Agencia de Tecnología y Certificación Electrónica

Política de Certificación de Certificados Cualificados de Representante de Entidad Jurídica en soporte software

Fecha: 06/07/2026	**Versión:** 3.0.5
Estado: APROBADO	**Nº de páginas:** 68
OID: 1.3.6.1.4.1.8149.3.30.3.0	**Clasificación: PUBLICO**
Archivo: ACCV-CP-30V3.0.5-ES-2026.odt	
Preparado por: Agencia de Tecnología y Certificación Electrónica - ACCV	

Este documento es propiedad de la Agencia de Tecnología y Certificación Electrónica – ACCV.
Licenciado bajo Creative Commons Attribuion-NoDerivatives 4.0 (CC BY-ND 4.0)

Cambios

Versión	Autor	Fecha	Observaciones
1.0.1	ACCV	03/05/2017	Cambios de adaptación RFC3647
1.0.2	ACCV	16/02/2020	Cambio de vigencia
1.0.3	ACCV	20/03/2021	Cambio de Sede y Policy Notice
2.0.1	ACCV	16/03/2022	Se pone el correo como opcional
2.0.2	ACCV	02/12/2022	Corrección de errores
3.0.1	ACCV	06/10/2023	Nueva jerarquía
3.0.2	ACCV	12/02/2024	Dejar sólo la nueva jerarquía
3.0.3	ACCV	07/02/2025	Revisión y correcciones menores
3.0.4	ACCV	04/02/2026	Revisión y correcciones menores
3.0.5	ACCV	06/07/2026	Cambio en los tiempos de gestión

Tabla de Contenido

1 INTRODUCCIÓN

1.1 Presentación

El presente documento es la Política de Certificación asociada a los Certificados Cualificados de Representante de Entidad Jurídica en soporte software, que contiene las reglas a las que se sujeta el uso de los certificados definidos en esta política. Se describen los papeles, responsabilidades y relaciones entre el usuario final y la Agencia de Tecnología y Certificación Electrónica y las reglas de solicitud, adquisición, gestión y uso de los certificados. Este documento matiza y complementa a la *Declaración de Prácticas de Certificación (CPS)* de la Agencia de Tecnología y Certificación Electrónica.

La Política de Certificación referida en este documento se utilizará para la emisión de certificados cualificados en soporte software para representantes de entidades o empresas con personalidad jurídica, según la legislación vigente.

La presente Declaración de Prácticas de Certificación está redactada siguiendo las especificaciones del RFC 3647 *"Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*" propuesto por *Network Working Group* para este tipo de documentos, al igual que la Declaración de Prácticas de Certificación, para facilitar la lectura o comparación con documentos homólogos.

Esta Política de Certificación asume que el lector conoce los conceptos básicos de Infraestructura de Clave Pública, certificado y firma digital, en caso contrario se recomienda al lector que se forme en el conocimiento de los anteriores conceptos antes de continuar con la lectura del presente documento.

1.2 Identificación

Nombre de la política	Política de Certificación de Certificados Cualificados de Representante de Entidad Jurídica en soporte software
Calificador de la política	`Certificado cualificado de Repr. en software expedido por por la ACCV (Pol. Ademuz, s/n. Burjassot, CP 46100, ESPAÑA. CIF A40573396)`
Versión de la política	3.0.5
Estado de la política	APROBADO
Referencia de la política / OID (Object Identifier)	1.3.6.1.4.1.8149.3.30.3.0
Fecha de emisión	6 de julio 2026
Fecha de expiración	No aplicable.
CPS relacionada	Declaración de Prácticas de Certificación (CPS) de la ACCV. Versión 5.0. OID: 1.3.6.1.4.1.8149.2.5.0 Disponible en `http://www.accv.es/pdf-politicas`
Localización	Esta Política de Certificación se puede encontrar en: http://www.accv.es/legislacion_c.htm

1.3 Comunidad de usuarios y ámbito de aplicación

1.3.1 Autoridades de Certificación

Las CAs que pueden emitir certificados acordes con esta política son ACCV RSA1 PROFESIONALES y ACCV ECC1 PROFESIONALES pertenecientes a la Agencia de Tecnología y Certificación Electrónica, cuya función es la emisión de certificados de entidad final para los suscriptores de ACCV. La elección de una u otra CA dependerá del tipo de claves utilizados para la emisión de los certificados finales: RSA o ECDSA.

Los certificados de ACCV RSA1 PROFESIONALES y ACCV ECC1 PROFESIONALES son válidos desde el día 25 de julio de 2023 hasta el 19 de julio de 2047.

1.3.2 Autoridades de Registro

La lista de Autoridades de Registro (Puntos de Registro de Usuario) que gestionan las solicitudes presenciales de certificados definidos en esta política se encuentra en la URL http://www.accv.es

1.3.3 Suscriptores

El grupo de usuarios que pueden solicitar certificados definidos por esta política está compuesto por los administradores de la Entidad, sus representantes legales y voluntarios con poder bastante a estos efectos.

La custodia de los datos de creación de firma asociados a cada certificado electrónico de representante de persona jurídica será responsabilidad del representante solicitante, cuya identificación se incluirá en el certificado electrónico.

El soporte de claves y certificados es software.

1.3.4 Partes confiantes

Se limita el derecho a confiar en los certificados emitidos conforme a la presente política a:

- Las aplicaciones y servicios pertenecientes a las Administraciones Públicas españolas o europeas. entidades u organizaciones.
- Las aplicaciones y servicios que, sin pertenecer al ámbito de la Administración Pública, requieran de sistemas de identificación y/o firma seguros, de acuerdo con la legislación española de firma electrónica o con la normativa europea.
- Los actos y las contrataciones de bienes o servicios que sean propios o concernientes al giro o tráfico ordinario de la persona jurídica y su representación.

1.3.5Otros participantes

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

1.4 Uso de los certificados

1.4.1 Usos Permitidos

Los certificados emitidos por la Agencia de Tecnología y Certificación Electrónica bajo esta Política de Certificación, pueden utilizarse para la firma electrónica y cifrado de cualquier información o

documento. Asimismo, pueden utilizarse como mecanismo de identificación ante servicios y aplicaciones informáticas.

1.4.2 Usos Prohibidos

Los certificados se utilizarán únicamente conforme a la función y finalidad que tengan establecida en la presente Política de Certificación, y con arreglo a la normativa vigente.

1.5 Política de Administración de la ACCV

1.5.1 Especificación de la Organización Administradora

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

1.5.2 Persona de Contacto

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

1.5.3 Competencia para determinar la adecuación de la CPS a la Políticas

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

1.5.4Procedimiento de aprobación.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

1.6 Definiciones y Acrónimos

1.6.1Definiciones

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

1.6.2Acrónimos

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

2 Publicación de información y repositorio de certificados

2.1 Repositorio de certificados

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

2.2 Publicación

La Agencia de Tecnología y Certificación Electrónica (ACCV) se ajusta a la versión actual del documento "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates", publicada en https://www.cabforum.org/. En el caso de cualquier incompatibilidad entre esta Política de Certificación y los requisitos del CAB Forum, dichos requisitos prevalecerán sobre el presente documento.

