Finances (IVF) (DOCV 7.202 of January 29, 2014).
- Law 21/2017, of December 28, on Fiscal Measures, Administrative and Financial Management, and Organization of the Generalitat (DOCV 8.202 of December 30, 2017).
- Law 27/2018, of December 27, on Fiscal Measures, Administrative and Financial Management, and Organization of the Generalitat (DOCV 8.453 of December 28, 2018).

In this file are recorded mainly those identification data (name, surname, ID card or equivalent) and contact (postal address, email,) necessary for the provision of digital certification services that ACCV offers to individuals and legal entities. Data legally considered as BASIC LEVEL due to its characteristics.

Additionally, in accordance with the obligations established by Regulation (EU) 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), ACCV has a public Register of Activities describing the technical and organizational measures carried out by the entity itself with the intention of protecting the personal data transferred in the performance of its functions.

9.4.2. Information Treated as Private

In accordance with the stipulations of Article 4.1 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, any information relating to identified or identifiable individuals is considered to be personal data.

Personal information that must not be included either on certificates or on the certificate status verification system is considered to be personal information of a private nature.

In any case, the following data is considered to be private information:

1. Certificate requests, whether approved or refused, and any other personal information obtained for the issue and maintenance of certificates if the information is not included in the Certificate and if the information is not public information.
2. Private keys generated and/or stored by ACCV.
3. Any other information identified as “Private information”

In addition, data received by the Certification Services Provider has the legal consideration of basic level data.

Pursuant to Regulation (EU) 2016/679 of 27 April 2016, confidential information is protected from loss, destruction, damage, falsification and illegal or unauthorized processing (article 5.1.f)

In no case ACCV includes data referred in article 9 of Regulation (EU) 2016/679 of 27 April 2016, in the digital certificates issued.

9.4.3. Information not Deemed Private

This information refers to the personal information included in the certificates and in the referred mechanism for checking the status of the certificates, in accordance with section 3.1 of this document.

The information is not private by law ("public data"), but is only published in the repository with the consent of the subscriber.

In any case, the following information is considered non-confidential:

a. Certificates issued or in the process of issuance.

b. The subscriber's attachment to a certificate issued by ACCV.

c. The name and surname of the subscriber of the certificate, as well as any other circumstances or personal data of the holder, in the event that they are significant according to the purpose of the certificate, in accordance with this document.

d. The e-mail address of the certificate subscriber.

e. The uses and economic limits outlined in the certificate.

f. The period of validity of the certificate, as well as the date of issuance of the certificate and the expiration date.

g. The serial number of the certificate.

h. The different statuses or situations of the certificate and the date of the beginning of each of them, specifically: pending generation and/or delivery, valid, revoked, suspended or expired and the reason that caused the change of status.

i. The certificate revocation lists (CRLs), as well as all other revocation status information.

j. The information contained in ACCV Repository.

9.4.4. Responsibility to Protect Private Information

ACCV guarantees compliance with its legal obligations as a certification service provider, in accordance with Regulation (EU) 910/2014 (eIDAS) and its amendment in Regulation (EU) 2024/1183, and by virtue of this, and in accordance with Article 24 of the aforementioned Regulation, it shall be liable for any damages caused in the development of its own activity, for failure to comply with the requirements contained in Article 8 of Law 6/2020, of November 11, regarding the protection of personal data.

9.4.5. Notice and Consent to Use Private Information

For the provision of the service, ACCV will have to obtain the consent of the holders of the data necessary to provide certification services. Consent will be understood to have been obtained with the signing of the certification contract and the collection of the certificates by the user.

ACCV will only use private information after obtaining consent or as required by applicable laws or regulations.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

ACCV may only communicate information classified as confidential or containing personal data in those cases in which it is required to do so by the competent public authority and in the cases provided for by law.

Specifically, ACCV is obliged to disclose the identity of the signatories when requested to do so by the judicial authorities in the exercise of the functions attributed to them, and in all other cases provided for in Article 52 of Organic Law 3/2018, of December 5, on the Protection of Personal Data and Guarantee of Digital Rights, in which this communication is required.

9.4.7. Other Information Disclosure Circumstances

ACCV includes, in the privacy policy provided at the beginning of section 9.4, prescriptions to allow the disclosure of key holder information directly to key holders or authorized third parties.

9.5. Intellectual Property Rights

All intellectual property rights, including those concerning certificates and CRLs issued by ACCV, OIDs and any other document not explicitly mentioned, whether electronic or otherwise, owned by ACCV, belong to ACCV.

The CPS and Certification Policies are issued by ACCV, and are licensed under a Creative Commons Attribution-NoDerivatives 4.0 (CC BY-ND 4.0) license.

Private keys and public keys are the property of the subscriber, regardless of the physical medium used to store them.

The subscriber shall retain any rights it may have in the product trademark or trade name registered on the certificate.

9.6. Representations and Warranties

9.6.1. CA Representations and Warranties

ACCV is obliged to:

- Conduct its operations in accordance with this CPS.
- Protect your private keys.
- Issue certificates in accordance with the applicable Certification Policies.
- Upon receipt of a valid certificate request, issue certificates compliant with the X.509 standard and the requirements of the request.
- Issue certificates that are in accordance with the information known at the time of issuance, and free of data entry errors.
- Ensure confidentiality in the signature creation data generation process and its delivery by a secure procedure to the signatory.
- Use reliable systems and products that are protected against tampering and that guarantee the technical and cryptographic security of the certification processes they support.
- Use reliable systems for storing qualified certificates that make it possible to verify their authenticity and prevent unauthorized persons from altering the data, restrict their accessibility in the cases or to the persons indicated by the signatory, and make it possible to detect any change that affects these security conditions.
- Ensure that the date and time at which a certificate was issued, terminated or suspended can be accurately determined.
- Employ personnel with the necessary qualifications, knowledge and experience to provide the certification services offered and the appropriate security and management procedures in the field of electronic signatures.
- Revoke the certificates under the terms of the *Certificate Suspension and Revocation* section of this document and publish the revoked certificates in the CRL of ACCV repository (www.accv.es), with the frequency stipulated in the *Frequency of issuance of CRLs* section of this document.

