Agencia de Tecnología
y Certificación Electrónica

Certification Policy for

Secure Server SSL

Date: 20/05/2018	**Version:** 3.0.2
Status: APPROVED	**Number of Pages:** 38
OID: 1.3.6.1.4.1.8149.3.3.3.0	**Classification: PUBLIC**
File: ACCV-CP-03V3.0.2-EN-2018.doc	
Prepared by: Agencia de Tecnología y Certificación Electrónica - ACCV	

This document is property of the Institut Valencià de Finances - ACCV.
It is forbidden its total or partial reproduction without previous authorization of the
Institut Valencià de Finances - ACCV

Table of Content

1. INTRODUCTION....9

1.1. PRESENTATION....9
1.2. IDENTIFICATION....9
1.3. USER COMMUNITY AND SCOPE OF APPLICATION....10
1.3.1. Certification Authorities....10
1.3.2. Register Authorities....10
1.3.3. End Users....10
1.3.3.1. Subscribers....10
1.3.3.2. Relying Third Parties....10
1.4. CERTIFICATE USAGE....10
1.4.1. Allowed Usages....10
1.4.2. Restricted Usages....10
1.5. ACVV MANAGEMENT POLICY....11
1.5.1. Managing Organization Policy....11
1.5.2. Contact Person....11
1.5.3. Competence for establish the CPS Suitability....11
1.6. DEFINITIONS AND ACRONYMS....11
1.6.1. Definitions....11
1.6.2. Acronyms....11

2. INFORMATION AND CERTIFICATES DISCLOSURE....12

2.1. CERTIFICATES REPOSITORY....12
2.2. DISCLOSURE....12
2.3. UPDATES FREQUENCY....12
2.4. CERTIFICATES REPOSITORY CONTROL ACCESS....12

3. IDENTIFICATION AND AUTHENTICATION....13

3.1. NAMES REGISTER....13
3.1.1. Type of names....13
3.1.2. Meaning of names....13
3.1.3. Names format interpretation....13
3.1.4. Names uniqueness....13
3.1.5. Resolution of names conflicts....13
3.1.6. Recognition, authentication and role of Trademarks....13
3.2. INITIAL IDENTITY VALIDATION....13
3.2.1. Methods to prove private key possession....13
3.2.2. Authentication of organization and domain identity....13
3.2.3. Authentication of individual identity....14

3.2.4. Verification of Requested Domain....14
3.3. IDENTIFICATION AND AUTHENTICATION OF PAIR KEY RENEWAL REQUESTS....15
3.3.1. Identification and authentication of routine renewal requests....15
3.3.2. Identification and authentication of key renewal requests after a revocation – Non-compromised key 16
3.4. IDENTIFICATION AND AUTHENTICATION OF PAIR KEY REVOCATION REQUESTS....16
4. CERTIFICATES LIFE CYCLE....17
4.1. CERTIFICATES APPLICATION....17
4.2. CERTIFICATES APPLICATION PROCESSING....17
4.3. CERTIFICATES ISSUANCE....17
4.4. CERTIFICATES ACCEPTANCE....18
4.5. PAIR KEYS AND CERTIFICATES USAGE....18
4.6. CERTIFICATES RENEWAL....18
4.7. KEYS RENEWAL....18
4.8. CERTIFICATES CHANGE....18
4.9. CERTIFICATES REVOCATION AND SUSPENSION....18
4.9.1. Circumstances for revocation....18
4.9.2. Entity that can apply for a revocation....18
4.9.3. Revocation application process....18
4.9.3.1. Telematic....18
4.9.4. Revocation Request Grace Period....19
4.9.5. .Time Within which CA Must Process the Revocation Request....19
4.9.6. Revocation Checking Requirement for Relying Parties....19
4.9.7. CRLs issuance frequency....19
4.9.8. Maximum Latency for CRLs....19
4.9.9. On-line Revocation/Status Checking Availability....19
4.9.10. On-line Revocation Checking Requirements....19
4.9.11. Other Forms of Revocation Advertisements Available....19
4.9.12. Special requirements of compromised key renewal....19
4.9.13. Circumstances for a suspension....19
4.9.14. Entities that can apply for the suspension....19
4.9.15. Procedure for the suspension request....19
4.9.16. Suspension period limit....19
4.10. CERTIFICATE STATUS SERVICES....19
4.11. END OF SUBSCRIPTION....20
4.12. KEYS ESCROW AND RECOVERY....20
4.13. CA CERTIFICATES KEYS EXPIRATION....20
5. PHYSICAL, PROCEDURAL AND MANAGEMENT CONTROLS....21