2.3 Frecuencia de actualizaciones

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

2.4 Controles de acceso al repositorio de certificados.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

3 Identificación y Autenticación

3.1 Registro de nombres

3.1.1 Tipos de nombres

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

3.1.2 Significado de los nombres

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

3.1.3 Interpretación de formatos de nombres

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

3.1.4 Unicidad de los nombres

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

3.1.5 Resolución de conflictos relativos a nombres

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

3.1.6 Reconocimiento, autenticación y función de las marcas registradas.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

3.2 Validación Inicial de la Identidad

3.2.1 Métodos de prueba de posesión de la clave privada.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

3.2.2 Autenticación de la identidad de una organización.

La autenticación de la identidad de una organización o entidad se realizará mediante la identificación del solicitante del certificado de Representante de Entidad (administrador, o el representante legal o voluntario con poder bastante) ante la Autoridad de Registro correspondiente habilitada para la emisión de este tipo de certificados, acreditando su identidad personal y aportando la documentación que se establece a continuación:

- La solicitud del certificado electrónico de representante de entidad para una Administración Pública (estatal, autonómica o local) deberá realizarla la persona responsable y con autoridad en la entidad a nivel de Director General, Gerente, Alcalde, Teniente Alcalde o Secretario, Presidente o Vicepresidente de la Diputación, acompañado del Diario o Boletín Oficial donde conste la publicación de su nombramiento.
- Para solicitar certificado electrónico de representante de una sociedad mercantil o cualquier sociedad de inscripción obligatoria en el Registro Mercantil (Sociedad Anónima, Sociedad de

Responsabilidad Limitada, Sociedad Laboral, Sociedad Deportiva, Sociedades Colectivas, Comanditarias o Cooperativas, Agrupaciones de Interés Económico, UTE, otras..), se deberá aportar certificado del Registro Mercantil relativo a la constitución, personalidad jurídica y nombramiento y vigencia del cargo de administrador o representante legal, expedido durante los 30 días anteriores a la fecha de presentación del certificado en la ACCV. Si no se aportara se entiende que presta el consentimiento a la ACCV para la consulta en registro público donde consten inscritos los documentos de constitución y apoderamiento. Si la representación es voluntaria, se sustituirá el certificado de nombramiento y vigencia del cargo por el poder notarial bastante, con la cláusula especial para poder solicitar el Certificado de Representante de Persona Jurídica.

La ACCV guardará copia de la documentación presentada por el solicitante o de la consultada en el Registro Mercantil.

3.2.3 Autenticación de la identidad de un individuo.

La autenticación de la identidad del solicitante de un certificado de representante de persona jurídica se realizará mediante su identificación ante la Autoridad de Registro correspondiente. En el caso de personarse ante el Operador del Punto de Registro habilitado para la emisión de este tipo de certificado, debe acreditarse la identidad mediante presentación del Documento Nacional de Identidad (DNI), pasaporte español, o el Número de Identificación de Extranjeros (NIE) del solicitante. Podrá prescindirse de la personación si su firma en la solicitud de expedición de un certificado cualificado ha sido legitimada en presencia notarial. En el caso de identificación no presencial frente a la Autoridad de registro, el usuario debe presentar un certificado cualificado personal de la ACCV o el DNIe. Previamente se debe haber registrado la solicitud y confirmado la documentación necesaria para identificar la identidad de la organización y la vinculación del solicitante con la misma.

En el caso de los mecanismos de videoidentificación, es necesario que las pruebas sean las mismas y tengan el mismo valor probatorio de identidad (misma calidad). La utilización de sistemas de verificación de identidad mediante videoidentificación está condicionada a la base legal correspondiente y a la normativa técnica asociada. En el caso de que se pueda utilizar este tipo de mecanismos, se incluirá una descripción completa de la solución en el Anexo III de esta política.

Tras producirse todas las comprobaciones el solicitante dispondrá de un máximo de 15 días para generar el certificado.

3.2.4 Información no verificada del subscriptor

Toda la información suministrada es verificada.

3.2.5 Validación de la representación

La capacidad del solicitante del certificado de realizar la solicitud de certificados en nombre de terceros se verifica durante la validación de la identidad del solicitante. Como se establece por ley es necesario un poder especial especifico para realizar esta operación.

3.2.6 Criterio para la interoperación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

3.3 Identificación y autenticación de las solicitudes de renovación de la clave.

3.3.1 Identificación y autenticación de las solicitudes de renovación rutinarias.

La identificación y autenticación para la renovación del certificado se realizará utilizando las técnicas y procedimientos recogidos en el punto 3.*2 Validación Inicial de la Identidad*.

3.3.2 Identificación y autenticación de las solicitudes de renovación de clave después de una revocación – Clave no comprometida.

La política de identificación y autenticación para la renovación de un certificado después de una revocación sin compromiso de la clave será la misma que para el registro inicial, o bien se empleará algún método electrónico que garantice de manera fiable e inequívoca la identidad del solicitante y la autenticidad de la solicitud.

3.4 Identificación y autenticación de las solicitudes de revocación de la clave

Para la revocación presencial del certificado de Representante de Entidad deberá personarse el solicitante del certificado u otra persona con poder bastante para representar a la Entidad (administrador o el representante legal o voluntario de la Entidad). La identificación de la persona y determinación del poder se llevará a cabo como se recoge en el punto 3.2. *Validación Inicial del la Identidad*

Telemática. Mediante la solicitud de revocación del solicitante del certificado el formulario de revocación ubicado en el Área Personal de Servicios de Certificación (en http://www.accv.es).

ACCV o cualquiera de las entidades que la componen pueden solicitar de oficio la revocación de un certificado si tuvieran el conocimiento o sospecha del compromiso de la clave privada del subscriptor, o cualquier otro hecho que recomendará emprender dicha acción.

4 El ciclo de vida de los certificados.

Las especificaciones contenidas en este apartado complementan estipulaciones previstas la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.1 Solicitud de certificados

4.1.1Quien puede enviar una solicitud de certificado

Los suscriptores enumerados en el punto 1.3.3 pueden presentar una solicitud de certificado.

4.1.2 Proceso de registro y responsabilidades

El solicitante del certificado que desee que le sea emitido un certificado de Representante de Entidad de acuerdo con esta política de certificación deberá presentarse para solicitarlo en una Autoridad de Registro de la Agencia de Tecnología y Certificación Electrónica, aportando previamente la documentación que se exige en el punto 3.2.2 *Autenticación de la identidad de una organización* utilizando los medios telemáticos que la ACCV pone a disposición del solicitante en https://www.accv.es. Si la presentación es presencial, debe hacerse en un Punto de Registro Autorizado de la Agencia de Tecnología y Certificación Electrónica con su Documento Nacional de Identidad (DNI), pasaporte español o Número de Identificación de Extranjero (NIE) en vigor. Si la presentación es telemática, debe identificarse frente a la Autoridad de Registro con un certificado cualificado personal de la ACCV o bien con el DNIe, en vigor en ambos casos.

En el caso de los mecanismos de identificación por vídeo, es necesario que las pruebas sean las mismas y tengan el mismo valor probatorio de identidad (misma calidad). El uso de sistemas de verificación de identidad mediante videoidentificación está condicionado a la base legal correspondiente y a la normativa técnica asociada. En el caso de que se pueda utilizar este tipo de mecanismo, se incluirá una descripción completa de la solución en el Anexo III de esta política. Este tipo de identificación es equivalente a la presencial en un punto de registro.

El listado de Puntos de registro autorizados para la emisión de este tipo de certificados se encuentra en la URL http://www.accv.es.

Asimismo, en el caso de solicitud de certificado a través de medios remotos sin identificación interactiva de la identidad, se exigirá un periodo de tiempo inferior a cinco años desde la identificación presencial.

La ACCV conserva la información asociada a las solicitudes de forma indefinida (con un límite de al menos 15 años), incluyendo su aprobación o rechazo, y los motivos del mismo.

4.2 Tramitación de la solicitud de certificados.

4.2.1Ejecución de las funciones de identificación y autenticación

Compete a la Autoridad o Entidad de Registro la comprobación de la identidad del solicitante, la verificación de la documentación y la constatación de que el solicitante ha firmado el contrato de certificación. Una vez completa la solicitud, la Autoridad de Registro la remitirá a la Autoridad de Certificación de la ACCV.

4.2.2Aprobación o rechazo de la solicitud

Es atribución de la Autoridad de Registro de la Agencia de Tecnología y Certificación Electrónica el determinar la adecuación de un tipo de certificado a las características del solicitante, en función de las disposiciones de la Política de Certificación aplicable, y de este modo acceder o denegar la gestión de la solicitud de certificación del mismo.

En caso de aceptación, la Autoridad de Registro notificará al solicitante a través de un correo electrónico a la dirección de correo electrónico que figura en la solicitud.

En el caso de denegación de la solicitud de certificación por parte de la Autoridad de Registro, el solicitante recibirá información de los motivos del rechazo de la misma.

Asimismo, en el caso de la solicitud de certificado mediante medios telemáticos se exigirá que haya transcurrido un período de tiempo desde la identificación presencial menor a los cinco años.

4.2.3Plazo para resolver la solicitud

El tiempo máximo para resolver la solicitud es de cinco días laborables.