- Publish this CPS and applicable CPs on the website www.accv.es, ensuring access to current as well as previous versions.

- Promptly notify, by e-mail, certificate subscribers in the event that the CA revokes the certificate and the reason for such revocation.

- Collaborate with the audits conducted by ACCV to validate the renewal of their own keys.

- Operate in accordance with applicable legislation. Specifically with:

  .1.1. Decree 220/2014, of December 12, of the Valencian Government, regulating the use of the advanced electronic signature in the Generalitat Valenciana.

  .1.2. Law 6/2020, of November 11, regulating certain aspects of electronic trust services.

  .1.3. Regulation (EU) number 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and its amendment in Regulation (EU) 2024/1183.

  .1.4. Law 39/2015, of October 1, on the Common Administrative Procedure of Public Administrations.

  .1.5. Decree 15/2014, of January 24, of the Consell, approving the Regulations on the Organization and Operation of the Institut Valencià de Finances (IVF).

  .1.6. Law 21/2017, of December 28, 2017 Generalitat Valenciana, approving the integration into the Generalitat Valenciana of the functions and competences in the field of certification and electronic signature developed by the Institut Valencià de Finances (IVF).

  .1.7. Law 27/2018 of December 27, 2018 of the Generalitat Valenciana, approving the creation of the new organization, ISTEC.

  .1.8. Order ETD/465/2021, of May 6, regulating remote video identification methods for issuing qualified electronic certificates.

  .1.9. Order ETD/743/2022, of July 26, amending Order ETD/465/2021, of May 6, regulating remote video identification methods for the issuance of qualified electronic certificates.

  .1.10. Royal Decree 203/2021, of March 30, which approves the Regulations for the performance and operation of the public sector by electronic means.

- Protect, if any, the keys in your custody.

- Ensure the availability of CRLs in accordance with the provisions of section 4.9.9 *Frequency of issuance of CRLs*, of this CPS.

- In the event of ceasing its activity, it must notify the holders of the certificates issued by ACCV, as well as the competent Ministry (at the date of writing this document it is the Ministry of Industry, Tourism and Trade), at least two months prior to the effective cessation, communicating the destination to be given to the certificates.

- Comply with the specifications contained in the regulations on Personal Data Protection.

- Keep on record all information and documentation relating to a qualified certificate and certification practice statements in effect at any given time for fifteen years from the time of issuance, so that signatures made with the certificate can be verified.

Root CAs shall be responsible for the performance and warranties of the Subordinate CAs, for the Subordinate CAs' compliance with these Requirements and for all liabilities and indemnification obligations of the Subordinate CAs under these Requirements, as if the Root CAs were the Subordinate CAs issuing the Certificates.

9.6.2. RA Representations and Warranties

Persons operating in the RAs integrated in ACCV hierarchy - User Registration Point operators - are obliged to:

- Conduct its operations in accordance with this CPS.
- Perform its operations in accordance with the Certification Policy applicable to the type of certificate requested on each occasion.
- Exhaustively verify the identity of the persons to whom the digital certificate processed by them is granted, for which they will require the presence of the applicant and the exhibition of the original and valid DNI, Spanish passport, or document admitted in law. In case of foreign users, they must show the document that identifies them and must be in possession of a Foreigner Identification Number (NIE) .
- Not to store or copy the signature creation data of the person to whom they have provided their services.
- Inform, prior to the issuance of a certificate, the person requesting its services, of the obligations it assumes, the way in which it must safeguard the signature creation data, the procedure to be followed to report the loss or misuse of the signature creation and verification data or devices, its price, the precise conditions for the use of the certificate, its limitations of use and the way in which it guarantees its possible financial liability, and the web page where it can consult any ACCV, CPS and CP information in force and previous, the applicable legislation, the applicable legislation, the possible financial liability, and the web page where it can consult any ACCV information, of its limitations of use and of the way in which it guarantees its possible patrimonial responsibility, and of the web page where you can consult any information of ACCV, the CPS and the current and previous CPs, the applicable legislation, the obtained certifications and the applicable procedures for the extrajudicial resolution of the conflicts that could arise by the exercise of the activity.
- Validate and securely send to the CA to which the RA is subordinated a certification request duly completed with the information provided by the subscriber and digitally signed, and receive the certificates issued in accordance with that request.
- Securely store both the documentation provided by the subscriber and that generated by the RA itself during the registration or revocation process, until the time of its submission to ACCV.
- Formalize the Certification Agreement with the subscriber as established by the applicable Certification Policy.
- Request the revocation of a certificate when it has knowledge or suspicion of the compromise of a private key.
- Authenticate end-user requests for renewal or revocation of their certificates, generate digitally signed renewal or revocation requests and send them to their superior CA.
- In the case of approval of a certification request notify the subscriber the issuance of their certificates and how to obtain it.
- In the case of rejection of an application for certification, notify the applicant of such rejection and the reason for it.
- Maintain under its strict control the digital certificate processing tools and notify ACCV of any malfunction or other eventuality that may deviate from the expected normal behavior.
- Send a signed copy of the certification contract and revocation requests to ACCV.