5.1. PHYSICAL CONTROLS....21
5.1.1. Site location and construction....21
5.1.2. Physical access....21
5.1.3. Power and air conditioning....21
5.1.4. Water exposure....21
5.1.5. Fire prevention and protection....21
5.1.6. Storage system....21
5.1.7. Waste disposal....21
5.1.8. Remote backup....21
5.2. PROCEDURAL CONTROLS....21
5.2.1. Trusted roles....21
5.2.2. Number of persons required per task....21
5.2.3. Identification and authentication for each role....21
5.3. PERSONNEL SECURITY CONTROLS....22
5.3.1. Background, qualifications, experience and accreditation requirements....22
5.3.2. Background check procedures....22
5.3.3. Training requirements....22
5.3.4. Retraining requirements and frequency....22
5.3.5. Task shifting frequency and sequence....22
5.3.6. Sanctions for unauthorized actions....22
5.3.7. Staffing requirements....22
5.3.8. Documentation supplied to personnel....22
5.3.9. Regular checks on compliance....22
5.3.10. End of contracts....22
5.4. SECURE CONTROLS PROCEDURES....22
5.4.1. Types of events recorded....22
5.4.2. Logs processing frequency....22
5.4.3. Audit logs retention period....22
5.4.4. Audit logs protection....23
5.4.5. Audit logs backup procedures....23
5.4.6. Audit information recovery system (internal vs external)....23
5.4.7. Notification to subject cause of the event....23
5.4.8. Vulnerability Analysis....23
5.5. INFORMATION AND RECORDS ARCHIVAL....23
5.5.1. Types of record information and events....23
5.5.2. Archival retention period....23
5.5.3. Archival protection....23
5.5.4. Archival backup procedure....23
5.5.5. Records time stamp requirements....23
5.5.6. Audit information recovery system....23

5.5.7. Procedures for obtaining and verifying recorded information....23
5.6. KEY CHANGE....23
5.7. KEY COMPROMISE OR DISASTER RECOVERY....24
5.7.1. Hardware, software o data manipulation resources....24
5.7.2. Entity public key is revoked....24
5.7.3. Entity key is compromised....24
5.7.4. Security installation after natural or other type of disaster....24
5.8. CESSATION OF A CA....24
6. TECHNICAL SECURITY CONTROLS....25
6.1. KEY PAIR GENERATION AND INSTALLATION....25
6.1.1. Key pair generation....25
6.1.2. Private key delivery to the entity....25
6.1.3. Public key delivery to certificates issuer....25
6.1.4. CA public key delivery to users....25
6.1.5. Keys size....25
6.1.6. Public key generation parameters....25
6.1.7. Quality parameters checking....25
6.1.8. Hardware/software of keys generation....26
6.1.9. Key pair purposes....26
6.2. PRIVATE KEY PROTECTION....26
6.2.1. Cryptography module standards....26
6.2.2. Server features the certificate was issued for....26
6.2.3. Private key multi-person control....26
6.2.4. Private key custody....26
6.2.5. Private key backup....26
6.2.6. Private key file....26
6.2.7. Private key introduction into the cryptography module....27
6.2.8. Private key activation method....27
6.2.9. Private key deactivating method....27
6.2.10. Private key destroying method....27
6.3. OTHER ASPECTS OF PAIR KEY MANAGEMENT....27
6.3.1. Private key file....27
6.3.2. Private and public key period of usage....27
6.4. ACTIVATION DATA....27
6.4.1. Activation data generation and installation....27
6.4.2. Activation data protection....27
6.4.3. Other aspects of activation data....27
6.5. COMPUTER SECURITY CONTROLS....27
6.6. LIFE CYCLE SECURITY CONTROLS....27

6.7. NETWORK SECURITY CONTROLS....28
6.8. CRYPTOGRAPHY CONTROLS....28

7. CERTIFICATE AND CERTIFICATE REVOCATION LISTS (CRL) PROFILES....29

7.1. CERTIFICATE PROFILE....29
7.1.1. Version number....29
7.1.2. Certificate extension....29
7.1.3. Algorithms object identifier (OID)....30
7.1.4. Names format....30
7.1.5. Names restrictions....31
7.1.6. Certification policy object identifier....31
7.1.7. "Policy Constraints" extension usage....31
7.1.8. Policy qualifiers syntax and semantics....31
7.1.9. Semantic treatment for "Certificate Policy" extension....31
7.2. CRL PROFILE....31
7.2.1. Version number....31
7.2.2. CRL and extensions....31
7.3. CERTIFICATE REVOCATION LIST....31
7.3.1. Temporal limit of the certificates in the CRLs....31

8. COMPLIANCE AUDIT....32

8.1. FREQUENCY OF COMPLIANCE CHECKS FOR EACH ENTITY....32
8.2. ASSESSOR IDENTIFICATION/QUALIFICATION....32
8.3. RELATIONSHIP BETWEEN THE ASSESSOR AND THE ASSISTED ENTITY....32
8.4. SUBJECTS COVERED BY COMPLIANCE CHECK....32
8.5. ACTIONS TO TAKE AS A RESULT OF A DEFICIENCY....32
8.6. COMMUNICATION OF RESULTS....32

9. COMMERCIAL AND LEGAL REQUIREMENTS....33

9.1. FEES....33
9.1.1. Certificates issuance fees or certificates renewal fees....33
9.1.2. Certificates access fees....33
9.1.3. Fees for access to status information....33
9.1.4. Fees of other services as policies information....33
9.1.5. Refund policy....33
9.2. FINANCIAL CAPACITY....33
9.2.1. Compensation for third parties that trust in certificates issued by ACCV....33
9.2.2. Fiduciary relationships....33
9.2.3. Administration processes....33
9.3. PRIVACY POLICY....33
9.3.1. Reliable data....33

