



# Agencia de Tecnología y Certificación Electrónica

## Certification Policy for Qualified Certificates based on software for citizens

<b>Date:</b> 12/02/2024	<b>Version:</b> 8.0.2
<b>Status:</b> APPROVED	<b>Number of pages:</b> 55
<b>OID:</b> 1.3.6.1.4.1.8149.3.7.8.0	<b>Classification:</b> PUBLIC
<b>File:</b> ACCV-CP-07V8.0.2-EN-2024.odt	
<b>Prepared by:</b> Agencia de Tecnología y Certificación Electrónica - ACCV	



## Changelog

Version	Author	Date	Observations
6.0.1	ACCV	18/06/2019	RFC3647 Changes
6.0.2	ACCV	20/01/2020	CAB/Forum modification
6.0.3	ACCV	02/03/2020	RFC3647 Changes
6.0.4	ACCV	20/03/2021	Policy Notice changes
7.0.1	ACCV	09/03/2022	Mail account and S/MIME usage are optional
7.0.3	ACCV	16/03/2023	Review and minor changes.
7.0.4	ACCV	31/08/2023	EKU SMIME is removed
8.0.1	ACCV	05/10/2023	New hierarchy
8.0.2	ACCV	12/02/2024	Changes in CAs to adjust scope

## Table of Content

<b>1. INTRODUCTION.....</b>	<b>11</b>
1.1. OVERVIEW.....	11
1.2. IDENTIFICATION.....	11
1.3. PKI PARTICIPANTS.....	11
1.3.1. Certification Authorities.....	11
1.3.2. Registration Authorities.....	12
1.3.3. Subscribers.....	12
1.3.4. Relying parts.....	12
1.3.5. Other participants.....	12
1.4. CERTIFICATES USAGE.....	12
1.4.1. Appropriate certificate uses.....	12
1.4.2. Prohibited certificate uses.....	12
1.5. POLICY ADMINISTRATION.....	12
1.5.1. Organization administering the document.....	12
1.5.2. Contact person.....	13
1.5.3. Person determining CPS suitability for the policy.....	13
1.5.4. CPS approval procedures.....	13
1.6. DEFINITIONS AND ACRONYMS.....	13
<b>2. PUBLICATION AND REPOSITORY RESPONSIBILITIES.....</b>	<b>14</b>
2.1. REPOSITORIES.....	14
2.2. PUBLICATION OF CERTIFICATION INFORMATION.....	14
2.3. TIME OR FREQUENCY OF PUBLICATION.....	14
2.4. ACCESS CONTROLS ON REPOSITORIES.....	14
<b>3. IDENTIFICATION AND AUTHENTICATION.....</b>	<b>15</b>
3.1. NAMING.....	15
3.1.1. Types of names.....	15
3.1.2. Need for names to be meaningful.....	15
3.1.3. Anonymity or pseudonymity of subscribers.....	15
3.1.4. Rules for interpreting various name forms.....	15
3.1.5. Uniqueness of names.....	15
3.1.6. Recognition, authentication, and role of trademarks.....	15
3.2. INITIAL IDENTITY VALIDATION.....	15
3.2.1. Method to prove possession of private key.....	15
3.2.2. Authentication of organization identity.....	15
3.2.3. Authentication of individual identity.....	15
3.2.4. Non-verified subscriber information.....	16



3.2.5. <i>Validation of authority</i> .....	16
3.2.6. <i>Criteria for interoperation</i> .....	16
3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS.....	16
3.3.1. <i>Identification and authentication for routine re-key</i> .....	16
3.3.2. <i>Identification and authentication for re-key after revocation – Not compromised key</i> .....	16
3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST.....	16
<b>4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS.....</b>	<b>17</b>
4.1. CERTIFICATES APPLICATION.....	17
4.1.1. <i>Who can submit a certificate application</i> .....	17
4.1.2. <i>Enrollment Process and Responsibilities</i> .....	17
4.2. CERTIFICATE APPLICATION PROCESSING.....	17
4.2.1. <i>Performing identification and authentication functions</i> .....	17
4.2.2. <i>Approval or rejection of certificate applications</i> .....	18
4.2.3. <i>Time to process certificate applications</i> .....	18
4.3. CERTIFICATES ISSUANCE.....	18
4.3.1. <i>CA actions during certificate issuance</i> .....	18
4.3.2. <i>Notification to subscriber by the CA of issuance of certificate</i> .....	19
4.4. CERTIFICATES ACCEPTANCE.....	19
4.4.1. <i>Conduct constituting certificate acceptance</i> .....	19
4.4.2. <i>Publication of the certificate by the CA</i> .....	19
4.4.3. <i>Notification of certificate issuance by the CA to other entities</i> .....	19
4.5. KEY PAIR AND CERTIFICATE USAGE.....	19
4.5.1. <i>Subscriber private key and certificate usage</i> .....	19
4.5.2. <i>Relying party public key and certificate usage</i> .....	19
4.6. CERTIFICATE RENEWAL.....	19
4.6.1. <i>Circumstance for certificate renewal</i> .....	19
4.6.2. <i>Who may request renewal</i> .....	19
4.6.3. <i>Processing certificate renewal requests</i> .....	19
4.6.4. <i>Notification of new certificate issuance to subscriber</i> .....	20
4.6.5. <i>Conduct constituting acceptance of a renewal certificate</i> .....	20
4.6.6. <i>Publication of the renewal certificate by the CA</i> .....	20
4.6.7. <i>Notification of certificate issuance by the CA to other entities</i> .....	20
4.7. CERTIFICATE RE-KEY.....	20
4.7.1. <i>Circumstance for certificate re-key</i> .....	20
4.7.2. <i>Who may request certification of a new public key</i> .....	20
4.7.3. <i>Processing certificate re-keying requests</i> .....	20
4.7.4. <i>Notification of new certificate issuance to subscriber</i> .....	20
4.7.5. <i>Conduct constituting acceptance of a re-keyed certificate</i> .....	20



4.7.6. *Publication of the re-keyed certificate by the CA*..... 20

4.7.7. *Notification of certificate issuance by the CA to other entities*..... 20

4.8. CERTIFICATE MODIFICATION..... 20

4.8.1. *Circumstance for certificate modification*..... 20

4.8.2. *Who may request certificate modification*..... 21

4.8.3. *Circumstance for certificate modification*..... 21

4.8.4. *Notification of new certificate issuance to subscriber*..... 21

4.8.5. *Conduct constituting acceptance of modified certificate*..... 21

4.8.6. *Publication of the modified certificate by the CA*..... 21

4.8.7. *Notification of certificate issuance by the CA to other entities*..... 21

4.9. CERTIFICATE REVOCATION AND SUSPENSION..... 21

4.9.1. *Circumstances for revocation*..... 21

4.9.2. *Who can request revocation*..... 21

4.9.3. *Procedure for revocation request*..... 21

4.9.3.1. *On-site processing*..... 21

4.9.3.2. *Web*..... 21

4.9.3.3. *Phone*..... 21

4.9.4. *Revocation request grace period*..... 21

4.9.5. *Time within which CA must process the revocation request*..... 22

4.9.6. *Revocation checking requirement for relying parties*..... 22

4.9.7. *CRL issuance frequency*..... 22

4.9.8. *Maximum latency for CRLs*..... 22

4.9.9. *On-line revocation/status checking availability*..... 22

4.9.10. *On-line revocation checking requirements*..... 22

4.9.11. *Other forms of revocation advertisements available*..... 22

4.9.12. *Special requirements re key compromise*..... 22

4.9.13. *Circumstances for the suspension*..... 22

4.9.14. *Who can request suspension*..... 22

4.9.15. *Procedure for the suspension request*..... 22

4.9.16. *Limits of suspension period*..... 22

4.10. CERTIFICATE STATUS SERVICES..... 22

4.10.1. *Operational Characteristics*..... 22

4.10.2. *Service Availability*..... 22

4.10.3. *Optional features*..... 23

4.11. END OF SUBSCRIPTION..... 23

4.12. KEY ESCROW AND RECOVERY..... 23

4.12.1. *Key escrow and recovery policy and practices*..... 23

4.12.2. *Session key encapsulation and recovery policy and practices*..... 23

**5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS..... 24**

Qif.: <b>PUBLIC</b>	Ref.: ACCV-CP-07V8.0.2-EN-2024.odt	Version: 8.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.8.0	Pg. 5 of 55



5.1. PHYSICAL CONTROLS.....	24
5.1.1. Site location and construction.....	24
5.1.2. Physical access.....	24
5.1.3. Power and air conditioning.....	24
5.1.4. Water exposure.....	24
5.1.5. Fire prevention and protection.....	24
5.1.6. Media storage.....	24
5.1.7. Waste disposal.....	24
5.1.8. Off-site backup.....	24
5.2. PROCEDURAL CONTROLS.....	24
5.2.1. Trusted roles.....	24
5.2.2. Number of persons that are required per task.....	24
5.2.3. Identification and authentication for each role.....	24
5.2.4. Roles requiring separation of duties.....	25
5.3. PERSONNEL CONTROLS.....	25
5.3.1. Qualifications, experience, and clearance requirements.....	25
5.3.2. Background check procedures.....	25
5.3.3. Training requirements.....	25
5.3.4. Retraining frequency and requirements.....	25
5.3.5. Job rotation frequency and sequence.....	25
5.3.6. Sanctions for unauthorized actions.....	25
5.3.7. Independent contractor requirements.....	25
5.3.8. Documentation supplied to personnel.....	25
5.3.9. Periodical compliance controls.....	25
5.3.10. End of contracts.....	25
5.4. AUDIT LOGGING PROCEDURES.....	25
5.4.1. Types of events recorded.....	25
5.4.2. Frequency of processing log.....	26
5.4.3. Retention period for audit log.....	26
5.4.4. Protection of audit log.....	26
5.4.5. Audit log backup procedures.....	26
5.4.6. Audit collection system (internal vs. external).....	26
5.4.7. Notification to event-causing subject.....	26
5.4.8. Vulnerability assessments.....	26
5.5. RECORDS ARCHIVAL.....	26
5.5.1. Types of records archived.....	26
5.5.2. Retention period for archive.....	26
5.5.3. Protection of archive.....	26
5.5.4. Archive backup procedures.....	26



5.5.5. Requirements for time-stamping of records.....	26
5.5.6. Archive collection system (internal or external).....	26
5.5.7. Procedures to obtain and verify archive information.....	26
5.6. KEY CHANGEOVER.....	27
5.7. COMPROMISE AND DISASTER RECOVERY.....	27
5.7.1. Incident and compromise handling procedures.....	27
5.7.2. Computing resources, software, and/or data are corrupted.....	27
5.7.3. Entity private key compromise procedures.....	27
5.7.4. Business continuity capabilities after a disaster.....	27
5.8. CA OR RA TERMINATION.....	27
<b>6. TECHNICAL SECURITY CONTROLS.....</b>	<b>28</b>
6.1. KEY PAIR GENERATION AND INSTALLATION.....	28
6.1.1. Key pair generation.....	28
6.1.2. Private key delivery to subscriber.....	28
6.1.3. Public key delivery to certificate issuer.....	28
6.1.4. CA public key delivery to relying parties.....	28
6.1.5. Key sizes.....	28
6.1.6. Public key parameters generation and quality checking.....	28
6.1.7. Key Usage Purposes (as per X.509 v3 key usage field).....	28
6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS.....	29
6.2.1. Cryptographic module standards and controls.....	29
6.2.2. Private key (n out of m) multi-person control.....	29
6.2.3. Private key escrow.....	29
6.2.4. Private key backup.....	29
6.2.5. Private key archival.....	29
6.2.6. Private key transfer into or from a cryptographic module.....	29
6.2.7. Private key storage on cryptographic module.....	29
6.2.8. Method of activating private key.....	29
6.2.9. Method of deactivating private key.....	29
6.2.10. Private key destruction method.....	29
6.2.11. Cryptographic Module Rating.....	30
6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT.....	30
6.3.1. Public key file.....	30
6.3.2. Usage period for public and private keys.....	30
6.4. ACTIVATION DATA.....	30
6.4.1. Activation data generation and installation.....	30
6.4.2. Activation data protection.....	30
6.4.3. Other aspects of activation data.....	30