- Process revocation requests that it receives immediately, after having carried out a reliable identification.
- Collaborate in all aspects of the operation, audit or control of the User Registration Point as requested by ACCV.
- To the most general and broad obligation of confidentiality, during and after the provision of the service as Registration Authority, with respect to the information received by ACCV and with respect to the information and documentation in which the service has been provided. In the same sense, not to transmit such information to third parties, under any circumstances, without the express, written and prior authorization of ACCV, in which case the same obligation of confidentiality shall be transferred to such third parties.

9.6.3. Subscriber Representations and Warranties

It is the obligation of the subscribers of the certificates issued under this policy:

- Limit and adapt the use of the certificate to lawful purposes and in accordance with the uses permitted by the relevant Certification Policy and this CPS.
- Take the necessary care and means to ensure the safekeeping of your private key.
- Immediately request the revocation of a certificate in case of knowledge or suspicion of compromise of the private key corresponding to the public key contained in the certificate. The ways in which this request can be made are specified in this document in section 4.9.3 *Revocation request procedures*.
- Not to use a digital certificate that has lost its effectiveness, because it has been suspended, revoked or because the validity period of the certificate has expired.
- Provide the Registration Authorities with information that they consider accurate and complete in relation to the data requested by them in order to carry out the registration process, as well as inform ACCV managers of any modification to this information.
- Pay, if applicable, the fees accrued for the certification services requested.
- Certificates with the use of serverAuthentication key are subject to the CA/Browser Forum definition at https://cabforum.org/working-groups/server/baseline-requirements/documents/. Among the conditions established is the obligation to revoke the certificates if it is detected that the issuance or operation does not comply with the defined regulations. This revocation must be done within a maximum period of five (5) calendar days and no postponement of any kind is possible; if it is not possible to comply with this condition, certificates issued under this regulation must never be used.

ACCV requires, as part of the Subscriber Agreement or Terms of Use, that the Applicant accepts the commitments and warranties in this section for the benefit of the CA and the Certificate Beneficiaries.

Prior to the issuance of a Certificate, ACCV shall obtain, for the express benefit of the CA and the Beneficiaries of the Certificate, either:

- The Applicant's acceptance of the Subscriber Agreement with the CA, and
- The Applicant's acknowledgement of the Terms of Use.

ACCV shall implement a process to ensure that each Subscriber Agreement or Terms of Use is legally enforceable against the Applicant. In any case, the Agreement must apply to the Certificate to be issued pursuant to the certificate application. ACCV may use an electronic or "click-through" Agreement provided that the CA has determined that such agreements are legally enforceable. A separate Agreement shall be used for each certificate application.

9.6.4. Relying Party Representations and Warranties

It is the obligation of the parties to rely on the certificates issued by ACCV:

- Limit the reliability of certificates to the permitted uses of the same, in accordance with what is expressed in the certificate extensions and the relevant Certification Policy.
- Verify the validity of the certificates at the time of performing or verifying any operation based on them.
- Assume responsibility for the correct verification of digital signatures.
- To assume its responsibility in verifying the validity, revocation or suspension of the certificates it trusts.
- Be fully aware of the warranties and liabilities applicable to the acceptance and use of the certificates relied upon, and agree to be bound by them.
- In the case of qualified certificates, verify that the service identifier is included in the most recent version of the ***Trusted Service List*** published by the responsible body of the European Commission.

9.6.5. Representations and Warranties of other Participants

No warranties or representations to other participants are considered.

9.7. Disclaimer of Warranties

ACCV may refuse all service guarantees that are not linked to the obligations stipulated by Law 6/2020 of November 11, regulating certain aspects of electronic trust services, and Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, especially guarantees of fitness for a particular purpose or guarantees of the use of certificates for commercial purposes.

9.8. Limitations of Liability

ACCV shall be liable for any damages it causes to any person in the exercise of its activity, when it fails to comply with the obligations imposed by Law 6/2020, of November 11, regulating certain aspects of electronic trust services, Decree 220/2014, of December 12, of the Valencian Government, and Regulation (EU) number 910/2014 of the European Parliament and of the Council, concerning electronic identification and trust services for electronic transactions in the internal market, or acts negligently.

ACCV shall be liable for any damages caused to the Signatory or bona fide third parties due to the lack or delay in the inclusion in the certificate validity query service of the expiration or suspension of the validity of the certificate issued by ACCV, once it becomes aware of it.

ACCV assumes all liability to third parties for the performance of persons performing the functions necessary for the provision of the certification service.

ACCV is the Agencia de Tecnología y Certificación Electrónica, which is a Subdirectorate of Infraestructures I Serveis De Telecomunicacions I Certificacio SA, Public Law Entity. The liability of the Administration is based on objective grounds and covers any injury suffered by individuals as long as it is a consequence of the normal or abnormal operation of public services.

ACCV will only be liable for damages caused by the improper use of the website authentication certificate, when it has not consigned in it, in a manner clearly recognizable by third parties, the limit as to its possible use or the amount of the value of valid transactions that can be made using it, ACCV shall not be liable when the signatory exceeds the limits contained in the certificate as to its possible uses and the individualized amount of the transactions that can be carried out with it or does not use it in accordance with the conditions established and communicated to the signatory by ACCV. ACCV shall not be liable either if the recipient of the electronically signed documents does not check and take into account the restrictions contained in the certificate as to its possible uses and the individualized amount of the transactions that can be carried out with it.