9.3.2. Non-confidential data....34
9.3.3. Certificates revocation/suspension data disclosure....34
9.4. PERSONAL DATA PROTECTION....34
9.4.1. Personal data protection scheme....34
9.4.2. Private data....34
9.4.3. Non-private data....34
9.4.4. Responsibilities....34
9.4.5. Personal data usage authorization....34
9.4.6. Data notification to administrative/judicial authorities....34
9.4.7. Other information disclosure methods....34
9.5. INTELLECTUAL PROPERTY RIGHTS....34
9.6. OBLIGATIONS AND CIVIL LIABILITY....34
9.6.1. Certification entity obligations....34
9.6.2. Register authority obligations....34
9.6.3. Subscribers obligations....35
9.6.4. Relying third parties obligations....35
9.6.5. Repository obligations....35
9.7. DISCLAIMERS OF WARRANTIES....35
9.8. LIABILITIES LIMITATIONS....35
9.8.1. Warranty and warranty limitations....35
9.8.2. Segregation of responsibilities....35
9.8.3. Loss limitations....35
9.9. TERM AND TERMINATION....35
9.9.1. Term....35
9.9.2. Termination....35
9.9.3. Survival....35
9.10. NOTIFICATIONS....35
9.11. MODIFICATIONS....36
9.11.1. Procedures of modification specifications....36
9.11.2. Procedures of publication and notification....36
9.11.3. Procedures of Certification Practices Statement acceptance....36
9.12. CONFLICTS RESOLUTION....36
9.12.1. Off-court conflict resolution....36
9.12.2. Competent jurisdiction....36
9.13. APPLICABLE LAW....36
9.14. ACCORDANCE WITH THE APPLICABLE LAW....36
9.15. VARIOUS CLAUSES....36
ANNEX I....37

1. INTRODUCTION

1.1. Presentation

This document is the Certification Policy corresponding to Secure Server SSL Certificates, that contains the terms associated to the management and usage of certificates that this policy describes. The roles, responsibilities and relations between the end-user and the Agencia de Tecnología y Certificación Electrónica are described in this paper. This Certification Policy details and complements the general information found in the Certification Practices Statement (CPS) of the Agencia de Tecnología y Certificación Electrónica.

The Certification Policy mentioned in this paper will be used for Secure Server Certificate issuance.

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

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

This Certification Policy assumes that the reader has a basic understanding of Public Key Infrastructure, digital certificates and electronic signature. If this is not the case, the reader is recommended to be trained in those concepts before continuing reading this document.

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

1.2. Identification

Policy Name	Certification Policy for Servers with SSL support certificates
Policy Qualifier	Certificado para Servidores con Soporte SSL expedido por el Instituto Valenciano de Finanzas - ACCV (Plz de Napoles y Sicilia, 6. Valencia CP 46003, ESPAÑA. CIF Q9650010C)
Policy Version	3.0.2
Policy Status	APPROVED
Policy Reference/OID	1.3.6.1.4.1.8149.3.3.3.0
Date of Issuance	20th may, 2017
Expiration Date	Not applicable.
Related CPS	Certification Practices Statement (CPS) of ACCV. Version 4.0 OID: 1.3.6.1.4.1.8149.2.4.0 Available at http://www.accv.es/pdf-politicas
Localization	This Certification Policy can be found at: http://www.accv.es/legislacion_c.htm

1.3. User community and scope of application

1.3.1.Certification Authorities

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

1.3.2.Register Authorities

The Register Authority that manages these types of certificates is the Agencia de Tecnología y Certificación Electrónica.

1.3.3.End Users

1.3.3.1. Subscribers

The group of users that can apply for the mentioned certificates of this Policy are formed by public or private entities leaders, who have representation capabilities of the requested entity.

In case of public entities, the application can be performed by Head of Area or equivalent organizational position of any type of Public Administration, being these ones the last in charge of its use between the different projects or information systems.

In case of private entities, persons with the entity representation capability or persons that have been authorized for its management will be able to apply for the certificates.

Certificate requesting rights defined in this Certification Policy are limited to individual persons. Applications performed by legal bodies, entities or organizations will not be accepted.

1.3.3.2. Relying Third Parties

The Secure Server SSL Certificates reliability issued under this Policy is not limited. Any natural person or computer system can trust in these certificates for server identity purposes and for communication encryption between them and their users.

1.4. Certificate Usage

1.4.1. Allowed Usages

Certificates that were issued by the Agencia de Tecnología y Certificación Electrónica under this Certification Policy can be used for bringing SSL/TLS capabilities to computer servers. At the same time, it can be used as an unambiguous server or internet domain identification method for users that apply for this service.

1.4.2.Restricted Usages

Certificates will be only used according to the function and objective that this Certification Policy describes, and in agreement with all other legislation in force.

1.5. ACVV Management Policy

1.5.1.Managing Organization Policy

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

1.5.2.Contact Person

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

1.5.3.Competence for establish the CPS Suitability

The competent body to determine the conformity of this CPS to the various Certification Policies is the Sub directorate of of Financial Institutions and Electronic Certification Institut Valencià de Finances (IVF).

1.6. Definitions and acronyms

1.6.1.Definitions

Secure Sockets Layer: (SSL) and its following, Transport Layer Security (TLS) are encrypted protocols that bring secure network connection, commonly Internet.

1.6.2.Acronyms

SSL: Secure Sockets Layer

TLS: Transport Security Layer

2. Information and certificates disclosure

2.1. Certificates Repository

As specified in ACCV Certification Practices Statement (CPS)

2.2. Disclosure

As specified in ACCV Certification Practices Statement (CPS)

2.3. Updates frequency

As specified in ACCV Certification Practices Statement (CPS)

2.4. Certificates repository control access

As specified in ACCV Certification Practices Statement (CPS)

3. Identification and Authentication

3.1. Names register

3.1.1.Type of names

As specified in ACCV Certification Practices Statement (CPS)

3.1.2.Meaning of names

As specified in ACCV Certification Practices Statement (CPS)

3.1.3.Names format interpretation

As specified in ACCV Certification Practices Statement (CPS)

3.1.4.Names uniqueness

Secure Server SSL Certificate will be issued with the full legal name (server name plus domain) that corresponds to the service that will bring SSL features. This name must be unique in the network. Partial names will not be accepted.