4.3 Emisión de certificados

ACCV no es responsable de la monitorización, investigación o confirmación de la exactitud de la información contenida en el certificado con posterioridad a su emisión. En el caso de recibir información sobre la inexactitud o la no aplicabilidad actual de la información contenida en el certificado, este puede ser revocado.

4.3.1Acciones de la CA durante el proceso de emisión

La emisión del certificado tendrá lugar una vez que ACCV haya llevado a cabo las verificaciones necesarias para validar la solicitud de certificación y en presencia del solicitante. El mecanismo por el que determina la naturaleza y la forma de realizar dichas comprobaciones es esta Política de Certificación.

La CA recibe una solicitud de certificado en formato PKCS10, bien del punto de registro, bien del equipo del usuario. Todos los datos que la componen ya ha sido verificados en pasos anteriores. La CA firma esa solicitud y la devuelve a la RA para su procesamiento posterior.

Cuando la CA de ACCV emita un certificado de acuerdo con una solicitud de certificación válida, enviará una copia del mismo a la RA que remitió la solicitud y otra al repositorio de ACCV

4.3.2Notificación de la emisión al suscriptor

Es tarea de la RA notificar al subscriptor de un certificado la emisión del mismo y proporcionarle una copia, o en su defecto, informarle del modo en que puede conseguirla.

ACCV notifica al suscriptor sobre la emisión del certificado, a través de un correo electrónico a la dirección de correo proporcionada en el proceso de solicitud.

4.4 Aceptación de certificados

4.4.1Conducta que constituye aceptación del certificado

La aceptación de los certificados por parte de los firmantes se produce en el momento de la firma del contrato de certificación asociado a la Política de Certificación. La aceptación del contrato implica el conocimiento y aceptación por parte del suscriptor de la Política de Certificación asociada.

El Contrato de Certificación es un documento que debe ser firmado por el solicitante y, en el caso de solicitud presencial, por la persona adscrita al Registro de usuarios, y cuyo fin es vincular a la persona a certificar con la acción de la solicitud, con el conocimiento de las normas de uso y con la veracidad de los datos presentados. El formulario del Contrato de Certificación se recoge en el Anexo I de esta Política de Certificación.

El usuario debe aceptar el contrato antes de la emisión del certificado.

4.4.2Publicación del certificado por la CA
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.4.3Notificación de la emisión a terceros
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.5 Uso del par de claves y del certificado.

4.5.1Clave privada del suscriptor y uso del certificado.
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.5.2Uso del certificado y la clave pública por terceros que confían
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.6 Renovación de certificados.

La renovación del certificado debe realizarse con los mismos procedimientos y métodos de identificación que la solicitud inicial.

4.6.1Circunstancias para la renovación del certificado
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.6.2Quién puede solicitar la renovación del certificado
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.6.3Tramitación de solicitudes de renovación de certificados
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.6.4Notificación de la emisión de un nuevo certificado al suscriptor
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.6.5Conducta que constituye la aceptación de la renovación del certificado
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.6.6Publicación del certificado de renovación por parte de la Autoridad de Certificación
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.6.7Notificación de la renovación del certificado a otras entidades
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.7 Renovación de claves

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.7.1Circunstancias para la renovación con regeneración de claves

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.7.2Circunstancias para la renovación con regeneración de claves

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.7.3Procesamiento de solicitudes de renovación con regeneración de claves

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.7.4Notificación de la renovación con regeneración de claves

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.7.5Conducta que constituye la aceptación de la renovación con regeneración de claves

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.7.6Publicación del certificado renovado

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.7.7Notificación de la renovación con regeneración de claves a otras entidades

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.8 Modificación de certificados.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.8.1Circunstancias para la modificación del certificado

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.8.2Quién puede solicitar la modificación del certificado

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.8.3Procesamiento de solicitudes de modificación del certificado

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.8.4Notificación de la modificación del certificado

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.8.5Conducta que constituye la aceptación de la modificación del certificado

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.8.6Publicación del certificado modificado

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.8.7Notificación de la modificación del certificado a otras entidades

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9 Revocación y suspensión de certificados.

4.9.1 Circunstancias para la revocación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.2 Entidad que puede solicitar la revocación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.3 Procedimiento de solicitud de revocación

La Agencia de Tecnología y Certificación Electrónica acepta solicitudes de revocación por los siguientes procedimientos

4.9.3.1 Presencial

Mediante la presentación e identificación del solicitante del certificado, o persona con poderes para representar a la Entidad de la cual es representante el suscriptor del certificado, en un Punto de Registro de Usuario y la cumplimentación y firma, por parte del mismo, del “Formulario de Solicitud de Revocación” que se le proporcionará y del que se adjunta copia en el anexo II

4.9.3.2 Telemático

El solicitante del certificado podrá solicitar la revocación de certificados, en la web de ACCV, en la URL http://www.accv.es, dentro del Área Personal de Servicios de Certificación, tras identificarse con su certificado personal o de entidad que haya sido solicitado por él mismo.

4.9.4 Periodo de gracia de la solicitud de revocación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.5 Tiempo dentro del cual la CA puede procesar la solicitud de revocación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.6Requisitos para la comprobación de la revocación para las partes confiantes

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.7Frecuencia de emisión de la CRL

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.8Máxima latencia de las CRLs
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.9Disponibilidad de los servicios de comprobación del estado de los certificados
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.10Requisitos de comprobación del estado de los certificados
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.11Otros sistemas para la información del estado de los certificados
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.12Requisitos especiales para el compromiso de clave
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.13Circunstancias para la suspensión
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.14Entidad que puede solicitar la suspensión
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.15Procedimiento para la solicitud de suspensión
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.16Limite para el periodo de supensión

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.10Servicios de comprobación de estado de certificados.

4.10.1Características operativas
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.10.2Disponibilidad del servicio
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.10.3Características opcionales
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.11Finalización de la suscripción.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.12Depósito y recuperación de claves.

4.12.1Prácticas y políticas de custodia y recuperación de claves

La ACCV no realiza el depósito de certificados y claves de cifrado emitidas bajo la presente Política.

4.12.2Prácticas y políticas de protección y recuperación de la clave de sesión

No esta soportada la recuperación de las claves de sesión.

5 Controles de seguridad física, de gestión y de operaciones

5.1 Controles de Seguridad Física

5.1.1 Ubicación y construcción
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.1.2 Acceso físico
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.1.3 Alimentación eléctrica y aire acondicionado
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.1.4 Exposición al agua
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.1.5 Protección y prevención de incendios
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.1.6 Sistema de almacenamiento
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.1.7 Eliminación de residuos
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.1.8 Backup remoto
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.2 Controles de procedimientos
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.2.1 Papeles de confianza
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.2.2 Número de personas requeridas por tarea
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.2.3 Identificación y autenticación para cada papel
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.3 Controles de seguridad de personal

Este apartado refleja el contenido del documento *Controles de Seguridad del Personal* de ACCV.

5.3.1 Requerimientos de antecedentes, calificación, experiencia, y acreditación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.3.2 Procedimientos de comprobación de antecedentes

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.3.3 Requerimientos de formación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.3.4 Requerimientos y frecuencia de actualización de la formación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.3.5 Frecuencia y secuencia de rotación de tareas

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.3.6 Sanciones por acciones no autorizadas

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.3.7 Requerimientos de contratación de personal

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.3.8 Documentación proporcionada al personal

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.3.9 Controles periódicos de cumplimiento

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.3.10 Finalización de los contratos

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.4 Procedimientos de Control de Seguridad

5.4.1 Tipos de eventos registrados

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.4.2 Frecuencia de procesado de logs
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.4.3 Periodo de retención para los logs de auditoría
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.4.4 Protección de los logs de auditoría
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.4.5 Procedimientos de backup de los logs de auditoría
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.4.6 Sistema de recogida de información de auditoría (interno vs externo)
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.4.7 Notificación al sujeto causa del evento
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.4.8 Análisis de vulnerabilidades
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.5 Archivo de informaciones y registros

5.5.1 Tipo de informaciones y eventos registrados
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.5.2 Periodo de retención para el archivo.
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.5.3 Protección del archivo.
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.5.4 Procedimientos de backup del archivo.
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.5.5 Requerimientos para el sellado de tiempo de los registros.
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.5.6 Sistema de recogida de información de auditoría (interno vs externo).
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.5.7 Procedimientos para obtener y verificar información archivada

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.6 Cambio de Clave

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.7 Recuperación en caso de compromiso de una clave o de desastre

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.7.1 Alteración de los recursos hardware, software y/o datos

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.7.2 La clave pública de una entidad se revoca

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.7.3 La clave de una entidad se compromete

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.7.4 Instalación de seguridad después de un desastre natural u otro tipo de desastre

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.8 Cese de una CA

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

6 Controles de seguridad técnica

6.1 Generación e Instalación del Par de Claves

En este punto se hace siempre referencia a las claves generadas para los certificados emitidos bajo el ámbito de la presente Política de Certificación. La información sobre las claves de las entidades que componen la Autoridad de Certificación se encuentra en el punto 6.1 de la Declaración de Prácticas de Certificación (CPS) de la Agencia de Tecnología y Certificación Electrónica.