6.5. COMPUTER SECURITY CONTROLS.....	30
6.5.1. <i>Specific computer security technical requirements</i> .....	30
6.5.2. <i>Computer security rating</i> .....	30
6.6. LIFECYCLE TECHNICAL CONTROLS.....	30
6.6.1. <i>System development controls</i> .....	30
6.6.2. <i>Security management controls</i> .....	30
6.6.3. <i>Life cycle security controls</i> .....	31
6.7. NETWORK SECURITY CONTROLS.....	31
6.8. TIME-STAMPING.....	31
<b>7. CERTIFICATE, CRL AND OCSP PROFILES.....</b>	<b>32</b>
7.1. CERTIFICATE PROFILE.....	32
7.1.1. <i>Version number(s)</i> .....	32
7.1.2. <i>Certificate extensions</i> .....	32
7.1.3. <i>Algorithms object identifiers (OID)</i> .....	33
7.1.4. <i>Name forms</i> .....	34
7.1.5. <i>Name constraints</i> .....	34
7.1.6. <i>Certification Policy object identifier (OID)</i> .....	34
7.1.7. <i>Usage of Policy Constraints extension</i> .....	34
7.1.8. <i>Policy qualifiers syntax and semantics</i> .....	35
7.1.9. <i>Processing semantics for the critical Certificate Policies extension</i> .....	35
7.2. CRL PROFILE.....	35
7.2.1. <i>Version number (s)</i> .....	35
7.2.2. <i>CRL and CRL entry extensions</i> .....	35
7.3. OCSP PROFILE.....	35
7.3.1. <i>Version number (s)</i> .....	35
7.3.2. <i>OCSP Extensions</i> .....	35
<b>8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS.....</b>	<b>36</b>
8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT.....	36
8.2. IDENTIFICATION/QUALIFICATION OF ASSESSOR.....	36
8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY.....	36
8.4. TOPICS COVERED BY ASSESSMENT.....	36
8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY.....	36
8.6. COMMUNICATION OF RESULTS.....	36
8.7. SELF-AUDITS.....	36
<b>9. OTHER BUSSINESS AND LEGAL MATTERS.....</b>	<b>37</b>
9.1. FEES.....	37
9.1.1. <i>Certificate issuance or renewal fees</i> .....	37





9.1.2. Certificate access fees.....	37
9.1.3. Revocation or status information access fees.....	37
9.1.4. Fees of other services.....	37
9.1.5. Refund policy.....	37
9.2. FINANCIAL RESPONSIBILITY.....	37
9.2.1. Insurance coverage.....	37
9.2.2. Other assets.....	37
9.2.3. Insurance or warranty coverage for end-entities.....	37
9.3. CONFIDENTIALITY OF BUSINESS INFORMATION.....	37
9.3.1. Scope of confidential information.....	37
9.3.2. Information not within the scope of confidential information.....	37
9.3.3. Responsibility to protect confidential information.....	37
9.4. PRIVACY OF PERSONAL INFORMATION.....	38
9.4.1. Privacy plan.....	38
9.4.2. Information treated as private.....	38
9.4.3. Information not deemed private.....	38
9.4.4. Responsibility to protect private information.....	38
9.4.5. Notice and consent to use private information.....	38
9.4.6. Disclosure pursuant to judicial or administrative process.....	38
9.4.7. Other information disclosure circumstances.....	38
9.5. INTELLECTUAL PROPERTY RIGHTS.....	38
9.6. REPRESENTATIONS AND WARRANTIES.....	38
9.6.1. CA representations and warranties.....	38
9.6.2. RA representations and warranties.....	38
9.6.3. Subscriber representations and warranties.....	38
9.6.4. Relying party representations and warranties.....	38
9.6.5. Representations and warranties of other participants.....	39
9.7. DISCLAIMERS OF WARRANTIES.....	39
9.8. LIMITATIONS OF LIABILITY.....	39
9.8.1. Warranties and its limitations.....	39
9.8.2. Demarcation of responsibilities.....	39
9.8.3. Loss limitations.....	39
9.9. INDEMNITIES.....	39
9.10. TERM AND TERMINATION.....	39
9.10.1. Term.....	39
9.10.2. Termination.....	39
9.10.3. Effect of termination and survival.....	39
9.11. NOTIFICATIONS.....	39
9.12. AMENDMENTS.....	39



9.12.1. Procedure for amendment.....	39
9.12.2. Notification mechanism and period.....	39
9.12.3. Circumstances under which OID must be changed.....	40
9.13. DISPUTE RESOLUTION PROVISIONS.....	40
9.13.1. Resolution of off-court conflicts.....	40
9.13.2. Competent jurisdiction.....	40
9.14. GOVERNING LAW.....	40
9.15. COMPLIANCE WITH APPLICABLE LAW.....	40
9.16. MISCELLANEOUS PROVISIONS.....	40
9.16.1. Entire agreement.....	40
9.16.2. Assignment.....	40
9.16.3. Severability.....	40
9.16.4. Enforcement (attorneys' fees and waiver of rights).....	40
9.16.5. Force Majeure.....	40
9.17. OTHER PROVISIONS.....	40
<b>ANNEX I - CERTIFICATION CONTRACT.....</b>	<b>41</b>
<b>ANNEX II – CERTIFICATE REVOCATION REQUEST FORM.....</b>	<b>44</b>
<b>ANNEX III - VIDEO ID IDENTIFICATION.....</b>	<b>46</b>

# 1. INTRODUCTION

## 1.1. Overview

The current document is the Certification Policy associated to the qualified certificates based on software for citizens, which contains the rules of management and use the certificates issued within this Certificate Policy. It also describes the roles, responsibilities and relationships between the end user and the Electronic Certification and Technology Agency, and the rules for request, acquisition and generation of the certificate. This document qualifies and complements the Certification Practices Statement (CPS) of the Agencia de Tecnología y Certificación Electrónica.

The Certification Policy that is referred in this document will be used for the issuance of qualified certificates based on software for citizens, following the legislation in force.

The current Certification Policy is drafted following the RFC 3674 “*Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*” specifications, proposed by *Network Working Group* for this type of documents, the same as the Certification Practices Statement, to ease the reading or comparison with counterparts documents.

This Certification Policy assumes that the reader has basic knowledge about the Public Key Infrastructure, digital certificates and signature concepts, otherwise the reader is recommended to be trained in these concepts before continuing reading the current document.

## 1.2. Identification

Policy Name	Certification Policy for Qualified Certificates in software support for Citizens
Policy Qualifier	Certificado cualificado para Ciudadano expedido por la ACCV (Pol. Ademuz, s/n. Burjassot, CP 46100, ESPAÑA. CIF A40573396)
Policy version	8.0.2
Policy status	APPROVED
Policy Reference / OID (Object Identifier)	1.3.6.1.4.1.8149.3.7.8.0
Date of issuance	February 12, 2024
Date of expiration	Not applicable.
Related CPS	Certification Practices Statement (CPS) of the ACCV. Version 5.0. OID: 1.3.6.1.4.1.8149.2.5.0 Available at <a href="http://www.accv.es/pdf-politicas">http://www.accv.es/pdf-politicas</a>
Location	This Certification Policy can be found at: <a href="http://www.accv.es/legislacion c.htm">http://www.accv.es/legislacion c.htm</a>

## 1.3. PKI participants

### 1.3.1. Certification Authorities

The CAs that can issue certificates in accordance with this policy are ACCV RSA1 CLIENTE and ACCV ECC1 CLIENTE belonging to the Agencia de Tecnología y Certificación Electrónica, whose function is to issue end-entity certificates for ACCV subscribers. The choice of one or another CA will depend on the type of keys used for the issuance of final certificates: RSA or ECDSA.

Qif.: PUBLIC	Ref.: ACCV-CP-07V8.0.2-EN-2024.odt	Version: 8.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.8.0	Pg. 11 of 55

ACCV RSA1 CLIENTE and ACCV ECC1 CLIENTE certificates are valid from July 25, 2023 to July 19, 2047.

### 1.3.2. Registration Authorities

The list of Registration Authorities (User Register Points) that manage the certificate requests that are defined in this policy is located at <https://www.accv.es>.

### 1.3.3. Subscribers

The group of users that can apply for the certificates that are defined in this policy, is made up of any natural person who possess the required identification elements (DNI, NIE, etc.).

The keys and certificates is based on software, non cryptographic storage.

The right to request certificates that are defined in this Certification Policy is limited to natural persons. Certification requests that are carried out in name of legal body, entity or organization, will not be accepted.

### 1.3.4. Relying parts

The right to trust in certificates that are issued in accordance with this policy, is limited to:

1. Applications and services belonging to the Generalitat, to any of the entities or organizations linked to the Generalitat or to Public or Corporate Administrations with which a certification agreement has been signed.
2. The applications and services of any Public Administration.
3. The applications or services of any public or private entity that requires a secure electronic identification or the citizens digital signature.

### 1.3.5. Other participants

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

## 1.4. Certificates usage

### 1.4.1. Appropriate certificate uses

The certificates that are issued by the Agencia de Tecnología y Certificación Electrónica under this Certification Policy, can be used for the electronic signature of any information or document. Likewise, they can be used as an identification mechanism in services and applications.

### 1.4.2. Prohibited certificate uses

The certificates will be used only in accordance with the purpose and function established in this Certification Policy, and with the existing regulatory framework.

## 1.5. Policy administration

### 1.5.1. Organization administering the document

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

Qif.: <b>PUBLIC</b>	Ref.: ACCV-CP-07V8.0.2-EN-2024.odt	Version: 8.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.8.0	Pg. 12 of 55



### 1.5.2. Contact person

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

### 1.5.3. Person determining CPS suitability for the policy

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

### 1.5.4. CPS approval procedures

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

## 1.6. Definitions and Acronyms

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

Qif.: <b>PUBLIC</b>	Ref.: ACCV-CP-07V8.0.2-EN-2024.odt	Version: 8.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.8.0	Pg. 13 of 55

## 2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

### 2.1. Repositories

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

### 2.2. Publication of certification information

In addition to what is specified in the Certification Practices Statement (CPS), ACCV conforms to the [current version](#) of the “*Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates*”, published at <https://www.cabforum.org/>. In the event of any inconsistency between this Certification Policy and the CAB Forum requirements, those requirements take precedence over the current document.

### 2.3. Time or frequency of publication

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

### 2.4. Access controls on repositories

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

Qif.: <b>PUBLIC</b>	Ref.: ACCV-CP-07V8.0.2-EN-2024.odt	Version: 8.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.8.0	Pg. 14 of 55

## 3. Identification and Authentication

### 3.1. Naming

#### 3.1.1. Types of names

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

#### 3.1.2. Need for names to be meaningful

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

#### 3.1.3. Anonymity or pseudonymity of subscribers

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

#### 3.1.4. Rules for interpreting various name forms

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

#### 3.1.5. Uniqueness of names

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

#### 3.1.6. Recognition, authentication, and role of trademarks

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

### 3.2. Initial identity validation

#### 3.2.1. Method to prove possession of private key

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

#### 3.2.2. Authentication of organization identity

The right to request the certificates that are defined in this Certification Policy is limited to natural persons. Certification requests made on behalf of legal bodies, entities or organization will not be accepted. Therefore, any organization identification will not be necessary.

#### 3.2.3. Authentication of individual identity

Authentication of the identity of the applicant for a certificate will be done by identification with the corresponding Registration Authority. In the case of presenting on site with a Registration Point Operator enabled for the issuance of this type of certificate, the identity must be accredited by presenting the National Identity Document (DNI), Spanish passport, the Foreigner Identification Number (NIE) of the applicant or other means admitted in Law. The presenting on site of the applicant may be dispensed using a power of attorney explicitly delegating the obtaining of the certificate to third party. In the case of non on site identification with the Registration Authority, the applicant will access the Personal Certification Services Area (APSC) by identifying himself through a qualified personal certificate of the ACCV or the DNLe.

In the case of video identification mechanisms, it is necessary that the evidences are the same and have the same probative value of identity (same quality). The use of identity verification systems through video identification is conditioned to the corresponding legal basis and associated technical

Qif.: <b>PUBLIC</b>	Ref.: ACCV-CP-07V8.0.2-EN-2024.odt	Version: 8.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.8.0	Pg. 15 of 55



regulations. In the event that this type of mechanism can be used, a complete description of the solution will be included in Annex III of this policy.

#### 3.2.4. Non-verified subscriber information

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

#### 3.2.5. Validation of authority

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

#### 3.2.6. Criteria for interoperation

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

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

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

The identification and authentication for routine re-key can be carried out using the techniques of initial authentication and identification (described at point 3.2.3. *Authentication of individual identity* of this Certification Policy). In case of remote identification in front of the Registration Authority, the user will access to the Personal Area of the Certification Services (APSC) identifying himself/herself with a personal qualified certificate of the ACCV or the DNle.

#### 3.3.2. Identification and authentication for re-key after revocation – Not compromised key.

The identification and authentication policy for certificate renewal following a revocation without key compromise shall be the same as for initial registration. In the case of finding insurmountable technical problems, ACCV can implement any method that guarantees in a reliable and unequivocal way the applicant identity and the application authentication, explaining in detail each step of the process.

### 3.4. Identification and authentication for revocation request

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

- On-site processing. The same method as for the initial register described at point 3.2.3. *Authentication of an individual identification*, in this Certification Policy.
- Web. Using the Personal Area of the Certification Services (APSC) at <https://www.accv.es>.
- Phone. By answering the questions of the Call Center support, available at the 963 866 014 phone number.