CN = SYSTEM NAME + DOMAIN IT BELONGS TO

3.1.5.Resolution of names conflicts

As specified in ACCV Certification Practices Statement (CPS)

3.1.6.Recognition, authentication and role of Trademarks

As specified in ACCV Certification Practices Statement (CPS)

3.2. Initial Identity Validation

3.2.1.Methods to prove private key possession

As specified in ACCV Certification Practices Statement (CPS)

3.2.2.Authentication of organization and domain identity

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

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

The applicant must submit the necessary documentation which determines

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

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

The domain possession (3.2.4).

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

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

Data Protection Agencies

Public Administrations register

Commercial register

Verification services and Consultation of identity data

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

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

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

3.2.3.Authentication of individual identity

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

The applicant must submit the necessary documentation which determines the representative capabilities of the entity that owns the referred domain and, which also determines that domain possession. This submitting will be carried out digitally using the sources and applications that ACCV provided to the users for this task (3.2.4).

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

Data Protection Agencies

Public Administrations register

Commercial register

Verification services and Consultation of identity data

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

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

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

3.2.4.Verification of Requested Domain

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

Specifically:

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

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

Contacting by mail, sending a unique random number in the mail to the domain name registrant's address, waiting for a time not exceeding 30 days.and checking the response that must include the same random number

Contacting by mail, sending a unique random number in the mail to tone or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name, including a Random Value in the email, and receiving a confirming response utilizing the Random Value., waiting for a time not exceeding 30 days.and checking the response that must include the same random number

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

Confirming the presence of a random number for either in a DNS CNAME, TXT or CAA record for either 1) an Authorization Domain Name; or 2) an Authorization Domain Name that is prefixed with a label that begins with an underscore character. Once the number is communicated to the applicant, it will only be valid for 30 days.

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

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

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

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

3.3. Identification and authentication of pair key renewal requests

3.3.1. Identification and authentication of routine renewal requests

For certificate renewal the identification and authentication can be carried out using the initial authentication and identification technique (described in points 3.2.2. *“Authentication of organization and domain identity”* and 3.2.3. “*Individual identity authentication”* of this Certification Policy). ACCV can reuse the stored information in the previous checks if there has not passed 13 months since the last data verification. Exist, therefore, one mechanism for the renewal:

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

3.3.2.Identification and authentication of key renewal requests after a revocation – Non-compromised key

The identification and authentication policy for a certificate renewal after a non-compromised key revocation will be the same as for the initial register, and it is possible to reuse the information that is in possession of ACCV if there has not passed 13 months since its last data verification. The ACCV can implement any digital method that guarantees in a reliable and unequivocal way the applicant identity and the application authentication because of technical questions and detailing every step that it takes.

3.4. Identification and authentication of pair key revocation requests

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

a) Telematic. Through a revocation form (located in the Non-Personal Certificates Management Area https://npsc.accv.es:8450/npsc) accessing by the certificate applicant or its responsible part, on the revocation date with a personal qualified certificate.

ACCV or any entity that is composed of, may apply for the revocation of a certificate if they have knowledge or suspect the certificate's private key associated to the certificate that is issued under this Certification Policy has been compromised or any other fact which would require such action.

4. Certificates life cycle

Specifications contained in this section complement the stipulations written in the ACCV Certification Practice Statement (CPS).

4.1. Certificates Application

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

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

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

4.2. Certificates application processing

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

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

In addition to check the associated credentials to the entity, ACCV will verify in the authorized registers the possession of domain or domains that appear in the certificate request, so there is no doubt about the existence of this possession, as detailed in sections 3.2.2, 3.2.3 and 3.2.4 of this policy. ACCV will leave a record of these searches and checks so they can be reproduced in every step. For this checking ACCV will use the mails and phones that were submitted in the register process, being necessary a direct connection between these data and the domains that are included in the application.

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

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

ACCV will use this information to decide on new applications.

4.3. Certificates issuance

ACCV will carry out frequent revisions about secure server certificates samples for guaranteeing the data accuracy. If in the course of these samplings it is confirmed a data change that may involve the domain possession loss, the ACCV will revoke the involved certificates. In case of inaccuracy of the information that is contained in the certificate or its non-applicability the same process will be applied. ACCV will leave a documentary proof of all these revisions and actions.

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

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

ACCV can carry out this authorization ex-officio in case the Secure Server Certificate's (SSL) responsible loses his management capabilities and there is no other authorized person.

4.4. Certificates acceptance

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

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

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

4.5. Pair keys and certificates usage

As specified in ACCV Certification Practices Statement (CPS)

4.6. Certificates renewal

As specified in ACCV Certification Practices Statement (CPS)

4.7. Keys renewal

As specified in ACCV Certification Practices Statement (CPS)

4.8. Certificates change

As specified in ACCV Certification Practices Statement (CPS)

4.9. Certificates revocation and suspension

4.9.1.Circumstances for revocation

As specified in ACCV Certification Practices Statement (CPS)

4.9.2.Entity that can apply for a revocation

Certificate's revocation can be requested by its same subscriber and by ACCV.