6.1.1 Generación del par de claves

El par de claves para el certificado emitido bajo el ámbito de la presente Política de Certificación se pueden generar en dos ubicaciones; el equipo del usuario en un proceso de autogeneración sin salir nunca del mismo equipo.

6.1.2 Entrega de la clave privada a la entidad

La clave privada para los certificados emitidos bajo el ámbito de la presente Política de Certificación se encuentra en el equipo del usuario donde se generó el par de claves.

6.1.3 Entrega de la clave pública al emisor del certificado

La clave pública a ser certificada es generada en el equipo del usuario y es entregada a la Autoridad de Certificación por la Autoridad de Registro mediante el envío de una solicitud de certificación en formato PKCS#10, firmada digitalmente por dicha Autoridad de Registro.

6.1.4 Entrega de la clave pública de la CA a los usuarios

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

6.1.5 Tamaño de las claves

El tamaño de las claves para los certificados emitidos bajo el ámbito de la presente Política de Certificación es:

- Para las claves RSA de al menos 3072 bits.
- Para las claves ECDSA de al menos NIST ECC P-256.

6.1.6Parámetros de generación de la clave pública y verificación de la calidad

Se utilizan los parámetros definidos en el documento ETSI TS 119 312 “Electronic Signatures and Infraestructures (ESI); Cryptographic Suites”.

Los parámetros utilizados son los siguientes:

Signature Suite	**Hash Function**	**Padding Method**	**Signature algorithm**
sha256-with-rsa	sha256	emsa-pkcs1-v1.5	rsa
ecdsa-with-SHA256	sha256		ecdsa

ACCV lleva a cabo la validación de las claves ECC siguiendo el procedimiento definido en NIST SP 800-89

6.1.7 Propósitos de uso de claves

Los certificados emitidos bajo la presente política contienen los atributos

"KEY USAGE" y "EXTENDED KEY USAGE", tal como se define en el estándar X.509v3.

Las claves definidas por la presente política se utilizarán para usos descritos en el punto de este documento 1.3 Comunidad de usuarios y ámbito de aplicación.

La definición detallada del perfil de certificado y los usos de las claves se encuentra en el apartado 7 de este documento *"Perfiles de certificado, CRL y OCSP"*.

6.2 Protección de la Clave Privada

En este punto se hace siempre referencia a las claves generadas para los certificados emitidos bajo el ámbito de la presente Política de Certificación. La información sobre las claves de las entidades que componen la Autoridad de Certificación se encuentra en el punto 6.2 de la Declaración de Prácticas de Certificación (CPS) de la Agencia de Tecnología y Certificación Electrónica.

6.2.1 Estándares para los módulos criptográficos

Los certificados emitidos bajo esta política de certificación están basados en software, por lo que los estándares y controles del módulo criptográfico dependen del sistema operativo del suscriptor.

6.2.2 Control multipersona de la clave privada

Las claves privadas para los certificados emitidos bajo el ámbito de la presente Política de Certificación se encuentran bajo el control exclusivo de los suscriptores de los mismos.

6.2.3 Custodia de la clave privada

No se custodian claves privadas de los suscriptores de los certificados definidos por la presente política.

6.2.4 Copia de seguridad de la clave privada

No se custodian claves privadas de los suscriptores de los certificados definidos por la presente política.

6.2.5 Archivo de la clave privada.

No se archivan claves privadas de los suscriptores de los certificados definidos por la presente política.

6.2.6Introducción de la clave privada en el módulo criptográfico.

La generación de las claves vinculadas al certificado se realiza en tel equipo del usuario y bajo su control.

6.2.7Almacenamiento de la clave privada en el módulo criptográfico

La generación de las claves vinculadas al certificado se realiza en software. No hay módulos criptográficos.

6.2.8Método de activación de la clave privada.

En el caso de autogeneración de la clave por parte del usuario el mecanismo de activación lo impone el usuario en el momento de la generación. En el caso de claves contenidas en un fichero PKCS#12

la activación de la clave privada se realizará a través de la introducción de la palabra de paso de acceso a esta clave.

6.2.9Método de desactivación de la clave privada

La desactivación se realizará cerrando la aplicación que la utiliza o cerrando el módulo criptográfico asociado.

6.2.10Método de destrucción de la clave privada

La destrucción debe ir siempre precedida de la revocación del certificado asociado a la clave privada, si ésta sigue activa.

La tarea a realizar consiste en borrar el contenedor de la clave privada.

6.2.11Clasificación del módulo criptográfico

Ver la sección 6.2.1 de la presente política.

6.3 Otros Aspectos de la Gestión del par de Claves.

6.3.1 Archivo de la clave pública

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

6.3.2 Periodo de uso para las claves públicas y privadas

Los certificados emitidos al amparo de la presente política tienen una validez de tres (3) años.

El par de claves utilizado para la emisión de los certificados se crea para cada emisión, y por tanto también tienen una validez de tres (3) años.

Los certificados de ACCV RSA1 PROFESIONALES y ACCV ECC1 PROFESIONALES son válidos desde el día 25 de julio de 2023 hasta el 19 de julio de 2047.

6.4 Datos de activación

6.4.1 Generación y activación de los datos de activación

En el caso de autogeneración de las claves el mecanismo de activación lo impone el usuario en el momento de la generación, es responsabilidad y obligación del suscriptor la elección de los mecanismos de seguridad adecuados y el mantenimiento de la clave privada bajo su control.

6.4.2 Protección de los datos de activación

El suscriptor del certificado es el responsable de la protección de los datos de activación de su clave privada.

6.4.3 Otros aspectos de los datos de activación

No hay otros aspectos a cosnsiderar.

6.5 Controles de Seguridad Informática

6.5.1Requisitos técnicos específicos de seguridad informática

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

6.5.2 Evaluación del nivel de seguridad informática

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

6.6 Controles de Seguridad del Ciclo de Vida.

6.6.1Controles de desarrollo de sistemas

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

6.6.2 Controles de gestión de la seguridad

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

6.6.3 Controles de seguridad del ciclo de vida

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

6.7 Controles de Seguridad de la Red

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

6.8 Fuentes de tiempo

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

7 Perfiles de certificados, CRL y OCSP

7.1 Perfil de Certificado

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

7.1.1 Número de versión

Ademas de lo establecido en la Declaración de Prácticas de Certificación (CPS) de la ACCV, esta política de certificación especifica la emisión de un certificado con los usos de firma digital, autenticación y cifrado de claves.