ACCV or any entity that makes it up, can ex-officio apply for a certificate revocation if they have knowledge or suspect about the subscriber's private key compromise, or any other fact that would recommend to carry out this action.

Qif.: PUBLIC	Ref.: ACCV-CP-07V8.0.2-EN-2024.odt	Version: 8.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.8.0	Pg. 16 of 55



## 4. Certificate life-cycle operational requirements

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

### 4.1. Certificates Application

#### 4.1.1. Who can submit a certificate application

Those subscribers listed in point 1.3.3 can submit a certificate application.

#### 4.1.2. Enrollment Process and Responsibilities

The citizen applying for a certificate issued under this policy must go to the ACCV's Registration Authority, presenting the necessary documentation established in this policy (point 3.2.3).

The list of authorized Registration Authorities is located at <https://www.accv.es>.

In the case of on-site applications, the application data is extracted from official documentation provided by the applicant, and it is the responsibility of the ACCV to verify the data and ensure the availability of the registration authorities and associated systems, as well as to inform the applicant of the different statuses through which the application passes. It is the applicant's responsibility to provide accurate information in their application.

In the case of video identification mechanisms, it is necessary that the evidences are the same and have the same probative value of identity (same quality). The use of identity verification systems through video identification is conditioned to the corresponding legal basis and associated technical regulations. In the event that this type of mechanism can be used, a complete description of the solution will be included in Annex III of this policy. This type of identification is equivalent to on-site identification at a registration point.

In the case of remote applications without interactive identity identification (using a qualified personal certificate) the data is obtained from the information available in the digital medium used to identify the applicant, and it is the responsibility of the ACCV to verify the data and ensure the availability of the registration authorities and associated systems, as well as to inform the applicant of the different statuses through which the application passes. It is the applicant's responsibility to provide accurate information in their application.

Likewise in case of certificate request through remote means, a period of time lower than five years will be demanded since the on-site identification.

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

### 4.2. Certificate application processing

The Registration Authority is the entity competence in charge of checking the applicant identity, to verify the documentation and validate that the applicant has signed the certification contract. Once the request is completed, the Registration Authority will remit it to ACCV.

#### 4.2.1. Performing identification and authentication functions

Authentication of the identity of the applicant for a certificate will be done by identification with the corresponding Registration Authority using the mechanisms described in section 3.2.3 Authentication of individual identity. Registration Authority Operator checks the documentation and validates the data using publicly accessible records for such verification.

Qlf.: <b>PUBLIC</b>	Ref.: ACCV-CP-07V8.0.2-EN-2024.odt	Version: 8.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.8.0	Pg. 17 of 55



#### 4.2.2. Approval or rejection of certificate applications

In case of acceptance, Registration Authority will notify the applicant through an electronic mail to the email address that is listed in the request.

In face-to-face applications, the Registration Authority will inform the user of acceptance or rejection directly, providing an alphanumeric code of sufficient length. This code can be sent electronically using verified means in possession of the applicant (preferred mechanism) or by printing it and delivering it on paper to the applicant.

In remote applications the applicant must access the Personal Area of Certification Services (remote Registration Authority) with a personal certificate or the DNle. If the applicant is able to make the application, the corresponding option will be shown.

In case of rejection the Registration Authority will inform the applicant using the corresponding mechanisms. For on-site applications the Operator shall inform the user directly of the rejection and the reason for it. In remote applications the Registration Authority will inform the user in an interactive way preventing the continuation of the process.

ACCV will use this information to decide on new applications.

#### 4.2.3. Time to process certificate applications

Maximum time to process certificate applications is five working days.

### 4.3. Certificates issuance

ACCV is not responsible for the monitoring, investigation or confirmation about the accuracy of the information that is contained in the certificate subsequently to its issuance. In case of receiving information about the inaccuracy or the current non-applicability of the information that is collected in the certificate, this one can be revoked.

The issuance of the certificate will be made when the ACCV has carried out the necessary verification to validate the certification request and in the presence of the applicant. The mechanism that determines the nature and manner of performing such verification is this Certification Policy.

When the ACCV issues a certificate in accordance with a valid certification request, it will send a copy of certificate to the RA that remitted the request and another copy to the ACCV repository.

RA will notify the subscriber of the certificate issuance and will provide the certificate or means to obtain it.

#### 4.3.1. CA actions during certificate issuance

The certificate issuance takes place once the RA has carried out the necessary verification for validating the certification request. The mechanism that determines the nature and form of performing these checks is this Certification Policy.

- The applicant identifies itself to the Registration Authority using the mechanisms and codes provided upon acceptance of the application.
- The Registration Authority requires the applicant to create the key pair and the CSR using the parameters defined in this policy.
- The applicant sends the CSR to the Registration Authority who verifies the format and checks the signature. Once verified if everything is correct, it is encapsulated in a request and signed, sending it to the Certification Authority.
- The Certification Authority validates all signatures and the format and parameters of the CSR. If everything is correct, it signs the CSR and returns the certificate to the Registration Authority.
- The Registration Authority communicates the certificate to the applicant.

Qif.: <b>PUBLIC</b>	Ref.: ACCV-CP-07V8.0.2-EN-2024.odt	Version: 8.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.8.0	Pg. 18 of 55



All these processes are done in the generation platform provided by the ACCV.

#### 4.3.2. Notification to subscriber by the CA of issuance of certificate

ACCV notifies the subscriber about the issuance of certificate, through an electronic mail to the email address provided in the application process.

### 4.4. Certificates acceptance

#### 4.4.1. Conduct constituting certificate acceptance

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

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

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

#### 4.4.2. Publication of the certificate by the CA

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

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

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

### 4.5. Key pair and certificate usage

#### 4.5.1. Subscriber private key and certificate usage

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

#### 4.5.2. Relying party public key and certificate usage

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

### 4.6. Certificate renewal

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

#### 4.6.1. Circumstance for certificate renewal

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

#### 4.6.2. Who may request renewal

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

#### 4.6.3. Processing certificate renewal requests

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

Qlf.: <b>PUBLIC</b>	Ref.: ACCV-CP-07V8.0.2-EN-2024.odt	Version: 8.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.8.0	Pg. 19 of 55

#### 4.6.4. Notification of new certificate issuance to subscriber

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

#### 4.6.5. Conduct constituting acceptance of a renewal certificate

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

#### 4.6.6. Publication of the renewal certificate by the CA

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

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

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

### 4.7. Certificate re-key

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

#### 4.7.1. Circumstance for certificate re-key

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

#### 4.7.2. Who may request certification of a new public key

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

#### 4.7.3. Processing certificate re-keying requests

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

#### 4.7.4. Notification of new certificate issuance to subscriber

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

#### 4.7.5. Conduct constituting acceptance of a re-keyed certificate

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

#### 4.7.6. Publication of the re-keyed certificate by the CA

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

#### 4.7.7. Notification of certificate issuance by the CA to other entities

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

### 4.8. Certificate modification

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

#### 4.8.1. Circumstance for certificate modification

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

Qif.: <b>PUBLIC</b>	Ref.: ACCV-CP-07V8.0.2-EN-2024.odt	Version: 8.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.8.0	Pg. 20 of 55

#### 4.8.2. Who may request certificate modification

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

#### 4.8.3. Circumstance for certificate modification

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

#### 4.8.4. Notification of new certificate issuance to subscriber

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

#### 4.8.5. Conduct constituting acceptance of modified certificate

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

#### 4.8.6. Publication of the modified certificate by the CA

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

#### 4.8.7. Notification of certificate issuance by the CA to other entities

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

### 4.9. Certificate revocation and suspension

#### 4.9.1. Circumstances for revocation

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

#### 4.9.2. Who can request revocation

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

#### 4.9.3. Procedure for revocation request

The Agencia de Tecnología y Certificación Electrónica accepts revocation requests by the following methods:

##### 4.9.3.1. On-site processing

By the subscriber appearance and identification in a RA and by signing and filling the “Revocation Request Form” that will be provided to him/her and which copy is included in the Annex II of this document.

##### 4.9.3.2. Web

There exists a certificate revocation request form at the ACCV web, at <http://www.accv.es> URL.

##### 4.9.3.3. Phone

Through a phone call to the phone support number of the Agencia de Tecnología y Certificación Electrónica, which is 963 866 014.

#### 4.9.4. Revocation request grace period

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

Qif.: PUBLIC	Ref.: ACCV-CP-07V8.0.2-EN-2024.odt	Version: 8.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.8.0	Pg. 21 of 55



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

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

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

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

#### 4.9.7. CRL issuance frequency

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

#### 4.9.8. Maximum latency for CRLs

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

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

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

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

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

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

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

#### 4.9.12. Special requirements re key compromise

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

#### 4.9.13. Circumstances for the suspension

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

#### 4.9.14. Who can request suspension

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

#### 4.9.15. Procedure for the suspension request

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

#### 4.9.16. Limits of suspension period

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

### 4.10. Certificate status services

#### 4.10.1. Operational Characteristics

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

#### 4.10.2. Service Availability

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

Qif.: <b>PUBLIC</b>	Ref.: ACCV-CP-07V8.0.2-EN-2024.odt	Version: 8.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.8.0	Pg. 22 of 55



#### 4.10.3. Optional features

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

#### 4.11. End of subscription

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

ACCV will inform the subscriber about the certificate revocation, through a email in a previous moment prior to the certificate disclosure in the Certificate Revocation List, specifying the reasons, date and time the certificate will lose its efficacy and notifying about its non-continuing usage.

#### 4.12. Key escrow and recovery

##### 4.12.1. Key escrow and recovery policy and practices

ACCV does not escrow private keys issued under this Policy.

##### 4.12.2. Session key encapsulation and recovery policy and practices

Session key recovery is not supported.

Qif.: <b>PUBLIC</b>	Ref.: ACCV-CP-07V8.0.2-EN-2024.odt	Version: 8.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.8.0	Pg. 23 of 55



## 5. Facility, management, and operational controls

### 5.1. Physical Controls

#### 5.1.1. Site location and construction

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

#### 5.1.2. Physical access

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

#### 5.1.3. Power and air conditioning

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

#### 5.1.4. Water exposure

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

#### 5.1.5. Fire prevention and protection

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

#### 5.1.6. Media storage

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

#### 5.1.7. Waste disposal

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

#### 5.1.8. Off-site backup

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

### 5.2. Procedural Controls

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

#### 5.2.1. Trusted roles

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

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

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

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

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

Qif.: <b>PUBLIC</b>	Ref.: ACCV-CP-07V8.0.2-EN-2024.odt	Version: 8.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.8.0	Pg. 24 of 55





#### 5.2.4. Roles requiring separation of duties

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

### 5.3. Personnel controls

This chapter reflects the content of the *Personal Security Controls* document of the ACCV.

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

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

#### 5.3.2. Background check procedures

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

#### 5.3.3. Training requirements

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

#### 5.3.4. Retraining frequency and requirements

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

#### 5.3.5. Job rotation frequency and sequence

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

#### 5.3.6. Sanctions for unauthorized actions

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

#### 5.3.7. Independent contractor requirements

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

#### 5.3.8. Documentation supplied to personnel

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

#### 5.3.9. Periodical compliance controls

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

#### 5.3.10. End of contracts

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

### 5.4. Audit logging procedures

#### 5.4.1. Types of events recorded

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

Qif.: <b>PUBLIC</b>	Ref.: ACCV-CP-07V8.0.2-EN-2024.odt	Version: 8.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.8.0	Pg. 25 of 55

#### 5.4.2. Frequency of processing log

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

#### 5.4.3. Retention period for audit log

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

#### 5.4.4. Protection of audit log

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

#### 5.4.5. Audit log backup procedures

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

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

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

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

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

#### 5.4.8. Vulnerability assessments

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

### 5.5. Records archival

#### 5.5.1. Types of records archived

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

#### 5.5.2. Retention period for archive

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

#### 5.5.3. Protection of archive

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

#### 5.5.4. Archive backup procedures

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

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

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

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

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

#### 5.5.7. Procedures to obtain and verify archive information

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

Qif.: <b>PUBLIC</b>	Ref.: ACCV-CP-07V8.0.2-EN-2024.odt	Version: 8.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.8.0	Pg. 26 of 55

## 5.6. Key changeover

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

## 5.7. Compromise and disaster recovery

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

### 5.7.1. Incident and compromise handling procedures

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

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

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

### 5.7.3. Entity private key compromise procedures

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

### 5.7.4. Business continuity capabilities after a disaster

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

## 5.8. CA or RA termination

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

## 6. Technical security controls

### 6.1. Key pair generation and installation

This point is always referred to the keys that are generated for the certificates that were issued over the scope of the current Certification Policy. The information about the keys of entities that make up the Certification Authority are found at point 6.1 of the Certification Practices Statement (CPS) of the Agencia de Tecnología y Certificación Electrónica.