Certificate's subscribers can apply for its revocation for any or none reason and this revocation application must be carried out by specified terms found in the following section.

4.9.3.Revocation application process

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

4.9.3.1. Telematic

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

4.9.4.Revocation Request Grace Period

As specified in ACCV Certification Practices Statement (CPS)

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

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

4.9.6.Revocation Checking Requirement for Relying Parties

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

4.9.7.CRLs issuance frequency

As specified in ACCV Certification Practices Statement (CPS)

4.9.8.Maximum Latency for CRLs

As specified in ACCV Certification Practices Statement (CPS)

4.9.9.On-line Revocation/Status Checking Availability

As specified in ACCV Certification Practices Statement (CPS)

4.9.10.On-line Revocation Checking Requirements

As specified in ACCV Certification Practices Statement (CPS)

4.9.11.Other Forms of Revocation Advertisements Available

As specified in ACCV Certification Practices Statement (CPS)

4.9.12.Special requirements of compromised key renewal

As specified in ACCV Certification Practices Statement (CPS)

4.9.13.Circumstances for a suspension

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

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

4.9.14.Entities that can apply for the suspension

As specified in ACCV Certification Practices Statement (CPS)

4.9.15.Procedure for the suspension request

As specified in ACCV Certification Practices Statement (CPS)

4.9.16.Suspension period limit

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

4.10. Certificate Status Services

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

4.11. End of Subscription

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

ACCV will notify the Secure Server Certificate's (SSL) person in charge, through a digital signed electronic email, in a period preceding the previous certification publication in the Certificate Revocation List, about the certificates suspension or revocation is subscriber or is in charge of, specifying the reasons, the date and time the certificate shall terminate, and notifying that it must not be used.

4.12. Keys escrow and recovery

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

4.13. CA certificates keys expiration

ACCV will avoid generating Secure Serve Certificates (SLL) which expire subsequently to CA certificates. For this, Secure Server Certificates (SSL) which validity period exceed the CA's certificate will not be issued and they will be generated with the new CA certificate, with the purpose of avoiding notifying the subscribers about the certificate renewal, in case the CA certificate expires earlier.

5. Physical, procedural and management controls

5.1. Physical Controls

5.1.1.Site location and construction
As specified in ACCV Certification Practices Statement (CPS)

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

5.1.3.Power and air conditioning
As specified in ACCV Certification Practices Statement (CPS)

5.1.4.Water exposure
As specified in ACCV Certification Practices Statement (CPS)

5.1.5.Fire prevention and protection
As specified in ACCV Certification Practices Statement (CPS)

5.1.6.Storage system
As specified in ACCV Certification Practices Statement (CPS)

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

5.1.8.Remote backup
As specified in ACCV Certification Practices Statement (CPS)

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

5.2.1.Trusted roles
As specified in ACCV Certification Practices Statement (CPS)

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

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

5.3. Personnel security controls

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

5.3.1.Background, qualifications, experience and accreditation requirements

As specified in ACCV Certification Practices Statement (CPS)

5.3.2.Background check procedures

As specified in ACCV Certification Practices Statement (CPS)

5.3.3.Training requirements

As specified in ACCV Certification Practices Statement (CPS)

5.3.4.Retraining requirements and frequency

As specified in ACCV Certification Practices Statement (CPS)

5.3.5.Task shifting frequency and sequence

As specified in ACCV Certification Practices Statement (CPS)

5.3.6.Sanctions for unauthorized actions

As specified in ACCV Certification Practices Statement (CPS)

5.3.7.Staffing requirements

As specified in ACCV Certification Practices Statement (CPS)

5.3.8.Documentation supplied to personnel

As specified in ACCV Certification Practices Statement (CPS)

5.3.9.Regular checks on compliance

As specified in ACCV Certification Practices Statement (CPS)

5.3.10.End of contracts

As specified in ACCV Certification Practices Statement (CPS)

5.4. Secure controls procedures

5.4.1.Types of events recorded

As specified in ACCV Certification Practices Statement (CPS)

5.4.2.Logs processing frequency

As specified in ACCV Certification Practices Statement (CPS)

5.4.3.Audit logs retention period

As specified in ACCV Certification Practices Statement (CPS)

5.4.4.Audit logs protection
As specified in ACCV Certification Practices Statement (CPS)

5.4.5.Audit logs backup procedures
As specified in ACCV Certification Practices Statement (CPS)

5.4.6.Audit information recovery system (internal vs external)
As specified in ACCV Certification Practices Statement (CPS)

5.4.7.Notification to subject cause of the event
As specified in ACCV Certification Practices Statement (CPS)

5.4.8.Vulnerability Analysis
As specified in ACCV Certification Practices Statement (CPS)

5.5. Information and records archival

5.5.1.Types of record information and events
As specified in ACCV Certification Practices Statement (CPS)

5.5.2.Archival retention period
As specified in ACCV Certification Practices Statement (CPS)

5.5.3.Archival protection
As specified in ACCV Certification Practices Statement (CPS)

5.5.4.Archival backup procedure
As specified in ACCV Certification Practices Statement (CPS)

5.5.5.Records time stamp requirements
As specified in ACCV Certification Practices Statement (CPS)

5.5.6.Audit information recovery system
As specified in ACCV Certification Practices Statement (CPS)

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

5.6. Key change
Not stipulated.

5.7. Key compromise or disaster recovery

As specified in ACCV Certification Practices Statement (CPS)