7.1.2 Extensiones del certificado

El perfil del certificado emitido bajo la presente política es el siguiente:

Campo	**Valor**
Subject	
SerialNumber	número DNI/NIE Opcionalmente se podrá utilizar la semántica propuesta por la norma ETSI EN319 412-1
GivenName	Nombre del representante , tal como aparece en el DNI
SurName	Apellidos del representante, tal como aparece en el DNI
CommonName	Ver apartado 7.1.2
OrganizationIdentifier (2.5.4.97)	NIF de la entidad, tal como figura en los registros oficiales. Codificado Según la Norma Europea ETSI EN 319 412-1
Description (2.5.4.13)	Codificación del documento público que acredita las facultades del firmante o los datos registrales. Ver posibles descripciones en el apartado 7.1.2
Organization	Razón Social, tal como figura en los registros oficiales.
Country	ES
Version	V3
SerialNumber	Identificador único del certificado. Menor de 32 caracteres hexadecimales.
Algoritmo de firma	ACCV_RSA1_PROFESIONALES: sha256withRSAEncryption ACCV_ECC1_PROFESIONALES: ecdsa-with-SHA256
Issuer (Emisor)	DN de la CA que emite el certificado (ver punto 7.1.4)
Válido desde	Fecha de Emisión
Válido hasta	Fecha de Caducidad
Clave Pública	Octet String conteniendo la clave pública del suscriptor
Extended Key Usage	
	Client Authentication

	Adobe Authentic Documents Trust (1.2.840.113583.1.1.5)	
CRL Distribution Point	ACCV_RSA1_PROFESIONALES: http://www.accv.es/gestcert/accv_rsa1_profesionales.crl ACCV_ECC1_PROFESIONALES: http://www.accv.es/gestcert/accv_ecc1_profesionales.crl	
SubjectAlternativeName		
DirectoryName		
	CN=Nombre del representante|Apellido1 del representante|Apellido2 del representante	
	UID=NIF del representante	
Certificate Policy Extensions		
Policy OID	2.16.724.1.3.5.8	
Policy Notice	Certificado de representante de persona jurídica	
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	1.3.6.1.4.1.8149.3.30.3.0	Política de Certificación de Certificados Cualificados de Representante de Entidad en Soporte Software
Policy CPS Location	http://www.accv.es/legislacion_c.htm	
Policy Notice	`Certificado cualificado de Repr. en software expedido por por la ACCV (Pol. Ademuz, s/n. Burjassot, CP 46100, ESPAÑA. CIF A40573396)`	
Authority Information Access		
Access Method	Id-ad-ocsp	
Access Location	http://ocsp.accv.es	
Access Method	Id-ad-calssuers	
Access Location	ACCV_RSA1_PROFESIONALES: http://www.accv.es/gestcert/accv_rsa1_profesionales.crt ACCV_ECC1_PROFESIONALES: http://www.accv.es/gestcert/accv_ecc1_profesionales.crt	
Fingerprint issuer	Fingerprint del certificado de la CA que emite el certificado (ver CPS)	
Algoritmo de hash	SHA-256	
KeyUsage (críticos)		
	RSA	**ECC**

	Digital Signature Content Commintment Key Encipherment	Digital Signature Content Commintment Key agreement
QcStatement	**Campos QC (Qualified Certificate)**	
QcCompliance		El certificado es cualificado
QcType	eSign	Tipo particular de certificado cualificado
QcRetentionPeriod	15y	Periodo de retención de la información material
QcPDS	https://www.accv.es/fileadmin/Archivos/Practicas_de_certificacion/ACCV-PDS-V1.1-EN.pdf	Ubicación de PKI Disclosure Statement

7.1.3 Identificadores de objeto (OID) de los algoritmos

IIdentificador de Objeto (OID) de los algoritmos Criptográficos:

- SHA1withRSA (1.2.840.113549.1.1.5)
- SHA256withRSA (1.2.840.113549.1.1.11)
- ecdsa-with-SHA256 (1.2.840.10045.4.3.2)

7.1.4 Formatos de nombres

Los certificados contienen el distinguished name X.500 del emisor y el suscriptor del certificado en los campos issuer name y subject name respectivamente.

Los Issuer names admitidos para certificados emitidos bajo esta politica son:

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

SubjectAlternativeName contiene al menos el nombre y apellidos del suscriptor separados por el caracter "|" (DirectoryName).

Subject name: serialNumber=*DNI NIE*, givenName=*Nombre del representante*, surname=*Apellido1 del representante Apellido2 del representante*, cn=<DEFINIDO A CONTINUACIÓN>, Description=<DEFINIDO A CONTINUACIÓN>, OrganizationIdentifier=NIF, o=Razón Social, c=ES

El campo cn tiene un tamaño máximo de 64 caracteres según la RFC 5280, y debe tener la siguiente forma:.

Campo	**Contenido**	**Ejemplo**	**tamaño ***
NIF	número DNI/NIE	12345678Z	10

Nombre	Tal y como figura en el DNI/NIE	Pedro Antonio	
Apellido 1	Tal y como figura en el DNI/NIE	López	
Literal	(R:		4
NIF de la empresa	NIF de la empresa, tal como figura en los registros oficiales.	B0085974Z	9
Literal	)		2

*(contando espacio en blanco posterior)

El campo ***Description*** (2.5.4.13) se codifica el documento publico que acredita las facultades del firmante o los datos registrales. Ademas de las taxonomias recogidas, podrá utilizarse texto libre si la información que acredita la representación no se ajusta a uno de los tipos preestablecidos.

- Registro mercantil o similar

R: XXX /Hoja /Tomo /Sección /Libro /Folio /Fecha (dd-mm-aaaa) /Inscripción

- Documento notarial

N: Nombre Apellido1 Apellido2 /Núm Protocolo /Fecha Otorgamiento (dd-mm-aaaa)

- Boletín oficial

B: XXX/Fecha (dd-mm-aaaa) /Numero resolución

- Otros

Texto libre detallando la fuente de datos que acredita la representación

Todos los campos del certificado del Subject y del Subject Alternative Name, exceptuando los que se refieren a nombre DNS o direcciones de correo, se cumplimentan obligatoriamente en mayúsculas, prescindiendo de acentos.

7.1.5 Restricciones de los nombres

Los nombres contenidos en los certificados están restringidos a distinguished names X.500, únicos y no ambiguos.

El resto de campos que se incluyen en el certificado son los estrictamente necesarios que se marcan en el RFC-3739 para la obtención de un perfil de certificado cualificado.

7.1.6 Identificador de objeto (OID) de la Política de Certificación

El identificador de objeto definido por la ACCV para identificar la presente política es el siguiente:

1.3.6.1.4.1.8149.3.30.3.0

En este caso se añade un OID para identificar el tipo de entidad que se representa según la definición de los perfiles por la Administración General del Estado.

2.16.724.1.3.5.8 **Certificado de representante de persona jurídica**

En este caso se añade un OID para identificar el tipo de entidad que se representa según la normativa ETSI TS 119 411-2

0.4.0.194112.1.0	**Política de certificación para certificados cualificados EU emitidos a personas físicas**

7.1.7 Uso de la extensión “Policy Constraints”

No se hace uso de la extensión “*Policy Constraints*” en los certificados emitidos bajo la presente Política de Certificación.

7.1.8 Sintaxis y semántica de los cualificadores de política

La extensión de las Políticas de Certificación puede incluir dos campos de Calificación de Políticas(ambos opcionales):

- CPS Pointer: contiene la URL donde se publican las Políticas de Certificación
- User Notice: contiene un texto de descripción

7.1.9 Tratamiento semántico para la extensión “Certificate Policy”

La extensión “*Certificate Policy*” identifica la política que define las prácticas que ACCV asocia explícitamente con el certificado. Adicionalmente la extensión puede contener un cualificador de la política.

7.2 Perfil de CRL

7.2.1 Número de versión

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

7.2.2 CRL y extensiones

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

7.3 Perfil de OCSP

7.3.1Número de versión

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

7.3.2 Extensiones

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

8 Auditoría de conformidad

8.1 Frecuencia de los controles de conformidad para cada entidad

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

8.2 Identificación/cualificación del auditor

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

8.3 Relación entre el auditor y la entidad auditada

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

8.4 Tópicos cubiertos por el control de conformidad

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

8.5 Acciones a tomar como resultado de una deficiencia.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

8.6 Comunicación de resultados

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9 Requisitos comerciales y legales

9.1 Tarifas

9.1.1 Tarifas de emisión de certificado o renovación

Los precios para la emisión inicial y la renovación de los certificados a los que se refiere la presente política de certificación se recogen en la Lista de Tarifas de la Agencia de Tecnología y Certificación Electrónica. Esta Lista se publica en la página web de la ACCV www.accv.es

9.1.2 Tarifas de acceso a los certificados

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.1.3 Tarifas de acceso a la información de estado o revocación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.1.4 Tarifas de otros servicios como información de políticas

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.1.5Política de reintegros

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.2 Capacidad financiera

9.2.1 Indemnización a los terceros que confían en los certificados emitidos por la ACCV.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.2.2 Relaciones fiduciarias

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.2.3 Procesos administrativos

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.3 Política de Confidencialidad

9.3.1Información confidencial.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.3.2 Información no confidencial

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.3.3 Divulgación de información de revocación /suspensión de certificados

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.4 Protección de datos personales

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.4.1 Plan de Protección de Datos Personales.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.4.2 Información considerada privada.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.4.3 Información no considerada privada.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.4.4 Responsabilidades.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.4.5 Prestación del consentimiento en el uso de los datos personales.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.4.6 Comunicación de la información a autoridades administrativas y/o judiciales.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.4.7 Otros supuestos de divulgación de la información.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.5 Derechos de propiedad Intelectual

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV..