#### 6.1.1. Key pair generation

The key pair for the certificate that is issued under the scope of this Certification Policy can be generated in two places; the subscriber workstation in a process of self-generation without leaving the system.

#### 6.1.2. Private key delivery to subscriber

The private key for the certificates that are issued under the scope of this Certification Policy are placed at the subscriber workstation where the key pair was generated.

#### 6.1.3. Public key delivery to certificate issuer

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

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

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

#### 6.1.5. Key sizes

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

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

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

The parameters defined in the ETSI TS 119 312 document "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
ecdsa-with-SHA256	sha256		ecdsa

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

The certificates issued under the present policy contain the attributes

"KEY USAGE" and "EXTENDED KEY USAGE", as defined in the X.509v3 standard.

Qif.: <b>PUBLIC</b>	Ref.: ACCV-CP-07V8.0.2-EN-2024.odt	Version: 8.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.8.0	Pg. 28 of 55

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

The detailed definition of the certificate profile and the usage of keys is located in the section 7 of this document "*Certificate profiles, CRL and OCSP*".

## 6.2. Private Key Protection and Cryptographic Module Engineering Controls

This chapter is always referred to the keys that are generated for the certificates issued under the scope of this Certification Policy. The information about the keys of entities that make the Certification Authority up, is included in the chapter 6.2 of the Certification Practices Statement (CPS) of the ACCV.

### 6.2.1. Cryptographic module standards and controls

The certificates issued under this Certificate Policy are software based, so the cryptographic module standards and controls depend on the subscriber's OS.

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

The private keys for the signature certificates issued within the scope of this Certification Policy is under the sole control of their subscribers.

### 6.2.3. Private key escrow

ACCV never escrows keys with usages of Digital Signature or Content Commitment.

### 6.2.4. Private key backup

ACCV never backups keys with usages of Digital Signature or Content Commitment.

### 6.2.5. Private key archival

ACCV never archives keys with usages of Digital Signature or Content Commitment.

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

The Key pair is based on software. There is not cryptographic devices.

### 6.2.7. Private key storage on cryptographic module

The Key pair is based on software. There is not cryptographic devices.

### 6.2.8. Method of activating private key

In case of keys auto-generation, the activation method is established by the user in the moment of generation.

### 6.2.9. Method of deactivating private key

The deactivation will be performed by closing the application that uses it.

### 6.2.10. Private key destruction method

Destruction must always be preceded by revocation of the certificate associated with the private key, If the key is still active.

The task to be performed consists of deleting the container of the private key.

Qlf.: <b>PUBLIC</b>	Ref.: ACCV-CP-07V8.0.2-EN-2024.odt	Version: 8.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.8.0	Pg. 29 of 55

### 6.2.11. Cryptographic Module Rating

See section Cryptographic module standards and controls of this Certification Policy.

## 6.3. Other aspects of key pair management

### 6.3.1. Public key file

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

### 6.3.2. Usage period for public and private keys

The certificates that are issued within the scope of this policy are valid for three (3) years.

The key pair that is used for the certificates issuance is created for every issuance, and therefore are valid for three (3) years.

The ACCV RSA1 CLIENTE and ACCV ECC1 CLIENTE certificates are valid from July 25, 2023 to July 19, 2047.

## 6.4. Activation data

### 6.4.1. Activation data generation and installation

In case of keys auto-generation the activation mechanism is established by the user in the moment of generation. The subscriber has the responsibility and obligation to chose the appropriate security mechanisms and maintain the private key under his/her sole control.

### 6.4.2. Activation data protection

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

### 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

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

### 6.5.2. Computer security rating

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

## 6.6. Lifecycle Technical Controls

### 6.6.1. System development controls

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

### 6.6.2. Security management controls

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

Qlf.: <b>PUBLIC</b>	Ref.: ACCV-CP-07V8.0.2-EN-2024.odt	Version: 8.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.8.0	Pg. 30 of 55



### 6.6.3. Life cycle security controls

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

## 6.7. Network Security Controls

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

## 6.8. Time-stamping

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

Qlf.: <b>PUBLIC</b>	Ref.: ACCV-CP-07V8.0.2-EN-2024.odt	Version: 8.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.8.0	Pg. 31 of 55

## 7. Certificate, CRL and OCSP profiles

### 7.1. Certificate Profile

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

#### 7.1.1. Version number(s)

In addition to what is established in the ACCV Certification Practices Statement (CPS), this certification policy specifies the use of a certificate with two uses; digital signature and authentication.

#### 7.1.2. Certificate extensions

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

Field	Value
<b>Subject</b>	
SerialNumber	Subscriber DNI or NIE. 9 characters filled with zeros on the left side
GivenName	Subscriber name, as it is in the DNI or NIE
SurName	Subscriber surname as it is in the DNI or NIE
CommonName	String composed in the following manner: NAME SURNAME1 SURNAME2 – NIF:SUBSCRIBERSNIF
OrganizationalUnit	Ciudadanos
Country	ES
<b>Version</b>	V3
<b>SerialNumber</b>	Certificate unique identifier (32 hexadecimal characters)
<b>Signature algorithm</b>	ACCV_RSA1_CLIENTE sha256withRSAEncryption ACCV_ECC1_CLIENTE ecdsa-with-SHA256
<b>Issuer</b>	DN of the CA issuing the certificate (see point 7.1.4)
<b>Valid since</b>	Date of issuance
<b>Valid until</b>	Date of expiration
<b>Public key</b>	Octet String containing the subscriber public key
<b>Extended Key Usage</b>	Client Authentication Adobe Authentic Documents Trust (1.2.840.113583.1.1.5)
<b>CRL Distribution Point</b>	ACCV_RSA1_CLIENTE: <a href="http://www.accv.es/gestcert/accv_rsa1_cliente.crl">http://www.accv.es/gestcert/accv_rsa1_cliente.crl</a> ACCV_ECC1_CLIENTE: <a href="http://www.accv.es/gestcert/accv_ecc1_cliente.crl">http://www.accv.es/gestcert/accv_ecc1_cliente.crl</a>
<b>SubjectAlternativeName</b>	
DirectoryName	
	CN=Name Surname1 Surname2
	UID=NIF
<b>Certificate Policy Extensions</b>	



Policy OID	QCP-n: certificate policy for EU qualified certificates issued to natural persons;  Itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural(0)	
Policy OID	1.3.6.1.4.1.8149.3.7.8.0	
Policy CPS Location	<a href="http://www.accv.es/legislacion_c.htm">http://www.accv.es/legislacion_c.htm</a> *	
Policy Notice	Certificado cualificado para Ciudadano expedido por la ACCV (Pol. Ademuz, s/n. Burjassot, CP 46100, ESPAÑA. CIF A40573396)	
<b>Authority Information Access</b>		
Access Method	Id-ad-ocsp	
Access Location	<a href="http://ocsp.accv.es">http://ocsp.accv.es</a>	
Access Method	Id-ad-caIssuers	
Access Location	<u>ACCV RSA1 CLIENTE: <a href="http://www.accv.es/gestcert/accv_rsa1_cliente.crt">http://www.accv.es/gestcert/accv_rsa1_cliente.crt</a></u> <u>ACCV ECC1 CLIENTE: <a href="http://www.accv.es/gestcert/accv_ecc1_cliente.crt">http://www.accv.es/gestcert/accv_ecc1_cliente.crt</a></u>	
<b>Fingerprint issuer</b>	Fingerprint of the certificate of the CA issuing the certificate (see CPS)	
<b>Algoritmo de hash</b>	SHA-256	
<b>KeyUsage (críticos)</b>		
	<b>RSA</b> Digital Signature Non-repudiation Key encipherment	<b>ECC</b> Digital Signature Non-repudiation Key agreement
<b>QcStatement (only certificates of signature)</b>	<b>Fields QC (Qualified Certificate)</b>	<b>QcStatement</b>
QcCompliance		The certificate is qualified
QcType	eSign	Particular type of qualified certificate
QcRetentionPeriod	15y	Retention period of the material information
QcPDS	<a href="https://www.accv.es/fileadmin/Archivos/Practicas_de_certificacion/ACCV-PDS-V1.1-EN.pdf">https://www.accv.es/fileadmin/Archivos/Practicas_de_certificacion/ACCV-PDS-V1.1-EN.pdf</a>	Location of PKI Disclosure Statement

*\*The existence of valid certificates that were issued with the pki.gva URL instead of accv.es is dismissed. The change from one URL to another is a gradual process which does not involve significant differences in the profile, neither the certificates functionality or its usage.*

### 7.1.3. Algorithms object identifiers (OID)

Object identifier (OID) of cryptography algorithms:

- SHA1withRSA (1.2.840.113549.1.1.5)

Qif.: <b>PUBLIC</b>	Ref.: ACCV-CP-07V8.0.2-EN-2024.odt	Version: 8.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.8.0	Pg. 33 of 55



- SHA256withRSA (1.2.840.113549.1.1.11)
- ecdsa-with-SHA256 (1.2.840.10045.4.3.2)

#### 7.1.4. Name forms

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

The Issuer names admitted for certificates issued under this policy are:

- cn=ACCV RSA1 CLIENTE,2.5.4.97=VATES-A40573396,o=ISTEC,l=BURJASSOT,s=VALENCIA,c=ES
- cn=ACCV ECC1 CLIENTE,2.5.4.97=VATES-A40573396,o=ISTEC,l=BURJASSOT,s=VALENCIA,c=ES

All the fields of the certificate of the Subject and the Subject Alternative Name, excepting those that regard DNS name or mail addresses, are obligatory filled with capital letters and without accents.

SubjectAlternativeName contain at least the subscriber's first and last name separated by the character "|" (DirectoryName).

Subject:

commonName (required). String composed in the following manner NAME SURNAME1 SURNAME2 – NIF:SUBSCRIBER NIF

GivenName Subscriber name, as it is in the DNI or NIE

SurName Subscriber surname as it is in the DNI or NIE

serialNumber (required). Subscriber DNI or NIE. 9 characters filled with zeros on the left side

OrganizationalUnit (required) fixed string "CIUDADANOS"

country (required) Country code ISO 3166-1

#### 7.1.5. Name constraints

The names contained in the certificates are restricted to distinguished names X.500, unique and unambiguous.

The rest of fields included in the certificate are strictly necessary and are marked in the RFC-3739 for the obtainment of a qualified certificate profile.

#### 7.1.6. Certification Policy object identifier (OID)

The object identifier defined by the ACCV for identifying the current policy is the following:

**1.3.6.1.4.1.8149.3.7.8.0**

In this case an OID is added for identifying the type of entity that is represented according to the ETSI TS 119 411-2 normative.

**0.4.0.194112.1.0**

**Certification policy for EU qualified certificates in software support issued for natural persons**

#### 7.1.7. Usage of Policy Constraints extension

The Policy Constraint extension is not used in the certificates issued under this Certification Policy.

Qif.: PUBLIC	Ref.: ACCV-CP-07V8.0.2-EN-2024.odt	Version: 8.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.8.0	Pg. 34 of 55

### 7.1.8. Policy qualifiers syntax and semantics

The Certificate Policies extension can include two Policy Qualifier fields (both optional):

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

User notice: contains a description text

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

The extension “Certificate Policy” identifies the policy which defines the practices that the ACCV explicitly associates with the certificate. In addition the extension can contain a policy qualifier.

## 7.2. CRL profile

### 7.2.1. Version number (s)

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

### 7.2.2. CRL and CRL entry extensions

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

## 7.3. OCSP profile

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

### 7.3.1. Version number (s)

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

### 7.3.2. OCSP Extensions

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

Qlf.: <b>PUBLIC</b>	Ref.: ACCV-CP-07V8.0.2-EN-2024.odt	Version: 8.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.8.0	Pg. 35 of 55



## 8. Compliance audit and other assessments

### 8.1. Frequency or Circumstances of Assessment

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

### 8.2. Identification/qualification of Assessor

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

### 8.3. Assessor's Relationship to Assessed Entity

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

### 8.4. Topics Covered by Assessment

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

### 8.5. Actions Taken as a Result of Deficiency

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

### 8.6. Communication of results

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

### 8.7. Self-Audits

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

Qlf.: <b>PUBLIC</b>	Ref.: ACCV-CP-07V8.0.2-EN-2024.odt	Version: 8.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.8.0	Pg. 36 of 55

## 9. Other bussiness and legal matters

### 9.1. Fees

#### 9.1.1. Certificate issuance or renewal fees

The fees for the initial issuance and certificates renovation are collected in the Agencia de Tecnología y Certificación Electrónica Fees List. This list is disclosed in the ACCV web page <https://www.accv.es>.

#### 9.1.2. Certificate access fees

The access to the certificates issued within this certification policy is free and therefore there is no applicable fee over it.

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

The access to the status or revocation information of the certificates is free and therefore, the is no applicable fee over it.