ACCV Registration Entities do not assume any liability in case of loss or damage:

- Of the services they provide, in case of war, natural disasters or any other case of force majeure.
- Caused by the use of certificates that exceeds the limits established by them, the relevant Certification Policy and this CPS.
- Caused by the improper or fraudulent use of certificates or CRLs issued by ACCV.
- Caused to the signatory or bona fide third parties if the recipient of the electronically signed documents does not verify and take into account the restrictions in the certificate as to its possible uses, or when not taking into account the suspension or loss of validity of the certificate published in the CRL, or when not verifying the electronic signature.

Except as set forth in the provisions of this CPS, ACCV makes no other commitments or warranties and assumes no other liability to subscribers or relying parties.

9.9. Indemnities

ACCV is a governmental entity, so it is not applicable.

There are no additional insurances or coverages beyond those covered by the liability insurance defined in section .9.2.1

9.10. Term and Termination

9.10.1. Term.

ACCV establishes, in its legal instruments with subscribers and verifiers, a clause that determines the period of validity of the legal relationship by virtue of which they provide certificates to subscribers.

The CPS, the PDS and the various CPs become effective upon publication.

9.10.2. Termination.

ACCV establishes, in its legal instruments with subscribers and verifiers, a clause that determines the consequences of the termination of the legal relationship by virtue of which they supply certificates to subscribers.

This CPS, the PDS and the various CPS will be repealed when a new version of the document is published. The new version will replace the previous document in its entirety.

9.10.3. Effect of Termination and Survival.

ACCV establishes, in its legal instruments with subscribers and verifiers, survival clauses, by virtue of which certain rules remain in force after the termination of the legal relationship regulating the service between the parties.

For current certificates issued under a previous Certification Policy and Practices Statement, the new version shall prevail over the previous one in all that does not oppose it.

9.11. Individual Notices and Communications with Participants

Any notice, demand, request or any other communication required under the practices described in this CPS shall be made by means of a document or electronic message in accordance with this CPS or in writing by certified mail addressed to any of the addresses contained in point *1.5* of this document. Electronic communications shall become effective upon receipt by the addressee to whom they are addressed.

9.12. Amendments

ACCV may unilaterally modify this document, subject to the following procedure:

- The modification must be justified from a technical and legal point of view.
- The modification proposed by ACCV cannot violate the provisions contained in the certification policies established by ACCV.
- A change control is established, based on ACCV's Change Management Policy.
- The implications that the change of specifications has on the user are established, and the need to notify the user of such modifications is foreseen.

9.12.1. Procedure for Amendment

The entity with the authority to make and approve changes to the CPS and CPs is ISTEC (specifically Deputy Directorate for Digital Identity/ACCV), whose contact details can be found in section 1.5.1. of this CPS.

In those cases in which it is considered that the modification of the CPS does not materially reduce the confidence that a Certification Policy or its implementation provides, nor alters the acceptability of the certificates supported by the policy for the purposes for which they have been used, the minor version number of the document and the last Object Identifier (OID) number that represents it will be increased, maintaining the major version number of the document, as well as the rest of its associated OID. It is not considered necessary to communicate this type of modification to the subscribers of the certificates corresponding to the modified CP or CPS.

In the event that the changes to the current specification affect the acceptability of certificates for specific purposes, the highest version number of the document will be increased and the lowest version number will be reset to zero. The last two numbers of the Object Identifier (OID) that represents it will also be modified.

9.12.2. Notification Mechanism and Period

Any modification to this Certification Practices Statement or the Certification Policy Documents will be published on ACCV website www.accv.es serving as notification to subscribers, users or third parties.

9.12.3. Circumstances Under Which OID Must be Changed

ISTEC is the competent entity to approve this Certification Practices Statement, as well as the Certification Policies associated with each type of certificate.

Likewise, it is the responsibility of ISTEC to approve and authorize the modifications of such documents.

9.13. Dispute Resolution Provisions

ACCV may establish, through the legal instruments through which its relationship with subscribers and verifiers is articulated, the mediation, arbitration and conflict resolution procedures deemed appropriate, all without prejudice to administrative procedure legislation.

Disputes arising from the provision of certification services by ACCV shall be submitted to the contentious-administrative jurisdiction, in accordance with the provisions of Law 29/1998, of July 13, 1998, Regulating Contentious-Administrative Jurisdiction.

9.14. Governing Law

The functioning and operations of ACCV, as well as this CPS, are governed by the Community, State and Valencian legislation in force at any given time.

The following standards are explicitly assumed to apply:

1..1. Decree 220/2014 of December 12, 2014, of the Valencian Government, regulating the use of advanced electronic signatures in the Generalitat Valenciana.

1..2. Law 6/2020, of November 11, regulating certain aspects of electronic trust services.

1..3. Law 39/2015, of October 1, 2015, on the Common Administrative Procedure of Public Administrations.

1..4. Law 40/2015, of October 1, 2015, on the Legal Regime of the Public Sector.

1..5. Law 5/2013, of December 23, 2013, on Fiscal Measures, Administrative and Financial Management, and Organization of the Generalitat.

1..6. Law 21/2017, of December 28, 2017 Generalitat Valenciana, approving the integration into the Generalitat Valenciana of the functions and competences in the field of certification and electronic signature developed by the Institut Valencià de Finances (IVF).

1..7. Law 27/2018 of December 27, 2018 of the Generalitat Valenciana, approving the creation of the new body, ISTEC.

1..8. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

1..9. Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards the establishment of the European digital identity framework.

1..10. Order ETD/465/2021, of May 6, regulating remote video identification methods for issuing qualified electronic certificates.