9.6 Obligaciones y Responsabilidad Civil

9.6.1 Obligaciones de la Entidad de Certificación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.6.2 Obligaciones de la Autoridad de Registro

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.6.3 Obligaciones de los suscriptores

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.6.4 Obligaciones de los terceros confiantes en los certificados emitidos por la ACCV

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.6.5 Obligaciones del repositorio

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.7 Renuncias de garantías

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.8 Limitaciones de responsabilidad

9.8.1 Garantías y limitaciones de garantías

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.8.2 Deslinde de responsabilidades

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.8.3 Limitaciones de pérdidas

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.9Indemnizaciones

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.10 Plazo y finalización.

9.10.1 Plazo.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.10.2 Finalización.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.10.3 Supervivencia.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.11 Notificaciones.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.12 Modificaciones.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.12.1 Procedimientos de especificación de cambios

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.12.2 Procedimientos de publicación y notificación.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.12.3 Procedimientos de aprobación de la Declaración de Prácticas de Certificación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.13 Resolución de conflictos.

9.13.1 Resolución extrajudicial de conflictos.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.13.2 Jurisdicción competente.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.14 Legislación aplicable

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.15 Conformidad con la Ley aplicable.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.16 Cláusulas diversas.

9.16.1Acuerdo integro

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.16.2Asignación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.16.3Severabilidad

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.16.4Cumplimiento (honorarios de los abogados y renuncia a los derechos)

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.16.5Fuerza Mayor

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.17Otras estipulaciones

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

10 Anexo I

CONTRATO DE CERTIFICACIÓN – CÓDIGO 1.3.6.1.4.1.8149.3.30

Secció 1 – Dades del subscriptor / Sección 2 – Datos del suscriptor

Cognoms/*Apellidos*:

Nom/*Nombre*:

DNI/NIF: Tel.:

Adreça de correu electrònic/*Dirección correo electrónico*:

Adreça postal/Dirección postal:

Població/Población: Província/Provincia:

Secció 2 – Dades de l'Entitat / *Sección 1 – Datos de la Entidad*

Raó Social/Razón Social::

CIF de l'Entitat/*CIFde la Entidad*:

Domicili Fiscal/Domicilio Fiscal::

Població/Población: Província/Provincia:

PIN : PUK: Tel. suport/ tel. soporte **963 866 014** **www.accv.es**

Secció 3 – Dades del operador del Punt de Registre / *Sección 3 – Datos del operador del Punto de Registro*

Nom i cognoms/*Nombre y Apellidos:*

Secció 4 - Data i Firma / Sección 4 – *Fecha y Firma*

Subscric el present contracte de certificació associat a la Política de Certificació de Certificats Reconeguts de Representant d'Entitat amb codi 1.3.6.1.4.1.8149.3.30, emés per la Agencia de Tecnología y Certificación Electrónica. Declare que conec i accepte les normes d'utilització d'este tipus de certificats que es troben exposades en http://www.accv.es. Declare, així mateix, que les dades posades de manifest són certes.

Suscribo el presente contrato de certificación asociado a la Política de Certificación de Certificados Reconocidos de Representante de Entidad con código 1.3.6.1.4.1.8149.3.30*, emitido por la la Agencia de Tecnología y Certificación Electrónica. Declaro conocer y aceptar las normas de utilización de este tipo de certificados que se encuentran expuestas en http://www.accv.es. Declaro, asimismo, que los datos puestos de manifiesto son ciertos.*

Firma del sol.licitant

Firma del solicitante

Firma i segell del Punt de Registre

Firma y sello del Punto de Registro

Firmat/*Firmado*:

Firmat/*Firmado:*

Exemplar per al sol.licitant - Anvers / *Ejemplar para el solicitante - Anverso*

CONTRATO DE CERTIFICACIÓN – CÓDIGO 1.3.6.1.4.1.8149.3.30
Condiciones de utilización de los certificados

1. Los certificados asociados a la Política de Certificación de Certificados Reconocidos de Representante de Entidad, emitidos por la Agencia de Tecnología y Certificación Electrónica son del tipo X.509v3 y se rigen por la Declaración de Prácticas de Certificación de la Agencia de Tecnología y Certificación Electrónica, en tanto que Prestador de Servicios de Certificación, así como por la Política de Certificación referida. Ambos documentos se deben interpretar según la legislación de la Comunidad Europea, el Ordenamiento Jurídico Español y la legislación propia de la Generalitat.
2. Los solicitantes deberán ser personas físicas, en posesión de un NIF, un NIE u otro documento de identificación válido en Derecho, con poder bastante para representar a la Entidad a la que hace referencia el certificado.
3. El solicitante es responsable de la veracidad de los datos aportados en todo momento a lo largo del proceso de solicitud y registro. Será responsable de comunicar cualquier variación de los datos aportados para la obtención del certificado.
4. El titular del certificado es responsable de la custodia de su clave privada y de comunicar a la mayor brevedad posible cualquier pérdida o sustracción de esta clave.
5. El titular del certificado es responsable de limitar el uso del certificado a lo dispuesto en la Política de Certificación asociada, que es un documento público y que se encuentra disponible en http://www.accv.es. En especial, este certificado de Representante de Entidad podrá ser utilizado cuando se admita en las relaciones entre la Entidad y las Administraciones Públicas o en la contratación de bienes o servicios que sean propios o concernientes a su giro o tráfico ordinario.
6. La Agencia de Tecnología y Certificación Electrónica no se responsabiliza del contenido de los documentos firmados haciendo uso de los certificados por ella emitidos.
7. La Agencia de Tecnología y Certificación Electrónica es responsable del cumplimiento de las legislaciones Europea, Española y Valenciana, por lo que a Firma Electrónica se refiere. Es, asimismo, responsable del cumplimiento de lo dispuesto en la Declaración de Prácticas de Certificación de la Agencia de Tecnología y Certificación Electrónica y en la Política de Certificación asociada a este tipo de certificados.
8. El periodo de validez de estos certificados es de tres (3) años. Para su renovación deberán seguirse el mismo procedimiento que para la primera solicitud o bien los procedimientos previstos en la Política de Certificación asociada.
9. Los certificados emitidos perderán su eficacia, además de al vencimiento del periodo de validez, cuando se produzca una revocación, cuando se inutilice el soporte del certificado, ante resolución judicial o administrativa que ordene la pérdida de eficacia, por inexactitudes graves en los datos aportados por el solicitante, por extinción o disolución de la personalidad jurídica de la Entidad, por alteración de las condiciones de custodia del certificado. Otras condiciones para la pérdida de eficacia se recogen en la Declaración de Prácticas de Certificación y en la Política de Certificación asociada a este tipo de certificado.
10. La documentación a aportar por la persona física solicitante del certificado será el Documento Nacional de Identidad, NIE o Pasaporte español, válido y vigente. El solicitante deberá aportar los datos relativos a la constitución y personalidad jurídica y la extensión y facultades de representación del solicitante.
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 de la existencia de un fichero automatizado de datos de carácter personal creado bajo la responsabilidad de la Agencia de Tecnología y Certificación Electrónica, denominado \"Usuarios de firma electrónica\". La finalidad de dicho fichero es la de servir a los usos relacionados con los servicios de certificación prestados por la Agencia de Tecnología y Certificación Electrónica. 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 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 de procesamiento y objeción sobre sus datos de carácter personal dirigiendo escrito a la Agencia de Tecnología y Certificación Electrónica, a través de cualquiera de los Registros de Entrada de la Generalitat Valenciana e indicando claramente esta voluntad.
14. Se aconseja al usuario realizar el cambio del PIN inicial que aparece en el presente contrato a través de las herramientas que pone a su disposición la Agencia de Tecnología y Certificación Electrónica.