#### 9.1.4. Fees of other services

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

#### 9.1.5. Refund policy

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

## 9.2. Financial responsibility

### 9.2.1. Insurance coverage

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

### 9.2.2. Other assets

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

### 9.2.3. Insurance or warranty coverage for end-entities

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

## 9.3. Confidentiality of business information

### 9.3.1. Scope of confidential information

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

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

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

### 9.3.3. Responsibility to protect confidential information

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

Qlf.: <b>PUBLIC</b>	Ref.: ACCV-CP-07V8.0.2-EN-2024.odt	Version: 8.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.8.0	Pg. 37 of 55



## 9.4. Privacy of personal information

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

### 9.4.1. Privacy plan

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

### 9.4.2. Information treated as private

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

### 9.4.3. Information not deemed private

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

### 9.4.4. Responsibility to protect private information

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

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

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

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

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

### 9.4.7. Other information disclosure circumstances

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

## 9.5. Intellectual property rights

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

## 9.6. Representations and warranties

### 9.6.1. CA representations and warranties

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

### 9.6.2. RA representations and warranties

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

### 9.6.3. Subscriber representations and warranties

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

### 9.6.4. Relying party representations and warranties

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

Qif.: <b>PUBLIC</b>	Ref.: ACCV-CP-07V8.0.2-EN-2024.odt	Version: 8.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.8.0	Pg. 38 of 55

#### 9.6.5. Representations and warranties of other participants

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

### 9.7. Disclaimers of warranties

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

### 9.8. Limitations of liability

#### 9.8.1. Warranties and its limitations

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

#### 9.8.2. Demarcation of responsibilities

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

#### 9.8.3. Loss limitations

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

### 9.9. Indemnities

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

### 9.10. Term and termination

#### 9.10.1. Term.

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

#### 9.10.2. Termination.

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

#### 9.10.3. Effect of termination and survival

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

### 9.11. Notifications.

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

### 9.12. Amendments

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

#### 9.12.1. Procedure for amendment

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

#### 9.12.2. Notification mechanism and period

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

Qif.: <b>PUBLIC</b>	Ref.: ACCV-CP-07V8.0.2-EN-2024.odt	Version: 8.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.8.0	Pg. 39 of 55

### 9.12.3. Circumstances under which OID must be changed

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

## 9.13. Dispute resolution provisions

### 9.13.1. Resolution of off-court conflicts

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

### 9.13.2. Competent jurisdiction

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

## 9.14. Governing law

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

## 9.15. Compliance with applicable law

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

## 9.16. Miscellaneous provisions

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

### 9.16.1. Entire agreement

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

### 9.16.2. Assignment

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

### 9.16.3. Severability

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

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

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

### 9.16.5. Force Majeure

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

## 9.17. Other provisions

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

Qif.: <b>PUBLIC</b>	Ref.: ACCV-CP-07V8.0.2-EN-2024.odt	Version: 8.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.8.0	Pg. 40 of 55







**CERTIFICATION CONTRACT - OID 1.3.6.1.4.1.8149.3.7**

**Conditions of use**

1. The certificates that are associated to the Certification Policy for Qualified Certificates based on software for Citizens, issued by the Agencia de Tecnología y Certificación Electrónica are X.509v3 type and they follow the Certification Practices Statement of the Agencia de Tecnología y Certificación Electrónica, as Qualified Certification Services Provider, and the mentioned Certification Policy. Both documents must be interpreted in accordance with the European law, the Spanish Juridic Order and the Valencian legislation.
2. The applicant must be natural person, with a NIF, NIE or any other identification document valid in Law.
3. The applicant is responsible for the veracity of all the data provided in the registration process. He/she will be responsible for communicating any change in the submitted data.
4. The subscriber is responsible for the custody of the signature creation data, and for communicating as soon as possible about any loss or subtraction of this data.
5. The subscriber is responsible for restricting the certificate usage to what is established in the regarding Certification Policy, which is a public document and it can be found at <https://www.accv.es>
6. The Agencia de Tecnología y Certificación Electrónica is not responsible for the content of the documents that are signed using the certificates that it issues.
7. The Agencia de Tecnología y Certificación Electrónica is responsible for the accomplishment of the European, Spanish and Valencian legislation, as far as electronic signature is concerned. It is, therefore, responsible for the accomplishment of what is established in the Certification Practices Statement of the Agencia de Tecnología y Certificación Electrónica and in the Certification Policy that is associated to this type of certificates.
8. The period of validity of these certificates is for three (3) years. The renewal uses the same process as for the first request or the procedures that are provided in the associated Certification Policy.
9. The issued certificates will lose their validity, in addition to the end of the official period of validity, when a revocation is produced, when the signature creation data store is broken, because of a judicial or administrative resolution that orders the validity loss, because of errors in the submitted data by the applicant or because of the subscriber decease. Other conditions for the validity loss are collected in the Certification Practices Statement and in the Certification Policy that is associated to this type of certificate.
10. The documentation to be submitted for the applicant identification will be the Identity National Document, NIE or Spanish passport, valid and in force.
11. In accomplishment with the Organic Law 3/2018 December 5, of Personal Data Protection, the applicant is informed about the existence of an automated file of personal data, created under the responsibility of the Agencia de Tecnología y Certificación Electrónica. The purpose of this file is to serve to the uses related to the certification services that the Agencia de Tecnología y Certificación Electrónica provides. The subscriber expressly authorizes his/her personal data usage that the file contains, as far as necessary for carrying out the provided actions in the Certification Policy.
12. The Agencia de Tecnología y Certificación Electrónica is committed to provide all the necessary means for avoiding the manipulation, loss or non authorized access to the personal data that is contained in the file.
13. The applicant can exercise his/her rights of access, rectification, cancellation, portability, restriction of processing and object to processing over his/her personal data, sending a written notification to the Agencia de Tecnología y Certificación Electrónica, through any Register Entry of the Generalitat and clearly indicating this willingness.
14. The subscriber is recommended to change the initial PIN that appears in the current contract with the use of tools provided by the Agencia de Tecnología y Certificación Electrónica.

With the signature of this document, the Agencia de Tecnología y Certificación Electrónica is authorized to consult the identity data that is stated in the Interior Ministry, avoiding on this manner the citizen to submit his/her identity document copy.

Copy for the subscriber - Reverse

Qif.: <b>PUBLIC</b>	Ref.: ACCV-CP-07V8.0.2-EN-2024.odt	Version: 8.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.8.0	Pg. 42 of 55



**CERTIFICATION CONTRACT - OID 1.3.6.1.4.1.8149.3.7**

**Section 1 – Subscriber's data**

Surname:

Name:

DNI/NIF:

Tel.:

Electronic mail address:

Post address:

**Section 2 – Data of the Registration Point Operator**

Name and surname:

**Section 3 – Date and Signature**

*I subscribe the current certification contract associated to the Certification Policy for Qualified Certificates based on software for citizens with the OID 1.3.6.1.4.1.8149.3.7, issued by the la Agencia de Tecnología y Certificación Electrónica. I declare I know and accept the rules of use of this type of certificates that are exposed at <http://www.accv.es>. Likewise, I declare that the exposed data is correct.*

Signature of the subscriber

Signature and stamp of the Registration Point

Signed:

Signed:

Nº of request

Copy for the ACCV

Qif.: <b>PUBLIC</b>	Ref.: ACCV-CP-07V8.0.2-EN-2024.odt	Version: 8.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.8.0	Pg. 43 of 55



## Annex II – Certificate revocation request form

CERTIFICATE REVOCATION REQUEST	
Date:.....	
<b>Section 1 – Subscriber data</b>	
Surname:	
Name:	
DNI/NIF:	
<b>Section 2 – Certificate identification *</b>	
Personal certificate:	Nº of the certificate request:
<b>Section 3 – Revocation reason*</b>	
* The will to revocation of the certificate subscriber is a valid reason for this request.	
<b>Section 4 – Authorization*</b>	
Certificate subscriber	
<i>Signature</i>	
Registration Point Operator:	
Signature:	

Copy for the ACCV

Qlf.: PUBLIC	Ref.: ACCV-CP-07V8.0.2-EN-2024.odt	Version: 8.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.8.0	Pg. 44 of 55



<b>CERTIFICATE REVOCATION REQUEST</b>	
V3.0	
Date:.....	
<p><b>Section 1 – Subscriber data</b></p> <p>Surname:</p> <p>Name:</p> <p>DNI/NIF:</p>	
<p><b>Section 2 – Certificate identification*</b></p> <p>Personal certificate: <span style="float: right;">Nº of the certificate request:</span></p>	
<p><b>Section 3 – Revocation reason*</b></p>   <p>* The will to revocation of the certificate subscriber is a valid reason for this request.</p>	
<p><b>Section 4 – Authorization*</b></p> <p>Certificate subscriber</p>     <p style="text-align: center;"><i>Signature</i></p> <p>Registration Point Operator:</p>     <p style="text-align: center;">Signature:</p>	

Copy for the applicant

## Annex III - Video ID identification

The following is a description of the asynchronous video identification mechanism used by ACCV - ISTECE to carry out the non-presential identification as regulated in the Order ETD/465/2021, of May 6, which regulates the methods of remote identification by video for the issuance of qualified electronic certificates.

For this work has been used as a remote video identification product VIDEO HIGH of the company electronic ID. This product has passed all the necessary reviews and audits required by this order.

1. The user enters his NIF/NIE: ARCA is called to see if he has active certificates of the same type.



If no application is pending, the applicant skips to step 2.

2. Create application:

2.1. Enter first and last name.

Qif.: <b>PUBLIC</b>	Ref.: ACCV-CP-07V8.0.2-EN-2024.odt	Version: 8.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.8.0	Pg. 46 of 55





# Certificado de ciudadano

## Soporte software (en fichero)

Puede Usted identificarse en cualquier dispositivo con cámara, pero no es posible generar el certificado en un dispositivo móvil o una tablet.

Rellene los siguientes cuadros de texto y pulse el botón de validar.

Nombre:

Primer apellido:

Segundo apellido:

Validar

2.2. Accepts the terms and conditions of the identification and certification contract, as well as expressly consents to the implementation of the non-face-to-face identification procedure.

Lea las condiciones del contrato. Para continuar marque los checks que encontrará debajo.

11. En cumplimiento de la ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, se informa al solicitante del tratamiento de datos de carácter personal bajo la responsabilidad de la Agencia de Tecnología y Certificación Electrónica - ISTECE. La finalidad de dicho tratamiento es la servir a los usos relacionados con los servicios de certificación prestados por la Agencia de Tecnología y Certificación Electrónica - ISTECE. El suscriptor consiente expresamente la utilización de sus datos de carácter personal contenidos en dicho fichero, en la medida en que sea necesario para llevar a cabo las acciones previstas en la Política de Certificación.

12. La Agencia de Tecnología y Certificación Electrónica - ISTECE se compromete a poner los medios a su alcance para evitar la alteración, pérdida o acceso no autorizado a los datos de carácter personal contenidos en el fichero.

13. El solicitante podrá ejercer sus derechos de acceso, rectificación, borrado, portabilidad, restricción

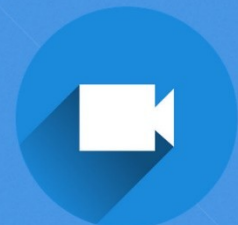
La generación de este certificado tiene un coste de 10.0€ (I.V.A. incluido) que se pagarán mediante pasarela de pagos.

Recuerde que el momento de acceder a la videoidentificación deberá hacerlo desde un ordenador/tablet/móvil con cámara, en un lugar suficientemente iluminado y tener a mano su teléfono móvil y su DNI/NIE, pasaporte español o permiso de conducir.

Soy mayor de 14 años, he leído las condiciones de la identificación y del contrato de certificación y estoy de acuerdo con ellas.

Consiento expresamente la realización de este procedimiento de identificación no presencial mediante Video Identificación y la grabación y conservación del mismo. Asimismo consiento que se consulten los datos de mi identidad que consten en el Ministerio de Interior.

Agencia de Tecnología  
y Certificación Electrónica ISTECE.



Qif.: PUBLIC	Ref.: ACCV-CP-07V8.0.2-EN-2024.odt	Version: 8.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.8.0	Pg. 47 of 55




2.3. Enter your phone number: after validation, an SMS message is sent to you with a code that you must type in a text box. You have 3 attempts. If you type it correctly you will go to the next step.

## Certificado de ciudadano

### Soporte software (en fichero)

Es necesario validar que dispone de un teléfono móvil ya que durante el proceso se le enviarán algunos SMS. En ningún caso se hará uso de esta información para ninguna acción que no esté relacionada con este proceso de generación de un certificado digital.

Teléfono móvil:

 **Enviar SMS**


## Certificado de ciudadano

### Soporte software (en fichero)

Es necesario validar que dispone de un teléfono móvil ya que durante el proceso se le enviarán algunos SMS. En ningún caso se hará uso de esta información para ninguna acción que no esté relacionada con este proceso de generación de un certificado digital.