1..11. Order ETD/743/2022, of July 26, amending Order ETD/465/2021, of May 6, regulating remote video identification methods for the issuance of qualified electronic certificates.

1..12. Royal Decree 203/2021, of March 30, which approves the Regulations for the performance and operation of the public sector by electronic means.

9.15. Compliance with Applicable Law

ACCV declares that this CPS complies with the legislation indicated in section 9.14

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

This CPS and all documents referred to herein constitute the entire agreement between the parties, superseding all other agreements that may exist with respect to the same subject matter.

All third parties relying on the certificates fully assume the contents of the latest version of this document, the PDS and the corresponding Policies.

9.16.2. Assignment

This CPS shall be binding on the successors, executors, heirs, representatives, administrators and assigns, express, tacit or apparent, of the parties.

The invalidity of one of the clauses contained in this CPS shall not affect the rest of the clauses. In such a case, said clause shall be deemed inapplicable.

9.16.3. Severability

In case of conflict of any part of this document with the current legislation of any jurisdiction in which a Certification Authority operates or issues certificates, after the corresponding legal review, ACCV may modify the conflicting points to the minimum extent necessary to comply with such legislation.

In such a case, (prior to issuing a certificate under the modified requirements) ACCV shall include in the subsections of this Section information on the Act requiring the modification and the specific change implemented by ACCV.

ACCV will also inform interested parties, such as the CAB Forum, of the newly added relevant information prior to issuing a certificate under the changes made.

9.16.4. Enforcement (Attorneys' Fees and Waiver of Rights)

ACCV may claim indemnification and attorneys' fees from a party for damages, losses and expenses related to such party's conduct. ACCV's failure to enforce a provision of this TOU does not waive ACCV's right to enforce the same provision later or the right to enforce any other provision of this TOU. To be effective, waivers must be in writing and signed by ACCV.

9.16.5. Force Majeure

ACCV will not accept any liability for failure or delay in the performance of any of the obligations contained in the CPS, if such failure or delay is the result of a force majeure event, unforeseeable circumstances or any circumstances over which no direct control can be exercised.

The operation of the Internet is beyond ACCV's reasonable control.

9.17. Other Provisions

In case of loss of QSCD certification of any of the qualified devices used by ACCV for end-entity certificates, ACCV will take the necessary measures to minimize the possible impact, informing the supervisory body and stopping the issuance of certificates on the affected devices.

10. Annex I

10.1. Qualified Website Authentication Certificates

CERTIFICATION CONTRACT - CODE 1.3.6.1.1.4.1.1.8149.3.3

Section 1 - Applicant Data
Last name:
Name:
Tax ID: Tel:
Position or position:
Administration-Organization:
CIF of the Organization:

E-mail address:

Mailing address:

Section 2 - Domain data
Qualified name:

Aliases:

Contact e-mail address:

Section 3 - *Date and Signature*

I sign this certification contract associated with the Certification Policy for Qualified Certificates for Website Authentication with code 1.3.6.1.1.4.1.8149.3.3, issued by Agencia de Tecnología y Certificación Electrónica. I declare to know and accept the rules of use of this type of certificates that are exposed in http://www.accv.es. I also declare that the information provided is true.

Applicant's signature

Firmat/Signed:

CERTIFICATION CONTRACT - CODE 1.3.6.1.4.1.8149.3.3

Conditions of use of certificates

1. The certificates associated with the Certification Policy of certificates for servers with SSL support, issued by Agencia de Tecnología y Certificación Electrónica are of type X.509v3 and are governed by the Certification Practices Statement of Agencia de Tecnología y Certificación Electrónica, as a Certification Service Provider, as well as by the Certification Policy referred to. Both documents must be interpreted according to the legislation of the European Community, the Spanish legal system and the legislation of the Generalitat Valenciana.

2. The applicant for the certificates must be a natural person, in possession of a qualified ACCV certificate or DNIe. The applicant must provide the data relating to their relationship with the Agency or Company on behalf of which they are requesting the certificate using the tools made available by ACCV.

3. The applicant of the certificates, specially authorized for the management of these by a given Organization or Company, is responsible for the veracity of the data provided at all times throughout the application and registration process. It will be responsible for communicating any variation of the data provided to obtain the certificate.

4. The certificate subscriber is responsible for the custody of his private key and for communicating as soon as possible any loss or theft of this key.

5. The certificate subscriber is responsible for limiting the use of the certificate to the provisions of the associated Certification Policy, which is a public document and is available at http://www.accv.es.

6. Agencia de Tecnología y Certificación Electrónica is not responsible for the operation of the computer servers that make use of the issued certificates.

7. The Agencia de Tecnología y Certificación Electrónica is responsible for compliance with the European, Spanish and Valencian legislation, as far as Electronic Signature is concerned. It is also responsible for compliance with the provisions of the Certification Practices Statement of the Agencia de Tecnología y Certificación Electrónica and the Certification Policy associated with this type of certificates.

8. The validity period of these certificates is a maximum of 12 months. For renewal, the same procedure must be followed as for the first application or the procedures set out in the associated Certification Policy.

9. The issued certificates will lose their effectiveness, in addition to the expiration of the validity period, when a revocation occurs, when the certificate support becomes unusable, when a judicial or administrative resolution ordering the loss of effectiveness is issued, for serious inaccuracies in the data provided by the applicant and by death of the subscriber of the certificate. Other conditions for the loss of effectiveness are included in the Certification Practices Statement and in the Certification Policy associated with this type of certificate.