5.7.1.Hardware, software o data manipulation resources

As specified in ACCV Certification Practices Statement (CPS)

5.7.2.Entity public key is revoked

As specified in ACCV Certification Practices Statement (CPS)

5.7.3.Entity key is compromised

As specified in ACCV Certification Practices Statement (CPS)

5.7.4.Security installation after natural or other type of disaster

As specified in ACCV Certification Practices Statement (CPS)

5.8. Cessation of a CA

As specified in ACCV Certification Practices Statement (CPS)

6. Technical Security Controls

6.1. Key pair generation and installation

Keys generated for certificates issued under this Certification Policy will be referred to in this section of this document. The information about the keys of entities which compose the Certification Authority is found in the section 6.1 of Agencia de Tecnología y Certificación Electrónica's Certification Practice Statement (CPS).

6.1.1.Key pair generation

The key pair of the certificate issued under this Certification Policy is software generated by the certificate's subscriber.

6.1.2.Private key delivery to the entity

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

6.1.3.Public key delivery to certificates issuer

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

6.1.4.CA public key delivery to users

As specified in ACCV Certification Practices Statement (CPS)

6.1.5.Keys size

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

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

6.1.6.Public key generation parameters

ACCVRAIZ1 and ACCVCA-120 root's keys are generates with RSA algorithm.

Parameters defined in cryptography suite 001 specified in ETSI TS 102 176-1 "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms" are used. ModLen=2048 is defined.

Signature suite entry name	Signature algorithm	Signature algorithm parameters	Key generation algorithm	Padding method	Cryptographic hash function
Sha-256-with-rsa	rsa	MinModLen=2048	rsagen1	emsa-pkcs1-v1_5	sha256

6.1.7.Quality parameters checking

Parameters defined in cryptography suite 001 specified in ETSI TS 102 176-1 "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms" are used. ModLen=2048 is defined.

Signature	Signature	Signature	Key generation	Padding method	Cryptographic hash

suite entry name	algorithm	algorithm parameters	algorithm		function
Sha-256-with-rsa	rsa	MinModLen=2048	rsagen1	emsa-pkcs1-v1_5	sha256

6.1.8.Hardware/software of keys generation

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

6.1.9.Key pair purposes

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

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

6.2. Private key protection

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

6.2.1.Cryptography module standards

Not applicable in this Policy domain.

6.2.2.Server features the certificate was issued for

It is recommended systems where the private keys are stored to meet a set of physical and logical security requirements. ACCV advises the subscriber organism to apply the NCC (National Cryptography Center) guides in its NCC-STIC serial, specifically for ensuring the safety of information and communication technology systems, so the Secure Socket Layer servers' security level increases and, so on, certificates' linked keys.

6.2.3.Private key multi-person control

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

6.2.4.Private key custody

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

6.2.5.Private key backup

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

6.2.6.Private key file

Private keys are not filed.

6.2.7.Private key introduction into the cryptography module

Not applicable in this Policy domain.

6.2.8.Private key activation method

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

6.2.9.Private key deactivating method

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

6.2.10.Private key destroying method

Not stipulated.

6.3. Other aspects of pair key management

6.3.1.Private key file

As specified in ACCV Certification Practices Statement (CPS)

6.3.2.Private and public key period of usage

Certificates issued under this Policy are valid for 3 years.

The key used for the certificates' issuance is generated for each issuance, and therefore they are valid for 3 years as well.

The ACCVCA-120 certificate is valid since 13th October 2011 to 1st January 2027.

6.4. Activation data

6.4.1.Activation data generation and installation

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

6.4.2.Activation data protection

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

6.4.3.Other aspects of activation data

Not stipulated.

6.5. Computer security controls

As specified in ACCV Certification Practices Statement (CPS)

6.6. Life cycle security controls

As specified in ACCV Certification Practices Statement (CPS)

6.7. Network security controls

As specified in ACCV Certification Practices Statement (CPS)

6.8. Cryptography controls

As specified in ACCV Certification Practices Statement (CPS)

7. Certificate and certificate revocation lists (CRL) profiles

7.1. Certificate profile

7.1.1.Version number

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

7.1.2.Certificate extension

The extensions used by certificates issued under this policy are:

Field	**Value**	
Subject		
SerialNumber	Administration NIF, organism or entity of private or public right that is the certificates subscriber, which the website is linked to.	
CommonName	Primary domain name (DNS) to which the certificate responds.	
OrganizationalUnit	Fixed chain with SERVIDORES value	
Organization	Designation ("official" name) of the Administration, organism or entity of public right that is the certificate subscriber and the domain owner.	
Locality	Town	
State	Province	
Country	Fixed chain with ES value	
Version	V3	
SerialNumber	Unique identifier of the certificate. Under 32 hexadecimals characters.	
Signature Algorithm	sha256withRSAEncryption	
Issuer		
CommonName	ACCVCA-120	
OrganizationalUnit	PKIACCV	
Organization	ACCV	
Country	ES	
Valid since	Issuance Date	
Valid until	Expiration date	
Public Key	Octet String that contains the SSL certificate's public key	
Extended Key Usage		
	Server Authentication	
CRL Distribution Point		
	distributionPoint	http://www.accv.es/fileadmin/Archivos/certificados/accvca120_der.crl
	distributionPoint	http://www.accv.es/gestcert/accvca120_der.crl
SubjectAlternativeName		