Teléfono móvil:

Código enviado por SMS:

 **Validar código**

Qif.: <b>PUBLIC</b>	Ref.: ACCV-CP-07V8.0.2-EN-2024.odt	Version: 8.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.8.0	Pg. 48 of 55




2.4. Enter the e-mail address. After validating it:

## Certificado de ciudadano

### Soporte software (en fichero)

Para finalizar esta recogida de información necesitamos que nos proporcione una dirección de e-mail. A esa dirección se le enviará un correo electrónico con un enlace para realizar el pago y la videoidentificación. En ningún caso se hará uso de esta información para ninguna acción que no esté relacionada con el ciclo de vida de su certificado digital.

E-mail:



## Certificado de ciudadano

### Soporte software (en fichero)

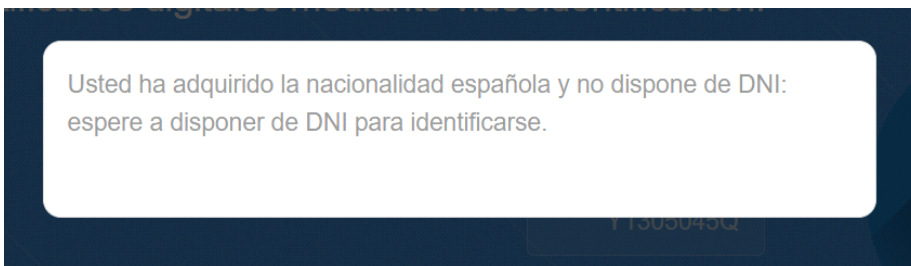
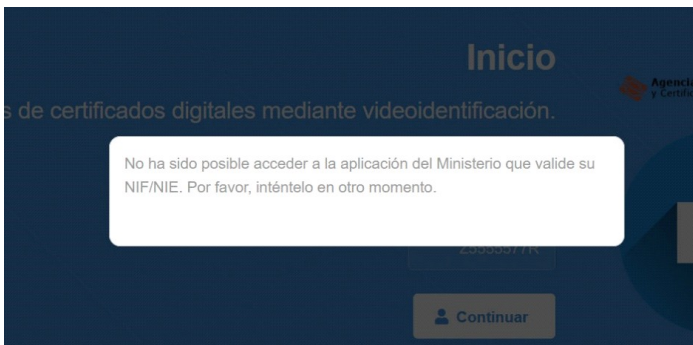
Se le ha enviado un correo con un enlace para continuar con el proceso. Recuerde abrirlo en el dispositivo donde tenga la cámara para ser videoidentificado.

2.4.1. The SVDRI is called to obtain name and surname.

If the SVDRI responds that there is a problem with the NIF entered, the request does not continue and the mail is not sent.

If the SVDRI does not respond at that time, it retries 2 more times and if it still does not respond, the 3 connection errors are saved and the process continues.

Qif.: <b>PUBLIC</b>	Ref.: ACCV-CP-07V8.0.2-EN-2024.odt	Version: 8.0.2
Est.: APPROVED	OID: 1.3.6.1.4.1.8149.3.7.8.0	Pg. 49 of 55



#### 2.4.2. The application information is stored.

The initial evidence is stored for retrieval, regardless of the final result of the request (successful and unsuccessful requests are stored).

#### 2.4.3. A code is generated and sent to the e-mail address provided.

3. The user clicks on the link in the email where the code is and accesses a page where a code is sent by SMS to be validated. The user has 3 attempts. If he/she writes it correctly, he/she will go to the next step.



4. Payment at the Redsys POS.



**Datos de la Compra**

Importe:	10,00 Euros
Comercio:	AUT CERTIFICACION DE LA C. (SPAIN)
Nº de pedido:	VID0002100
Fecha:	24/06/2022
Hora:	14:03

**Pago con tarjeta**

Nº Tarjeta

Caducidad Mes  Año

Cód. Seguridad  ?

**Aceptar**

4.1. If the user has previously paid and cut the connection, it will allow him to continue with the process.





5. Go to the video identification page:

From here the process managed by the VideoID High tool starts.

Seleccione el tipo de documento con el que realizará la videoidentificación.

Documento nacional de identidad (DNI)

Número de identidad de extranjero (NIE)

Pasaporte español


Carnet de conducir español


[▶▶ Continuar](#)


Hola, vamos a realizar una grabación para verificar tu identidad.

[Continuar](#)

¿Qué necesitas?

 Un lugar bien iluminado.

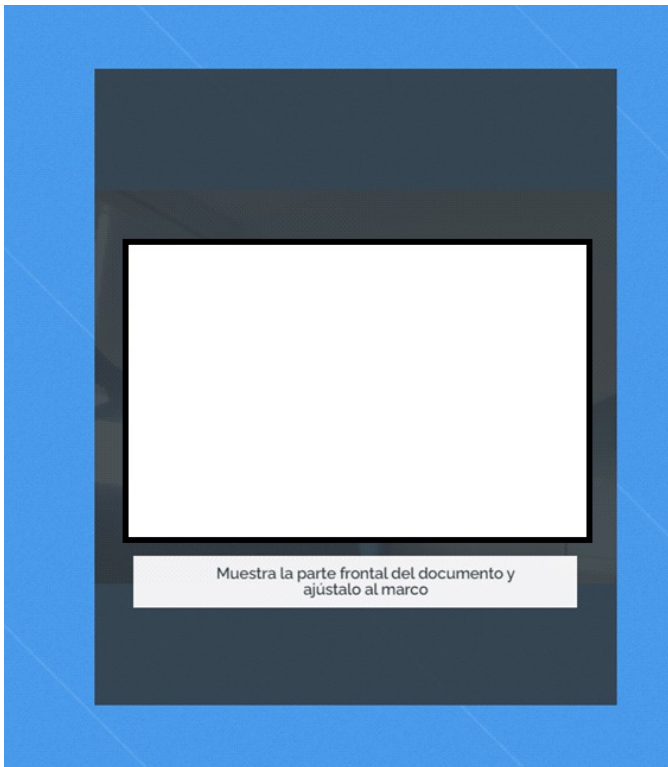
 Tu documento original, en vigor y sin fundas.

 Conexión a internet estable y de capacidad.

[Comenzar](#)



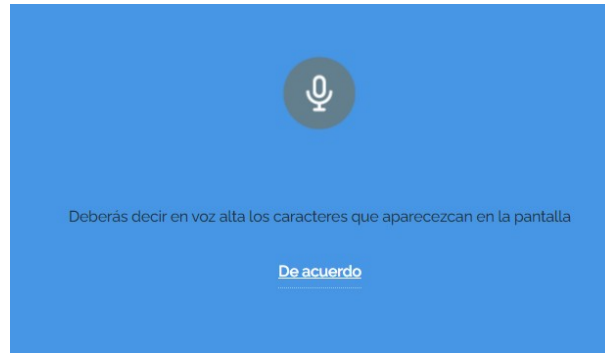
You must present the front of the document



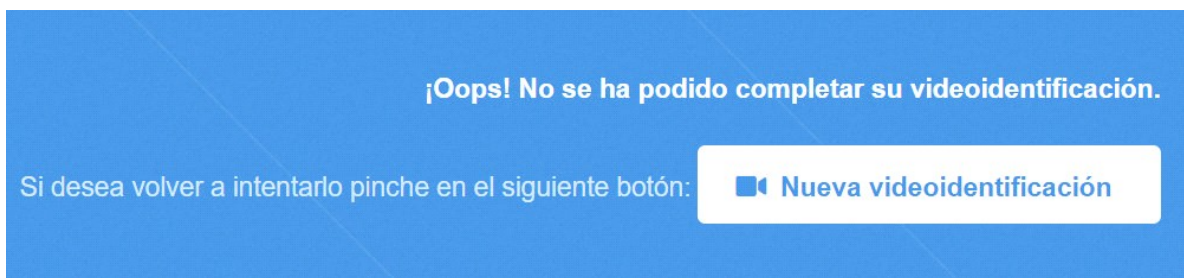
The user then displays the reverse side of the document



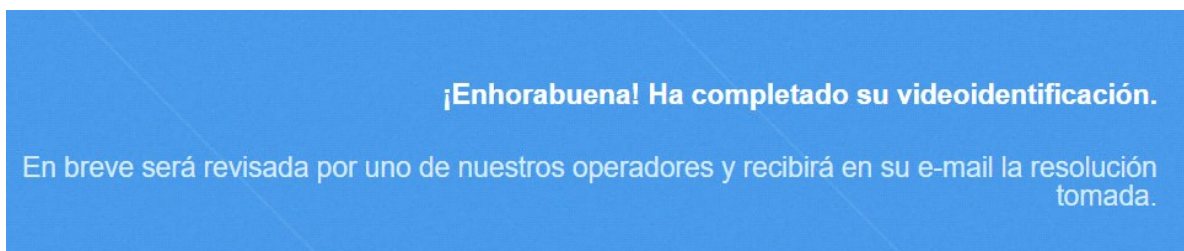
It will then ask you to smile at the camera and finally to read a series of random characters.



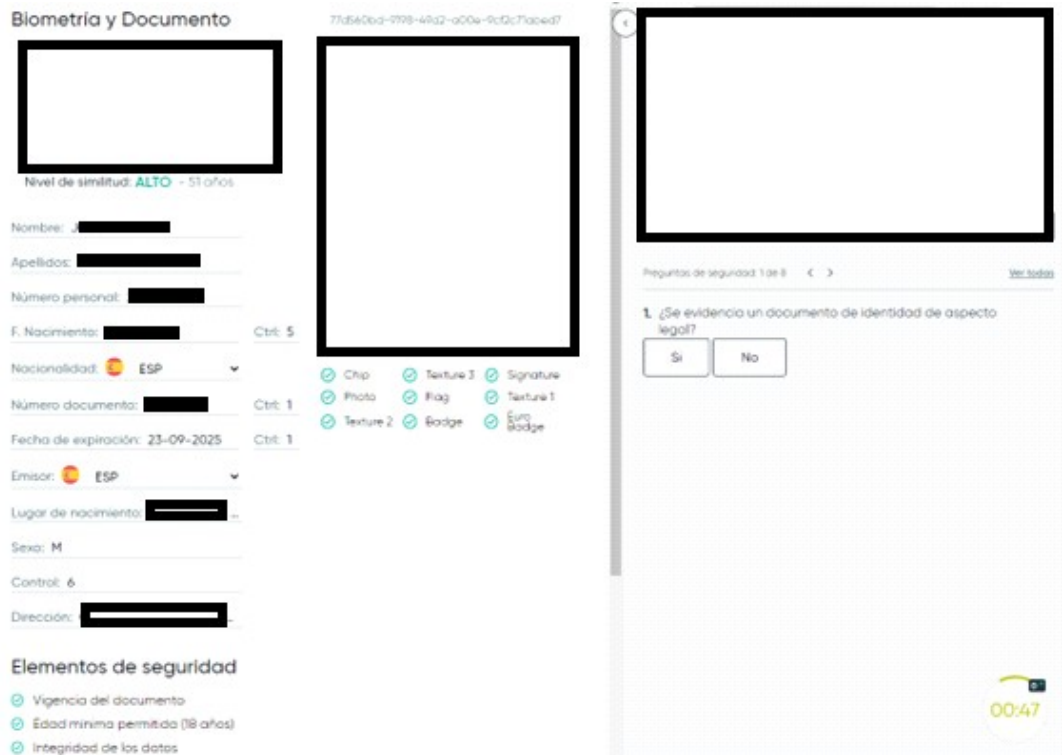
5.1. If the video-identification fails, the application allows to restart the video-identification. The failed video identification creates evidence in CouchDB.



5.2. Once successfully completed, a message is displayed to the user, who at this point ends his intervention. If the ID number obtained in the video-identification differs from the one entered in the application, the application is marked as "reviewable by operator". It is also marked as "reviewable by operator" if the name and surname of the request (obtained by SVDRI or entered by the user) are not the same as those returned by the video-identification. In both cases it warns of this circumstance in an email to all operators.



6. An operator verifies video identification:



6.1. If the application is rejected for any of the reasons offered, an email is sent to the user informing that by accessing the same place in point 1 and entering their ID card they can try again. All these actions create evidence in the application.

6.2. Accepted: the request is saved as pre-accepted. A process periodically reviews these requests:

6.2.1. If the application is found "reviewable by operator" it does nothing. In the daily reviews by operators should be checked, at that time it is shown in NIF of the same as well as the photo of the document so you can determine if the numbers are different or not. If they are different, the application is rejected. If they are the same, name and surname are checked and can be modified by the operator according to what is seen in the photo and the flag "reviewable by operator" is unchecked..

6.2.2. If the request is not found to be "reviewable by operator", evidence is created in CouchDB and ARCA is called to generate a web request that continues its normal processing. The contract shown in point 2.2 and the response from SVDRI are passed to ARCA as evidence.