10. The identification of the applicants will be based on their personal digital certificate issued by ACCV or their DNIe.

11. In compliance with the Organic Law 3/2018 of December 5, 2018, on the Protection of Personal Data, the applicant is informed of the existence of an automated file of personal data, created under the responsibility of Agencia de Tecnología y Certificación Electrónica. The purpose of this file is to serve the uses related to the certification services provided by Agencia de Tecnología y Certificación Electrónica. The subscriber expressly authorizes the use of his personal data contained in the file, to the extent necessary to carry out the actions set out in the Certification Policy.

12. Agencia de Tecnología y Certificación Electrónica undertakes to put the means at its disposal to prevent alteration, loss or unauthorized access to personal data contained in the file.

13. The applicant may exercise their rights of access, rectification or cancellation of their personal data by writing to Agencia de Tecnología y Certificación Electrónica, through any of the Entry Registries of the Generalitat Valenciana and clearly indicating this desire.

Revocation Reason

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 requesting a new certificate to replace an existing certificate.

cessationOfOperation

You SHOULD choose this revocation reason 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 of his certificate has been compromised. For example if an unauthorized person has gained access to the private key of his 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.

Certificates with serverAuthentication keyuse are subject to the CA/Browser Forum definition at https://cabforum.org/working-groups/server/baseline-requirements/documents/. Among the conditions established is the obligation to revoke the certificates if it is detected that the issuance or operation does not comply with the defined regulations. This revocation must be made within a maximum period of between one (1) and five (5) calendar days depending on the type of incident and no postponement of any kind is possible. If it is not possible to comply with this condition, certificates issued under this regulation should never be used.

By signing this document, the citizen authorizes ACCV to consult the identity data contained in the Ministry of Interior, avoiding the citizen to provide a photocopy of his identity document.

10.2. Electronic Administrative Headquarters Certificates in Hardware Secure Module

CERTIFICATION CONTRACT - CODE 1.3.6.1.1.4.1.8149.3.14

Section 1 - Applicant Data
Last name:
Name:
Tax ID: Tel:
Position or position:
Administration-Organization:
CIF of the Organization:

E-mail address:

Mailing address:

Section 2 - E-Office data
Qualified name:

Alias (if the certificate is not issued to the qualified name):

Descriptive name of the electronic site:

Contact e-mail address:

Section 3 - ***Date and Signature***

I sign this certification contract associated with the Certification Policy for Electronic Administrative Headquarters Certificates in Hardware Secure Module with code 1.3.6.1.1.4.1.8149.3.14, issued by Agencia de Tecnología y Certificación Electrónica. I declare to know and accept the rules for the use of this type of certificates that are exposed in http://www.accv.es. I also declare that the information provided is true.

Applicant's signature

Firmat/Signed:

CERTIFICATION CONTRACT - CODE 1.3.6.1.1.4.1.8149.3.14
Conditions of use of certificates

1. The certificates associated with the Certification Policy for Qualified Certificates of Administrative Electronic Headquarters in secure device, issued by ACCV are of type X.509v3 and are governed by the Certification Practices Statement of ACCV, as Certification Service Provider, as well as by the Certification Policy referred to. Both documents must be interpreted according to the legislation of the European Community, the Spanish legal system and the legislation of the Generalitat de Catalunya.

2. The applicant of the certificates must be a natural person, in possession of a recognized certificate of Agencia de Tecnología y Certificación Electrónica, and must be employed in a Public Administration, Instrumental Entity of the Administration or Corporate Entity.

3. The applicant of the certificates, specially authorized for the management of these by a specific Administration or Public Entity, is responsible for the veracity of the data provided at all times throughout the application and registration process. He/she will be responsible for communicating any variation of the data provided to obtain the certificate.

4. The certificate subscriber is responsible for the custody of his private key and for communicating as soon as possible any loss or theft of this key.

5. The certificate subscriber is responsible for limiting the use of the certificate to the provisions of the associated Certification Policy, which is a public document and is available at http://www.accv.es.

6. Agencia de Tecnología y Certificación Electrónica is not responsible for the content of the documents signed using the certificates issued by it.

7. Agencia de Tecnología y Certificación Electrónica is responsible for compliance with European, Spanish and Valencian legislation, as far as Electronic Signature is concerned. It is also responsible for compliance with the provisions of the Certification Practices Statement of ACCV and the Certification Policy associated with this type of certificates.

8. The validity period of these certificates is a maximum of 12 months. For renewal, the same procedure must be followed as for the first application or the procedures set out in the associated Certification Policy.

9. The issued certificates will lose their effectiveness, in addition to the expiration of the validity period, when a revocation occurs, when the certificate support becomes unusable, when a judicial or administrative resolution ordering the loss of effectiveness is issued, for serious inaccuracies in the data provided by the applicant and by death of the subscriber of the certificate. Other conditions for the loss of effectiveness are included in the Certification Practices Statement and in the Certification Policy associated with this type of certificate.

10. The documentation to be provided for the identification of the natural person requesting the certificate will be the National Identity Document, NIE or Passport valid and in force. The applicant must provide the data related to its relationship with the Public Administration, Instrumental Entity of the Administration or Corporate Entity of Public Law.

11. In compliance with the Organic Law 3/2018 of December 5, 2018, on the Protection of Personal Data, the applicant is informed of the existence of an automated personal data file, created under the responsibility of Agencia de Tecnología y Certificación Electrónica. The purpose of this file is to serve the uses related to the certification services provided by Agencia de Tecnología y Certificación Electrónica. The subscriber expressly authorizes the use of his personal data contained in the file, to the extent necessary to carry out the actions set out in the Certification Policy.