Con la firma del presente documento se autoriza a la Agencia de Tecnología y Certificación Electrónica a consultar los datos de identidad que consten en el Ministerio de Interior, evitando que el ciudadano aporte fotocopia de su documento de identidad.

Ejemplar para el solicitante – Reverso

CONTRATO DE CERTIFICACIÓN – CÓDIGO 1.3.6.1.4.1.8149.3.30

Secció 1 – Dades del subscriptor / Sección 2 – Datos del suscriptor

Cognoms/*Apellidos*:

Nom/*Nombre*:

DNI/NIF: Tel.:

Adreça de correu electrònic/*Dirección correo electrónico*:

Adreça postal/Dirección postal:

Població/Población: Província/Provincia:

Secció 2 – Dades de l'Entitat / *Sección 1 – Datos de la Entidad*

Raó Social/Razón Social::

CIF de l'Entitat/*CIFde la Entidad*:

Domicili Fiscal/Domicilio Fiscal:

Població/Población: *Província/Provincia:*

Tel. suport/ tel. soporte **963 866 014** **www.accv.es**

Secció 3 – Dades del operador del Punt de Registre / *Sección 3 – Datos del operador del Punto de Registro*

Nom i cognoms/*Nombre y Apellidos:*

Secció 4 - Data i Firma / Sección 4 – *Fecha y Firma*

Subscric el present contracte de certificació associat a la Política de Certificació de Certificats Reconeguts de Representant d'Entitat amb codi 1.3.6.1.4.1.8149.3.30, emés per la Agencia de Tecnología y Certificación Electrónica. Declare que conec i accepte les normes d'utilització d'este tipus de certificats que es troben exposades en http://www.accv.es. Declare, així mateix, que les dades posades de manifest són certes.

Suscribo el presente contrato de certificación asociado a la Política de Certificación de Certificados Reconocidos de Representante de Entidad con código 1.3.6.1.4.1.8149.3.30, emitido por la la Agencia de Tecnología y Certificación Electrónica. Declaro conocer y aceptar las normas de utilización de este tipo de certificados que se encuentran expuestas en http://www.accv.es. Declaro, asimismo, que los datos puestos de manifiesto son ciertos.

Firma del sol.licitant

Firma del solicitante

Firma i segell del Punt de Registre

Firma y sello del Punto de Registro

Firmat/*Firmado*:

Firmat/*Firmado:*

Nº de petició Exemplar per a la ACCV/ *Ejemplar para la ACCV*

11Anexo II – Formulario de solicitud de revocación de certificado

SOLICITUD DE REVOCACIÓ DE CERTIFICAT ***SOLICITUD DE REVOCACIÓN DE CERTIFICADO***
Data/Fecha:.....
Secció 1 – Dades del subscriptor / *Sección 2 – Datos del suscriptor* Cognoms/*Apellidos*: Nom/*Nombre*: DNI/NIF: Tel.: **Secció 2 – Dades de l'Entitat / Sección 1 – *Datos de la Entidad*** *Raó Social/Razón Social:*: CIF de l'Entitat/*CIFde la Entidad*:
Secció 2 – Identificació del certificat* / *Sección 2* – Identificación del certificado* Certificado personal: Nº de petición del certificado:
Secció 3 - Motiu de la revocació* / Sección 3 – *Motivo de la revocación** * La simple voluntad de revocación del suscriptor o del solicitante del certificado es un motivo válido para la solicitud de la misma.
Secció 4 – Autorització* / *Sección 2* – Autorización* Subscriptor del certificat *Subscriptor del certificado* *Firma* Solicitat al operador del Punt de Registre d'Usuari / Solicitado al operador de Punto de Registro de Usuario: Firma:

Exemplar per a la Agencia de Tecnología y Certificación Electrónica
Ejemplar para la Agencia de Tecnología y Certificación Electrónica

SOLICITUD DE REVOCACIÓ DE CERTIFICAT ***SOLICITUD DE REVOCACIÓN DE CERTIFICADO***

Data/Fecha:.....

Secció 1 – Dades del subscriptor / *Sección 2 – Datos del suscriptor*

Cognoms/*Apellidos*:

Nom/*Nombre*:

DNI/NIF: Tel.:

Secció 2 – Dades de l'Entitat / Sección 1 – *Datos de la Entidad*

Raó Social/Razón Social::

CIF de l'Entitat*/CIFde la Entidad:*

Secció 2 – Identificació del certificat* / *Sección 2* – Identificación del certificado*
Certificado personal: Nº de petición del certificado:

Secció 3 - Motiu de la revocació* / Sección 3 – *Motivo de la revocación**

* La simple voluntad de revocación del suscriptor o del solicitante del certificado es un motivo válido para la solicitud de la misma.

Secció 4 – Autorització* / *Sección 2* – Autorización*
Subscriptor del certificat
Subscriptor del certificado

Firma

Solicitat al operador del Punt de Registre d'Usuari / Solicitado al operador de Punto de Registro de Usuario:

Firma:

Exemplar per al sol·licitant / Ejemplar para el solicitante

12Anexo III – Mecanismo de Video Identificación

A continuación, se describe el mecanismo de video identificación asíncrona utilizado por ACCV – ISTEC para llevar a cabo la identificación no presencian tal y como se regula en la Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados.

Para esta labor se ha utilizado como producto de identificación remota por vídeo VIDEO HIGH de la empresa electronic ID. Este producto ha pasado todas las revisiones y auditorias necesarias que exige dicha orden.

1. El usuario introduce su NIF/NIE: se llama a ARCA para ver si dispone de certificados activos SW o peticiones web activas de ciudadano o de representante y autorizaciones SW de representante.

Si no tiene ninguna solicitud pendiente el solicitante salta al paso 2.

2. Crear solicitud:

2.1. Introduce nombre y apellidos.

2.2. Acepta las condiciones de la identificación y del contrato de certificación, así como consiente expresamente la realización del procedimiento de identificación no presencial.

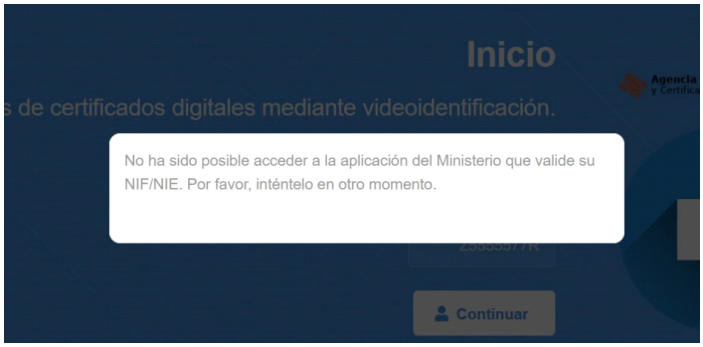
2.3. Introduce el teléfono: tras validarlo se le envía un mensaje SMS con un código que debe escribir en un cuadro de texto. Tiene 3 intentos. Si lo escribe bien irá al siguiente paso.

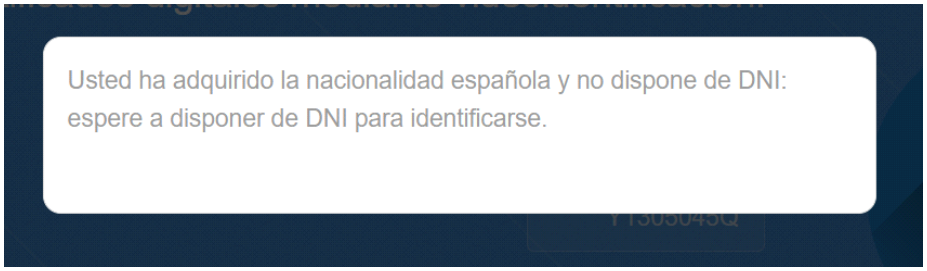
2.4. Introduce el e-mail. Tras validarlo:

2.4.1. Se llama al SVDRI para obtener nombre y apellidos.

Si el SVDRI responde que hay algún problema con el NIF introducido la solicitud no continua y no llega a enviar el correo.