	dnsName	Domain Name DNS 1 (matches with the domain in the common name)
	dnsName	DNS2 Domain Name
	dnsName	DNS3 Domain Name
Certificate Policy Extensions		
Policy OID	1.3.6.1.4.1.8149.3.3.3.0	
Policy CPS Location	http://www.accv.es/legislacion_c.htm*	
Policy Notice	Certificado para Servidores con Soporte SSL expedido por el Instituto Valenciano de Finanzas - ACCV (Plz de Napoles y Sicilia, 6. Valencia CP 46003, ESPAÑA. CIF Q9650010C)	
Authority Information Access	*Access Method*	Id-ad-ocsp
	Access Location	http://ocsp.accv.es
	Access Method	Id-ad-caIssuers
	Access Location	http://www.accv.es/gestcert/ ACCVCA120SHA2.cacert.crt
Fingerprint issuer	48 72 a4 c3 df 17 4c ef 34 d7 7f e6 a3 b4 e7 be 7d f2 d2 5d	
Hash Algorithm	SHA-256	
Qualified Certificate Statements	QcCompliance	
	QcEuRetention Period	15
KeyUsage (critical)		
	Digital Signature Key Encipherment	

7.1.3.Algorithms object identifier (OID)

Object identifier (OID) of cryptography algorithms:

- SHA1withRSA (1.2.840.113549.1.1.5)
- SHA256withRSA (1.2.840.113549.1.1.11)

7.1.4.Names format

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

- Subject name: cn=*Primary domain name (DNS) to which the certificate responds*, ou=*Servidores*, o=*Designation ("official" name) of the Administration, organism or entity of public right that is the certificate subscriber and the domain owner,* c=*ES*
- Issuer name: cn=ACCVCA-120, ou=PKIACCV o=ACCV, c=ES

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

7.1.5.Names restrictions

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

7.1.6.Certification policy object identifier

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

1.3.6.1.4.1.8149.3.3.3.0

7.1.7.“Policy Constraints” extension usage

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

7.1.8.Policy qualifiers syntax and semantics

Not stipulated.

7.1.9.Semantic treatment for “Certificate Policy” extension

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

7.2. CRL profile

7.2.1.Version number

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

7.2.2.CRL and extensions

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

7.3. Certificate Revocation List

7.3.1.Temporal limit of the certificates in the CRLs

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

8. Compliance audit

8.1. Frequency of compliance checks for each entity

As specified in ACCV Certification Practices Statement (CPS)

8.2. Assessor identification/qualification

As specified in ACCV Certification Practices Statement (CPS)

8.3. Relationship between the assessor and the assisted entity

As specified in ACCV Certification Practices Statement (CPS)

8.4. Subjects covered by compliance check

As specified in ACCV Certification Practices Statement (CPS)

8.5. Actions to take as a result of a deficiency

As specified in ACCV Certification Practices Statement (CPS)

8.6. Communication of results

As specified in ACCV Certification Practices Statement (CPS)

9. Commercial and legal requirements

9.1. Fees

9.1.1. Certificates issuance fees or certificates renewal fees

The initial issuance and certificate renewal fee that this certification policy refers to, is contained in ACCV fees list. This list is published in ACCV web site www.accv.es

9.1.2. Certificates access fees

The access for certificates issued under this policy, is open and free and, therefore there is no fee to be applied.

9.1.3. Fees for access to status information

The access for certificates' status or revocation information is open and free and, therefore there is no fee to be applied.

9.1.4. Fees of other services as policies information

As specified in ACCV Certification Practices Statement (CPS)

9.1.5. Refund policy

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

9.2. Financial capacity

9.2.1. Compensation for third parties that trust in certificates issued by ACCV

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

9.2.2. Fiduciary relationships

As specified in ACCV Certification Practices Statement (CPS)

9.2.3. Administration processes

As specified in ACCV Certification Practices Statement (CPS)

9.3. Privacy policy

9.3.1. Reliable data

As specified in ACCV Certification Practices Statement (CPS)

9.3.2.Non-confidential data

As specified in ACCV Certification Practices Statement (CPS)

9.3.3.Certificates revocation/suspension data disclosure

As specified in ACCV Certification Practices Statement (CPS)

9.4. Personal data protection

As specified in ACCV Certification Practices Statement (CPS)

9.4.1.Personal data protection scheme

As specified in ACCV Certification Practices Statement (CPS)

9.4.2.Private data

As specified in ACCV Certification Practices Statement (CPS)

9.4.3.Non-private data

As specified in ACCV Certification Practices Statement (CPS)

9.4.4.Responsibilities

As specified in ACCV Certification Practices Statement (CPS)

9.4.5.Personal data usage authorization

As specified in ACCV Certification Practices Statement (CPS)

9.4.6.Data notification to administrative/judicial authorities

As specified in ACCV Certification Practices Statement (CPS)

9.4.7.Other information disclosure methods

As specified in ACCV Certification Practices Statement (CPS)

9.5. Intellectual property rights

As specified in ACCV Certification Practices Statement (CPS)

9.6. Obligations and civil liability

9.6.1.Certification entity obligations

As specified in ACCV Certification Practices Statement (CPS)

9.6.2.Register authority obligations

As specified in ACCV Certification Practices Statement (CPS)

9.6.3.Subscribers obligations

As specified in ACCV Certification Practices Statement (CPS)

9.6.4.Relying third parties obligations

As specified in ACCV Certification Practices Statement (CPS)

9.6.5.Repository obligations

As specified in ACCV Certification Practices Statement (CPS)

9.7. Disclaimers of warranties

As specified in ACCV Certification Practices Statement (CPS)

9.8. Liabilities limitations

9.8.1.Warranty and warranty limitations

As specified in ACCV Certification Practices Statement (CPS)

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

9.8.2.Segregation of responsibilities

As specified in ACCV Certification Practices Statement (CPS)

9.8.3.Loss limitations

As specified in ACCV Certification Practices Statement (CPS)

9.9. Term and termination

9.9.1.Term

As specified in ACCV Certification Practices Statement (CPS)

9.9.2.Termination.