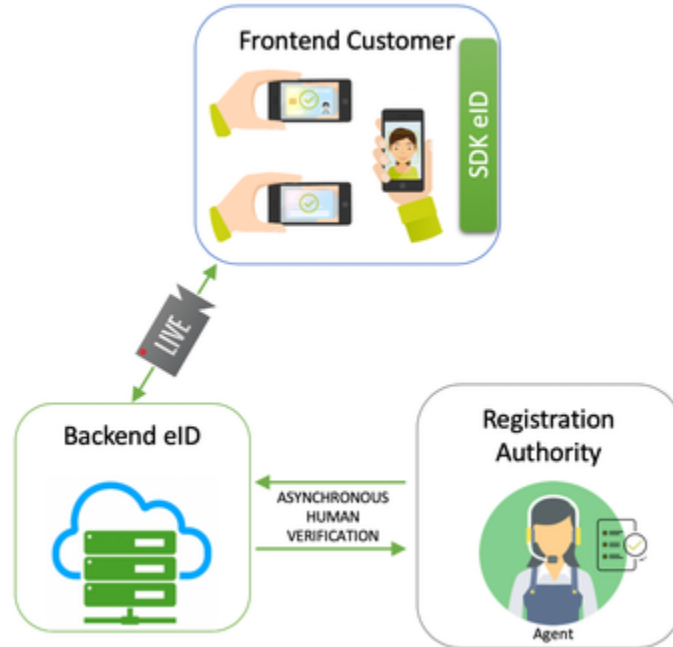
*Below is a document provided by the manufacturer explaining how the VideoID High solution works.*

# VideoID - High

## How is it consumed?

Because this product performs a video transmission from our client's frontend directly to the eID backend, our client must integrate the eID SDK into their application for the product to work.

This product includes a human agent verification, through the "Registry" solution, which occurs through an asynchronous request.



We provide the following SDKs:

- Web SDK: it is a JavaScript library, for applications that run on a web browser. It works in desktop computers, laptops, cell phones and tablets.
- iOS SDK: for native applications on devices with iOS operating systems. It works on cell phones and tablets.
- Android SDK: for native applications from devices with Android operating systems. It works on cell phones and tablets

## Typical Client Process

Typically, this product is used in processes of new registrations (Onboarding) from our Client's application, which for regulatory reasons, must go through a human verification of the video once it has been recorded.

Each onboarding process varies from client to client, but generally consists of a series of steps that we detail below:

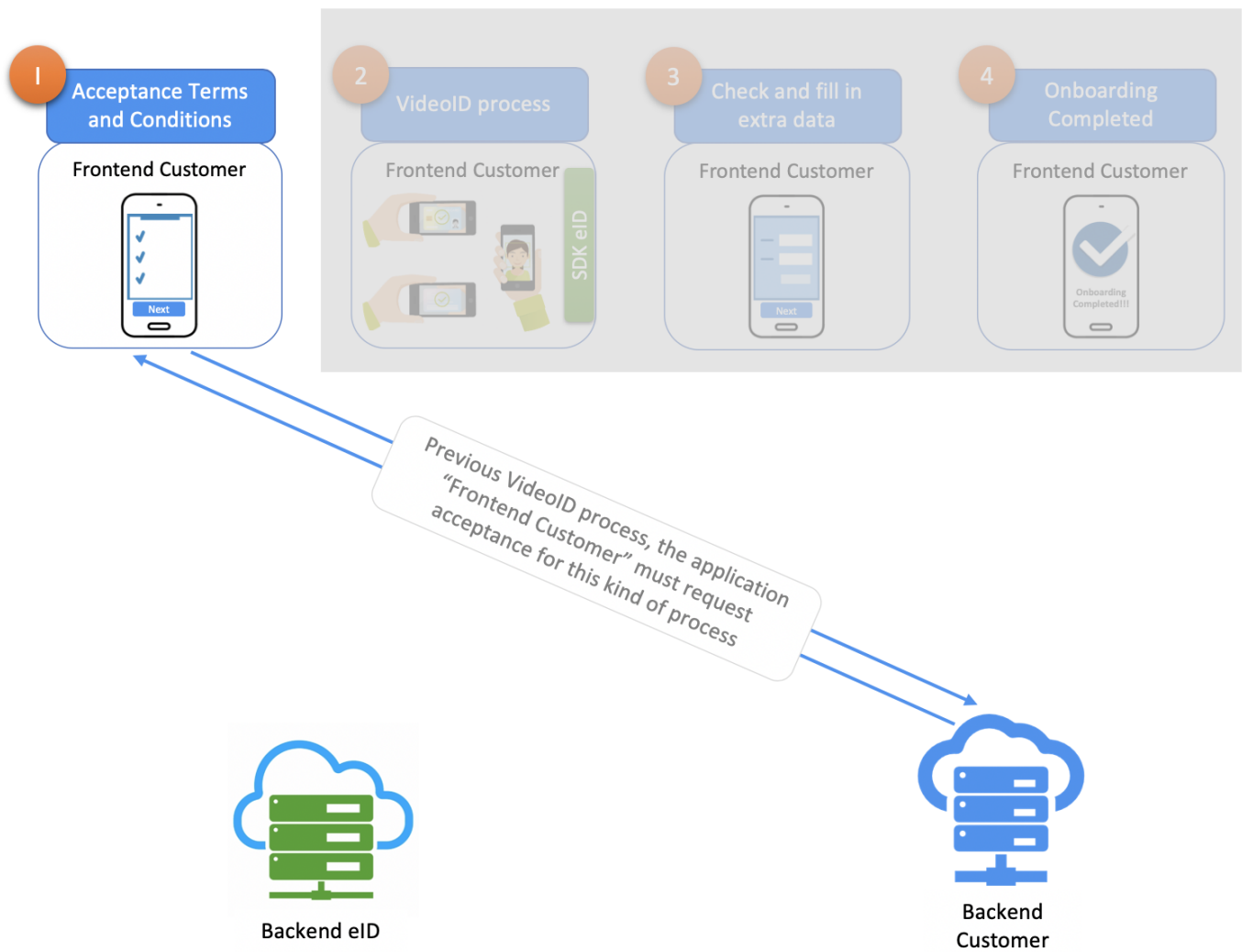
1. Acceptance of terms and conditions before starting the process
2. VideoID Process
3. Additional data and checks
4. End of the onboarding process

### 1) Acceptance of terms and conditions before starting the process

For regulatory compliance in terms of data protection, it is necessary that the Person accepts that it will be recorded and that his or her data will be treated according to the current regulations, before starting the process.

**Note:** see diagram below.





## 2) VideoID Process

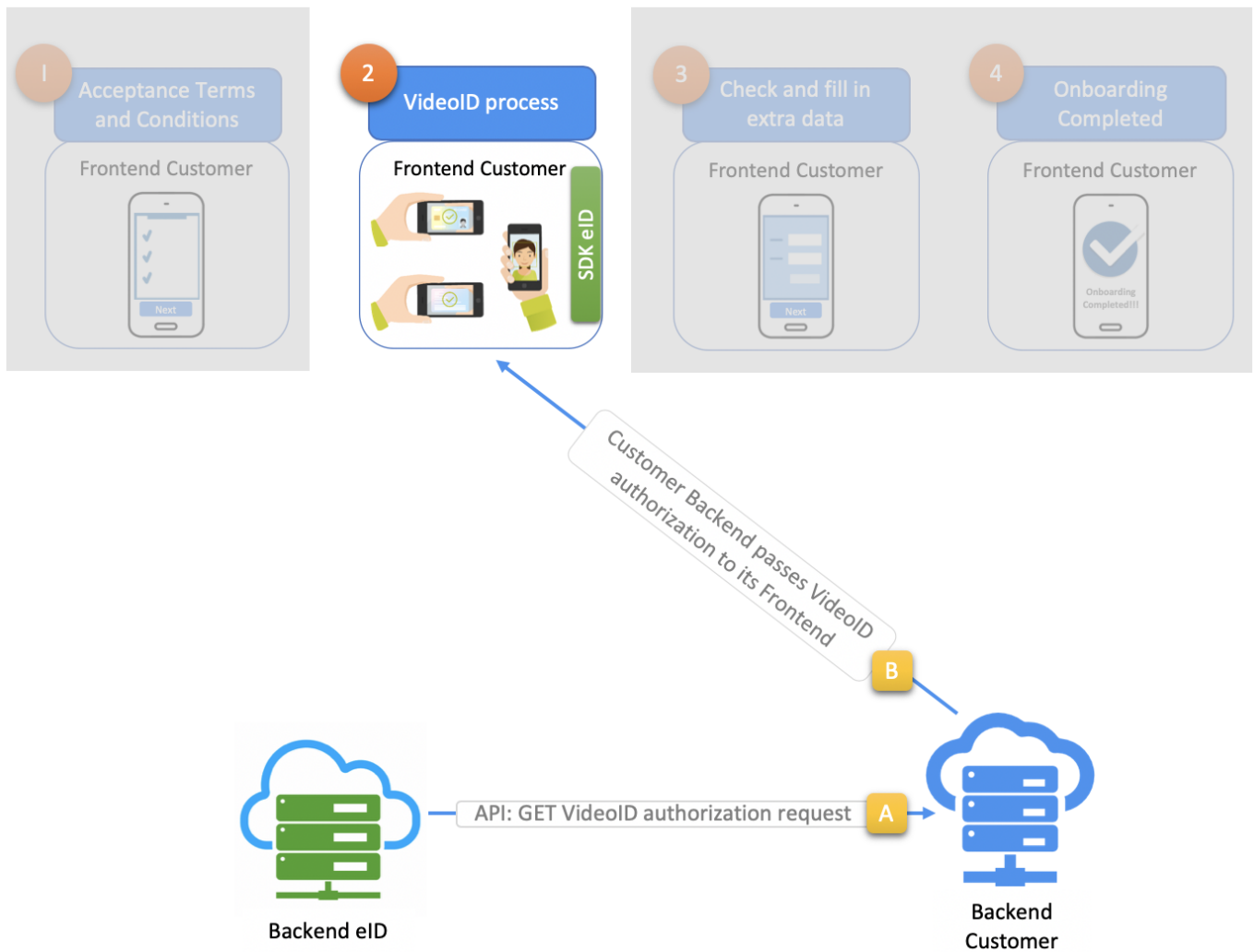
In order to start each VideoID process, the eID API must provide an "Authorization". This Authorization is a code used at the Frontend Customer level to initiate the transmission of the VideoID to the Backend eID. For security reasons, the Authorization is temporary and it only allows one VideoID to be made.

**Note:** from a technical point of view, the integration of the "VideoID - High" product is done using the API calls for VideoID in "Unattended" processing mode. Conceptually it means that it is a video ID that is not attended by humans during video transmission (also known as VideoID with Asynchronous verification). In any case, the full technical detail can be found in the API documentation.

**Note:** see diagram below.

**A:** The "Backend Customer" requests the Authorization with an API call.

**B:** The Backend Customer sends the Authorization to the Frontend Customer to be used by the SDK at the beginning of the video transmission.