12. Agencia de Tecnología y Certificación Electrónica undertakes to put the means at its disposal to prevent alteration, loss or unauthorized access to personal data contained in the file.

13. The applicant may exercise their rights of access, rectification or cancellation of their personal data by writing to Agencia de Tecnología y Certificación Electrónica, through any of the Entry Registries of the Generalitat de Catalunya, clearly indicating this desire.

Revocation Reason

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 requesting a new certificate to replace an existing certificate.

cessationOfOperation

You SHOULD choose this revocation reason 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 of his certificate has been compromised. For example if an unauthorized person has gained access to the private key of his 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.

Certificates with serverAuthentication keyuse are subject to the CA/Browser Forum definition at https://cabforum.org/working-groups/server/baseline-requirements/documents/. Among the conditions established is the obligation to revoke the certificates if it is detected that the issuance or operation does not comply with the defined regulations. This revocation must be made within a maximum period of between one (1) and five (5) calendar days depending on the type of incident and no postponement of any kind is possible. If it is not possible to comply with this condition, certificates issued under this regulation should never be used.

By signing this document, the citizen authorizes ACCV to consult the identity data contained in the Ministry of Interior, avoiding the citizen to provide a photocopy of his identity document.

10.3. Electronic Administrative Headquarters Certificates based on software

CERTIFICATION CONTRACT - CODE 1.3.6.1.1.4.1.8149.3.15

Section 1 - Applicant Data
Last name:
Name:
Tax ID: Tel:
Position or position:
Administration-Organization:
CIF of the Organization:

E-mail address:

Mailing address:

Section 2 - E-Office data
Qualified name:

Alias (if the certificate is not issued to the qualified name):

Descriptive name of the electronic site:

Contact e-mail address:

Section 3 - *Date and Signature*

I sign this certification contract associated with the Certification Policy for Electronic Administrative Headquarters Certificates based on software with code 1.3.6.1.1.4.1.8149.3.15, issued by Agencia de Tecnología y Certificación Electrónica. I declare to know and accept the rules of use of this type of certificates that are exposed in http://www.accv.es. I also declare that the information provided is true.

Applicant's signature

Firmat/Signed:

CERTIFICATION CONTRACT - CODE 1.3.6.1.1.4.1.8149.3.15
Conditions of use of certificates

1. The certificates associated with the Certification Policy for Qualified Certificates of Administrative Electronic Headquarters in software support, issued by ACCV are of type X.509v3 and are governed by the Certification Practices Statement of ACCV, as Certification Service Provider, as well as by the Certification Policy referred to. Both documents must be interpreted according to the legislation of the European Community, the Spanish legal system and the legislation of the Generalitat de Catalunya.

2. The applicant of the certificates must be a natural person, in possession of a qualified certificate, and must be employed in a Public Administration, Instrumental Entity of the Administration or Corporate Entity.

3. The applicant of the certificates, specially authorized for the management of these by a specific Administration or Entity, is responsible for the veracity of the data provided at all times throughout the application and registration process. He/she will be responsible for communicating any variation of the data provided to obtain the certificate.

4. The certificate subscriber is responsible for the custody of his private key and for communicating as soon as possible any loss or theft of this key.

5. The certificate subscriber is responsible for limiting the use of the certificate to the provisions of the associated Certification Policy, which is a public document and is available at http://www.accv.es.

6. Agencia de Tecnología y Certificación Electrónica is not responsible for the content of the documents signed using the certificates issued by it.

7. Agencia de Tecnología y Certificación Electrónica is responsible for compliance with European, Spanish and Valencian legislation, as far as Electronic Signature is concerned. It is also responsible for compliance with the provisions of the Certification Practices Statement of ACCV and the Certification Policy associated with this type of certificates.

8. The validity period of these certificates is a maximum of 12 months. For renewal, the same procedure must be followed as for the first application or the procedures set out in the associated Certification Policy.

9. The issued certificates will lose their effectiveness, in addition to the expiration of the validity period, when a revocation occurs, when the certificate support becomes unusable, when a judicial or administrative resolution ordering the loss of effectiveness is issued, for serious inaccuracies in the data provided by the applicant and by death of the subscriber of the certificate. Other conditions for the loss of effectiveness are included in the Certification Practices Statement and in the Certification Policy associated with this type of certificate.

10. The documentation to be provided for the identification of the natural person requesting the certificate will be his or her personal qualified certificate before the registration authority. The applicant must provide the data related to its relationship with the Public Administration, Instrumental Entity of the Administration or Public Law Corporate Entity.

11. In compliance with the Organic Law 3/2018 of December 5, 2018, on the Protection of Personal Data, the applicant is informed of the existence of an automated file of personal data, created under the responsibility of Agencia de Tecnología y Certificación Electrónica. The purpose of this file is to serve the uses related to the certification services provided by Agencia de Tecnología y Certificación Electrónica. The subscriber expressly authorizes the use of his personal data contained in the file, to the extent necessary to carry out the actions set out in the Certification Policy.

12. Agencia de Tecnología y Certificación Electrónica undertakes to put the means at its disposal to prevent alteration, loss or unauthorized access to personal data contained in the file.

13. The applicant may exercise their rights of access, rectification, cancellation, portability, restriction of processing and objection to their personal data by writing to Agencia de Tecnología y Certificación Electrónica, through any of the Entry Registries of the Generalitat, clearly indicating this desire.

Revocation Reason

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 requesting a new certificate to replace an existing certificate.

cessationOfOperation

You SHOULD choose this revocation reason 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 of his certificate has been compromised. For example if an unauthorized person has gained access to the private key of his 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.