As specified in ACCV Certification Practices Statement (CPS)

9.9.3.Survival.

As specified in ACCV Certification Practices Statement (CPS)

9.10. Notifications.

As specified in ACCV Certification Practices Statement (CPS)

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

9.11. Modifications.

As specified in ACCV Certification Practices Statement (CPS)

9.11.1.Procedures of modification specifications

As specified in ACCV Certification Practices Statement (CPS)

9.11.2.Procedures of publication and notification

As specified in ACCV Certification Practices Statement (CPS)

9.11.3.Procedures of Certification Practices Statement acceptance

As specified in ACCV Certification Practices Statement (CPS)

9.12. Conflicts resolution

9.12.1.Off-court conflict resolution

As specified in ACCV Certification Practices Statement (CPS)

9.12.2.Competent jurisdiction

As specified in ACCV Certification Practices Statement (CPS)

9.13. Applicable law

As specified in ACCV Certification Practices Statement (CPS)

9.14. Accordance with the applicable law

As specified in ACCV Certification Practices Statement (CPS)

9.15. Various clauses

As specified in ACCV Certification Practices Statement (CPS)

Annex I

CERTIFICATION CONTRACT – OID 1.3.6.1.4.1.8149.3.3

Section 1 – Applicant information

Surname: .....

Name: ..... DNI/NIF: .....

Entity / Service: .....

Authority: .....

E-mail address: .....

Mailing address: ..... Tel.: .....

Section 2 – Computer system to be certificated information

Qualified name: .....

Nickname (if the certificate is not issued for qualified name): .....

IP Address: ..... Service: .....

Section 4 – Date and Signature

I apply for the Certificate associated to the 1.3.6.1.4.1.8149.3.3 Certification Policy for Secure Servers (SSL) issued by ACCV. I declare the knowledge and acceptance of these certificates' terms of usage, which can be found at http://www.accv.es I declare that all data stated here is correct.

At ..... on .... of 2.0....

Signature of applicant

Fdo.:

CERTIFICATION CONTRACT – OID 1.3.6.1.4.1.8149.3.3

Certificate usage conditions

- Certificates associated to Secure Servers Certificates' (SSL) Certification Policy, issued by ACCV are X.509v3 type and follow ACCV Certification Practices Statement, as Certification Services Provider and so the referred Certification Policy. Both documents should be considered in accordance with the European Community law, the Spanish legal order and the Generalitat's law.

- Certificate's applicant must be a natural person with a certificate recognized by Agencia de Tecnología y Certificación Electrónica and they must be implemented in a Public Administration, Administration Legal Body or Corporate Entity.

- Certificates' applicant, specially someone who was enabled for their management by a public Entity or Administration, is the responsible for verifying the given information veracity along the request process and register. He will carry out the corresponding notification about any given information changes.

- Certificate's subscriber is responsible for its private key safeguarding and for notifying as soon as possible about its possible loss or subtraction.

- Certificate's subscriber is responsible for limiting the certificate's usage as the associated Certification Policy determines in a public document found at http://www.accv.es

- ACCV is not responsible for the contents of documents signed with their certificates.

- ACCV is responsible for the accomplishment of European, Spanish and Valencian laws in order to the Electronic Signature. Therefore, it is responsible for complying ACCV Certification Practices Statement and the Certification Policy associated to this type of certificates specifications.

- These type of certificate will be valid for three (3) years as maximum. For its renewal the same steps as for its request or the ones provided by the associated Certification Policy will be followed.

- The issued certificates will lose their efficacy, besides its period of validity expiration, when a revocation is produced, when its hardware becomes disabled, in presence of a judicial or administrative resolution which governs the efficacy loss, because of serious inaccuracies of submitted data by the requester and because of the certificate subscriber death. Other conditions for the efficacy loss are listed in the Certification Practices Statement and in the associated Certification Policy to this type of certificates.

- In accordance to Personal Data Protection Basic Law 15/1999, 13th December, the applicant will be informed about a personal information automated file created under the responsibility of ACCV, named "Electronic Signature Users".The purpose of said file is to serve to related uses with certification services provided by ACCV. The subscriber authorizes the use of his/her private data that is contained in said file, as necessary, for carrying out the action that are planned in the Certification Policy

- ACCV is committed to avoid any alteration, loss or unauthorized access to the personal data contained in the file.

- The applicant will be able to exercise his rights of access, rectification or cancellation of his personal information sending a written notification to the Agencia de Tecnología y Certificación Electrónica, indicating clearly this request through any established Generalitat's Entry Registers.

- ACCV has formed a bank guarantee of three millions euros (3.000.000 €) to deal with the risk of damages actions that issued certificates and digital certification services usage could cause.

With the signature of the current document ACCV is authorized to consult identity data that are listed in the Interior Ministry, avoiding the citizen to submit a copy of his/her identity document.