**Note:** see diagram below.

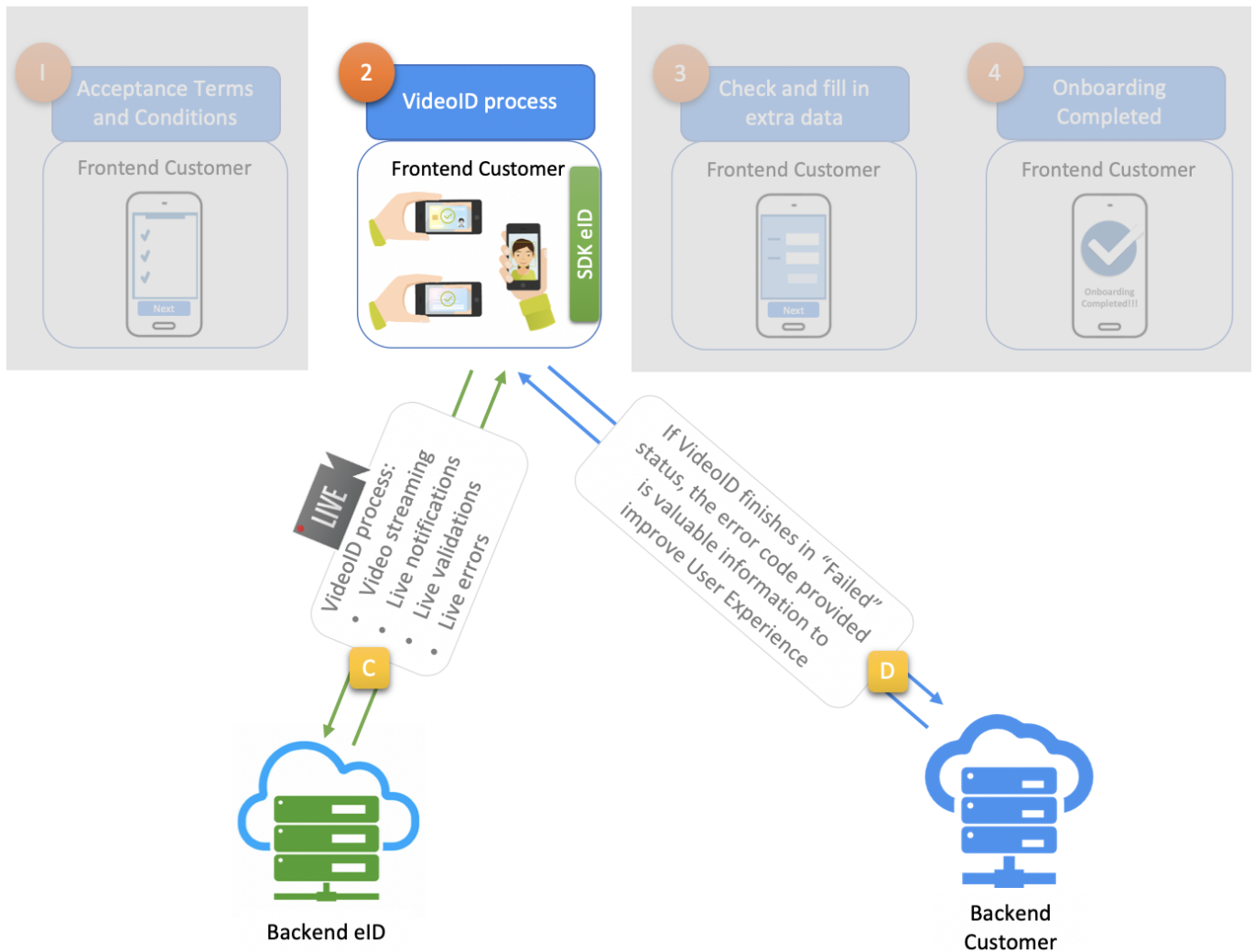
**C:** using the "Authorization" previously requested to the API, it is passed to the SDK and the request is made to start the video transmission. Once the process is started, everything happens automatically and the VideoID shows help messages to the Person who identifies himself, both in the step of showing the ID card and in the step of showing the face.

**D:** During the process, there could be different circumstances that prevent the Person from advancing in the process, or to finish the VideoID correctly. If this happens, the SDK allows to get the reason that made the video process not finish correctly through an error code, for example: low lighting, slow or unstable connection, etc. Note: the catalog of these errors is available in the API documentation.

In operational terms, a VideoID exists in several states, visible in Grafana reports or from direct database queries (in the Dashboard API it is not possible to see these states):

- **Pending:** An "Authorization" request has been made but for technical or operational reasons, the video transmission to the "Backend eID" has not been initiated.
- **Failed:** The VideoID started working but could not finish correctly.
- **Completed:** the VideoID reached the end of the process correctly.
- **Ongoing:** the video is being transmitted.

**Note:** only VideoIDs completed in "Completed" status can be sent for verification by human agents.



### 3) Additional data and checks

Once the VideoID process is completed, the eID Client can retrieve all data collected by the technology and corresponding evidence through the eID API.

Typically, a Client will also use the data collected through the eID technology to make queries to third party screening services (blacklists, sanctioned individuals, known terrorists, etc.).

**Note:** see diagram below.

**A:** The "Backend Customer" can get all data collected by VideoID during the process through an eID API call, for use it in the next steps of the Onboarding process.

**B:** The Backend Customer makes an eID API call to request a human agent to review the recorded VideoID. NOTE: This step is what makes the VideoID "High", because for regulatory purposes, human review adds greater safeguards to the video identification process.

**B1:** The eID API is responsible for queuing the verification request in the corresponding "Registry" (Registration Authority), so that an available agent can review and validate the VideoID. The verification time of an agent can have a defined maximum or it can be indefinite, depending upon customer needs.

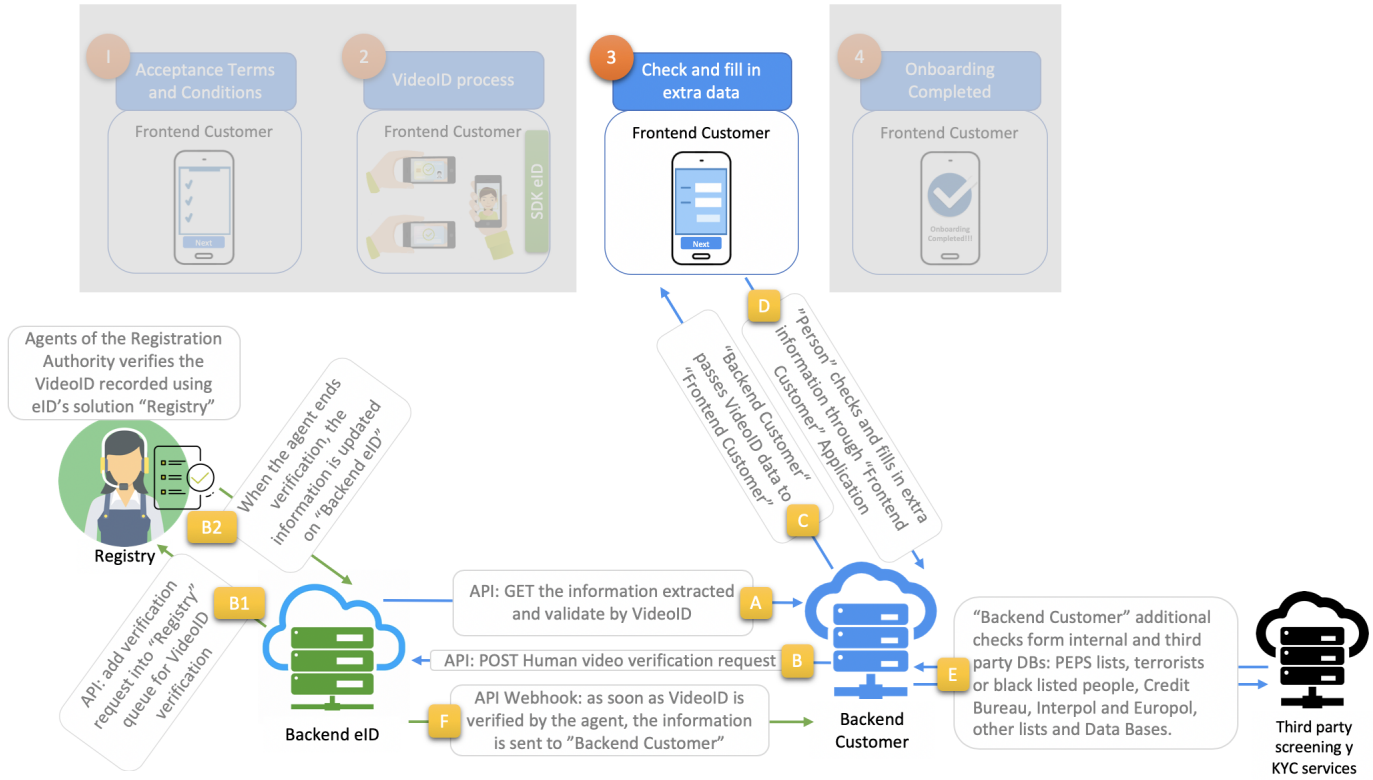
**B2:** Once the VideoID is reviewed by the verifying agent, the eID API updates the verification information and makes it available via eID API and/or Webhook (see step F).

**C:** once the data collected by VideoID is retrieved, the Customer can show it to the user through the "Frontend Customer" to pre-fill the form and ask him to fill in the remaining fields, improving the user experience.

**D:** Once the person fills in all the remaining data, they are updated in the "Backend Customer" to complete the next steps of their onboarding process.

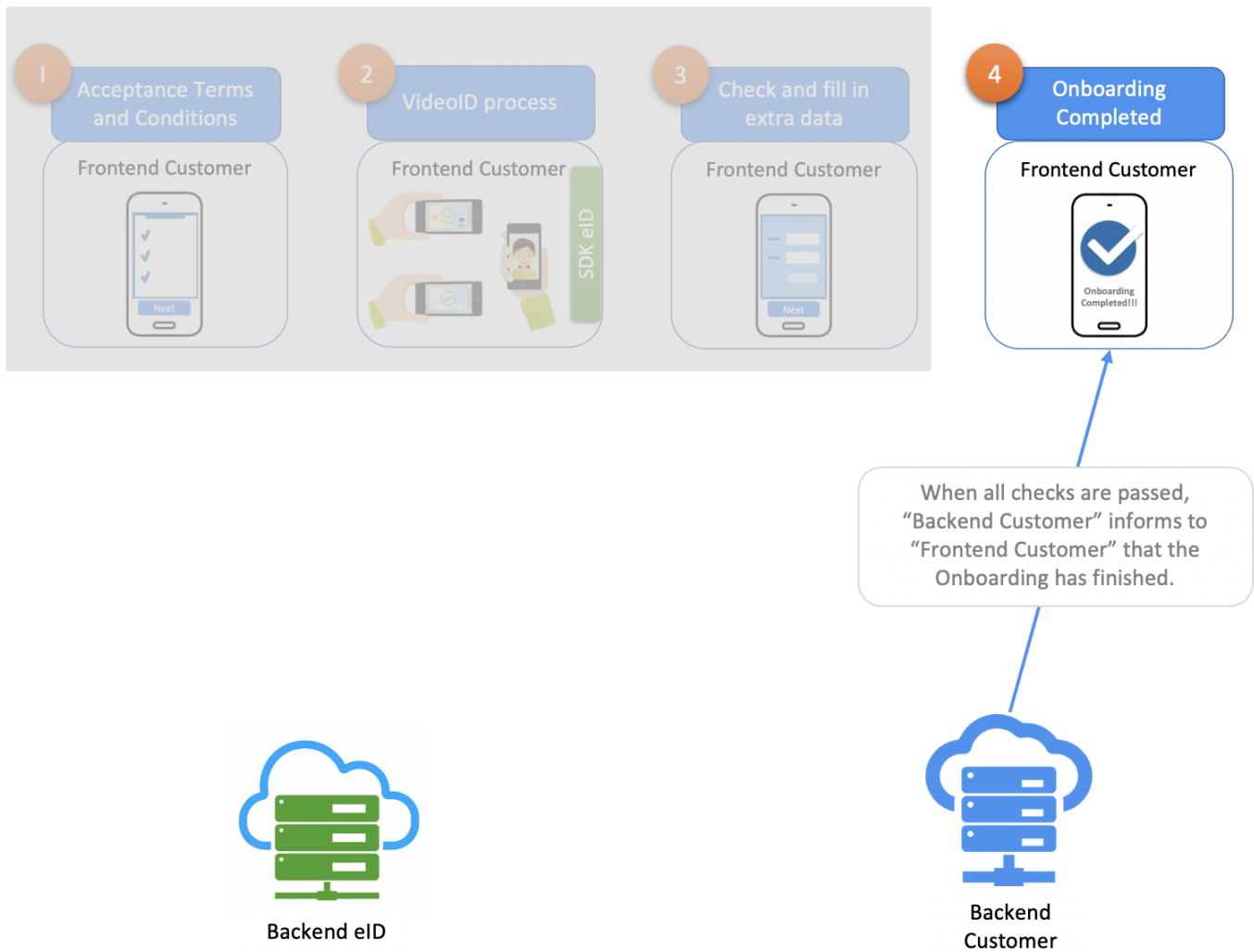
**E:** The VideoID data, retrieved through the eID API, is used by the Customer to make queries to sanctioned list providers, political responders (PEPS), terrorist lists and other queries necessary for regulatory compliance, depending on the case of use.

**F:** If the Customer has the eID Webhook configured, it will automatically know when the agent finishes the verification, because the eID API is in charge of informing it through the Webhook, otherwise, it can call the API to know the verification status of that VideoID.



#### 4) End of the Onboarding process

When the "Backend Customer" has all the information needed for the onboarding process, the process ends, and the person is informed that the Onboarding has finished.



### Information held by eID available for Customers

At the end of a VideoID process, all information captured and generated during the process is available via eID API to be consumed by the Client, as long as the contractual relationship between eID and Client is maintained.

The information of a VideoID available for download via API includes, among others:

- VideoID identifier.
- Result of the automatic validations made by the VideoID on the identity document and the face of the person.
- Personal data extracted from the ID document.
- Image of the identity document in standard market format. If it is a two-sided document, images of each side will be available.
- Image of the person's face.
- Video of the whole process carried out by the person in market standard format.
- Identifiers of the Registration Authority (Registry) and the human agent who performed the verification.

In addition, there is the possibility for the customer to remove all information relating to a specific VideoID using the eID API.

**Note:** the information is permanently deleted, there is no way to recover the information once deleted.