Certificates with serverAuthentication keyuse are subject to the CA/Browser Forum definition at https://cabforum.org/working-groups/server/baseline-requirements/documents/. Among the conditions established is the obligation to revoke the certificates if it is detected that the issuance or operation does not comply with the defined regulations. This revocation must be made within a maximum period of between one (1) and five (5) calendar days depending on the type of incident and no postponement of any kind is possible. If it is not possible to comply with this condition, certificates issued under this regulation should never be used.

By signing this document, the citizen authorizes ACCV to consult the identity data contained in the Ministry of Interior, avoiding the citizen to provide a photocopy of his identity document.

10.4. Server Authentication Certificates

CERTIFICATION CONTRACT - CODE 1.3.6.1.1.4.1.8149.3.36

Section 1 - Applicant Data
Last name:
Name:
Tax ID: Tel:
Position or position:
Administration-Organization:
CIF of the Organization:

E-mail address:

Mailing address:

Section 2 - Domain data
Qualified name:

Aliases:

Contact e-mail address:

Section 3 - *Date and Signature*

I sign this certification contract associated with the Certification Policy for Website Authentication Certificates with code 1.3.6.1.4.1.1.8149.3.36, issued by Agencia de Tecnología y Certificación Electrónica. I declare to know and accept the rules of use of this type of certificates that are exposed in http://www.accv.es. I also declare that the information provided is true.

Applicant's signature

Firmat/Signed:

CERTIFICATION CONTRACT - CODE 1.3.6.1.1.4.1.8149.3.36

Conditions of use of certificates

1. The certificates associated with the Certification Policy of certificates for servers with SSL support, issued by Agencia de Tecnología y Certificación Electrónica are of type X.509v3 and are governed by the Certification Practices Statement of Agencia de Tecnología y Certificación Electrónica, as a Certification Service Provider, as well as by the Certification Policy referred to. Both documents must be interpreted according to the legislation of the European Community, the Spanish legal system and the legislation of the Generalitat Valenciana.

2. The applicant for the certificates must be a natural person, in possession of a qualified ACCV certificate or DNIe. The applicant must provide the data relating to their relationship with the Agency or Company on behalf of which they are requesting the certificate using the tools made available by ACCV.

3. The applicant of the certificates, specially authorized for the management of these by a specific Organization or Company, is responsible for the veracity of the data provided at all times throughout the application and registration process. He/she will be responsible for communicating any variation of the data provided to obtain the certificate.

4. The certificate subscriber is responsible for the custody of his private key and for communicating as soon as possible any loss or theft of this key.

5. The certificate subscriber is responsible for limiting the use of the certificate to the provisions of the associated Certification Policy, which is a public document and is available at http://www.accv.es.

6. Agencia de Tecnología y Certificación Electrónica is not responsible for the operation of the computer servers that make use of the issued certificates.

7. The Agencia de Tecnología y Certificación Electrónica is responsible for compliance with the European, Spanish and Valencian legislation, as far as Electronic Signature is concerned. It is also responsible for compliance with the provisions of the Certification Practices Statement of the Agencia de Tecnología y Certificación Electrónica and the Certification Policy associated with this type of certificates.

8. The validity period of these certificates is a maximum of 12 months. For renewal, the same procedure must be followed as for the first application or the procedures set out in the associated Certification Policy.

9. The issued certificates will lose their effectiveness, in addition to the expiration of the validity period, when a revocation occurs, when the certificate support becomes unusable, when a judicial or administrative resolution ordering the loss of effectiveness is issued, for serious inaccuracies in the data provided by the applicant and by death of the subscriber of the certificate. Other conditions for the loss of effectiveness are included in the Certification Practices Statement and in the Certification Policy associated with this type of certificate.

10. The identification of the applicants will be based on their personal digital certificate issued by ACCV or their DNIe.

11. In compliance with the Organic Law 3/2018 of December 5, 2018, on the Protection of Personal Data, the applicant is informed of the existence of an automated personal data file, created under the responsibility of Agencia de Tecnología y Certificación Electrónica. The purpose of this file is to serve the uses related to the certification services provided by Agencia de Tecnología y Certificación Electrónica. The subscriber expressly authorizes the use of his personal data contained in the file, to the extent necessary to carry out the actions set out in the Certification Policy.

12. Agencia de Tecnología y Certificación Electrónica undertakes to put the means at its disposal to prevent alteration, loss or unauthorized access to personal data contained in the file.

13. The applicant may exercise their rights of access, rectification or cancellation of their personal data by writing to Agencia de Tecnología y Certificación Electrónica, through any of the Entry Registries of the Generalitat Valenciana and clearly indicating this desire.

Revocation Reason

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 requesting a new certificate to replace an existing certificate.

cessationOfOperation

You SHOULD choose this revocation reason 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 of his certificate has been compromised. For example if an unauthorized person has gained access to the private key of his 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.

Certificates with serverAuthentication keyuse are subject to the CA/Browser Forum definition at https://cabforum.org/working-groups/server/baseline-requirements/documents/. Among the conditions established is the obligation to revoke the certificates if it is detected that the issuance or operation does not comply with the defined regulations. This revocation must be made within a maximum period of between one (1) and five (5) calendar days depending on the type of incident and no postponement of any kind is possible. If it is not possible to comply with this condition, certificates issued under this regulation should never be used.

By signing this document, the citizen authorizes ACCV to consult the identity data contained in the Ministry of Interior, avoiding the citizen to provide a photocopy of his identity document.