Si el SVDRI no responde en ese momento se reintenta 2 veces más y si sigue sin responder se guardan los 3 errores de conexión y se continúa el proceso.





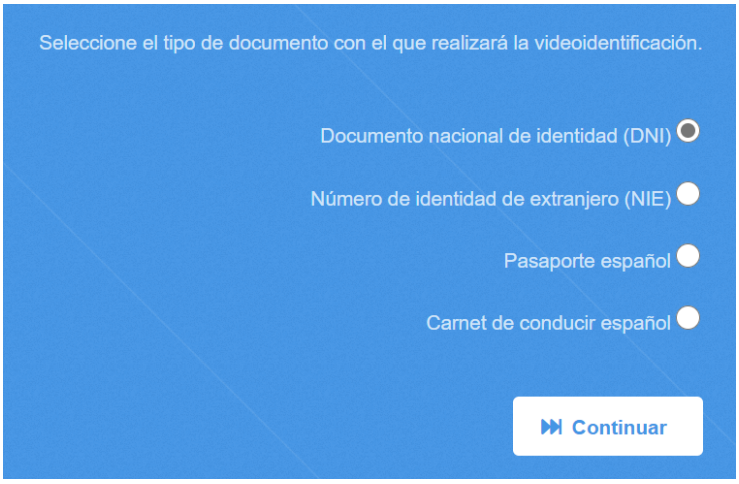
2.4.2. Se guarda la información de la solicitud.

Se almacenan las evidencias iniciales para su recuperación, independientemente del resultado final de la solicitud (se almacenan las exitosas y las fallidas)

2.4.3. Se genera un código que se envía al e-mail proporcionado.

3. El usuario pincha en el enlace del correo donde está el código y accede a una página donde se le envía un código por SMS para ser validado. Tiene 3 intentos. Si lo escribe bien irá al siguiente paso.

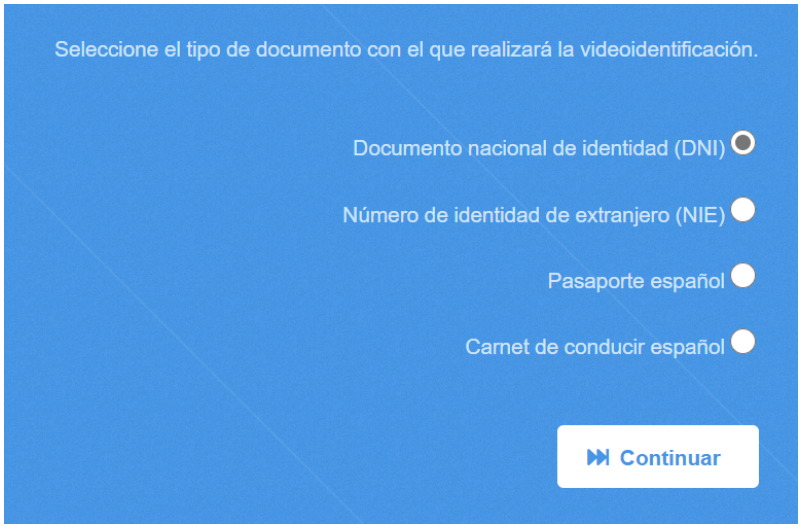
4. El pago del certificado se ha realizado previamente por lo que se va directamente a la selección de documento de identificación.

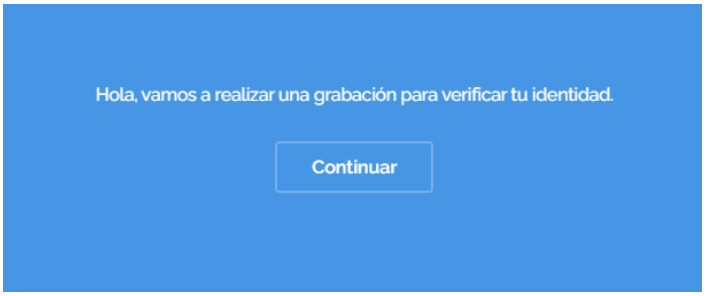


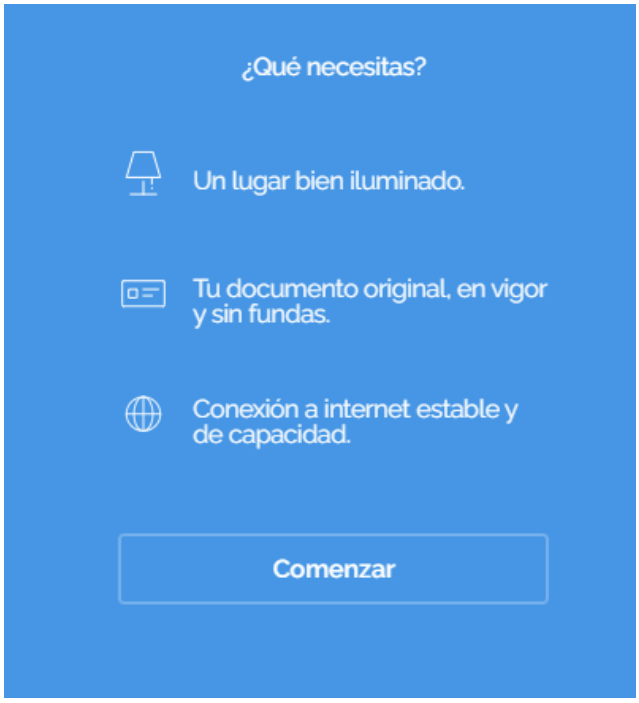
4.1. En el caso de corte de la conexión se le permitirá continuar con el proceso

5. Ir a la página de videoidentificación:

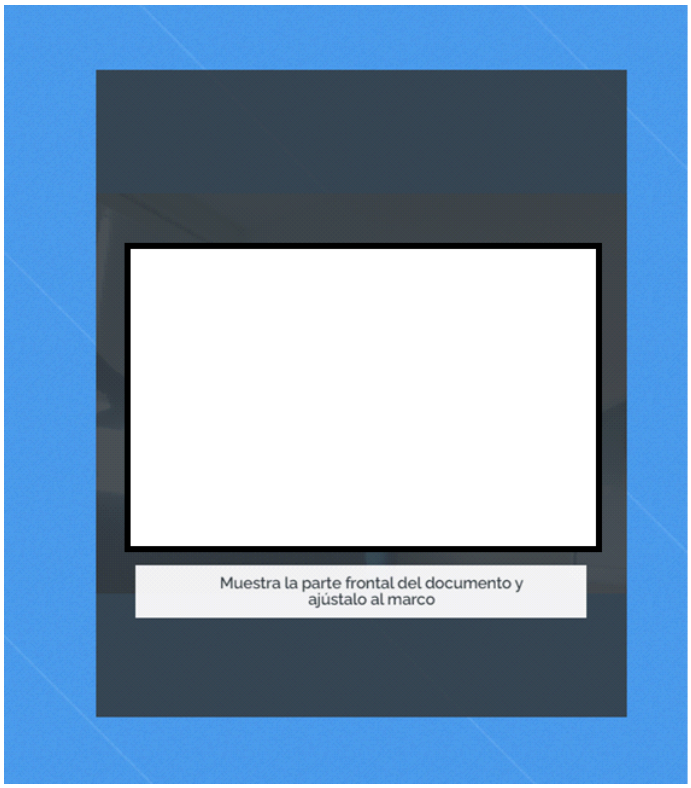
A partir de aquí se inicia el proceso gestionado por la herramienta VideoID High





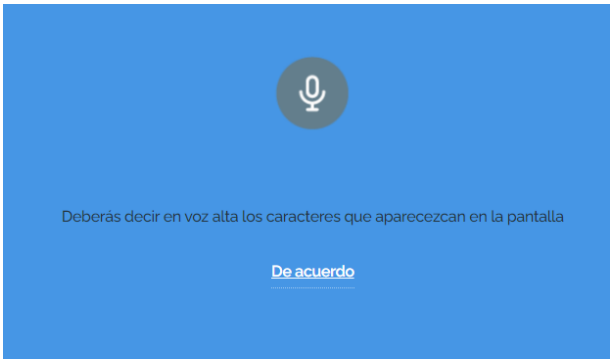


Debe presentar el anverso del documento

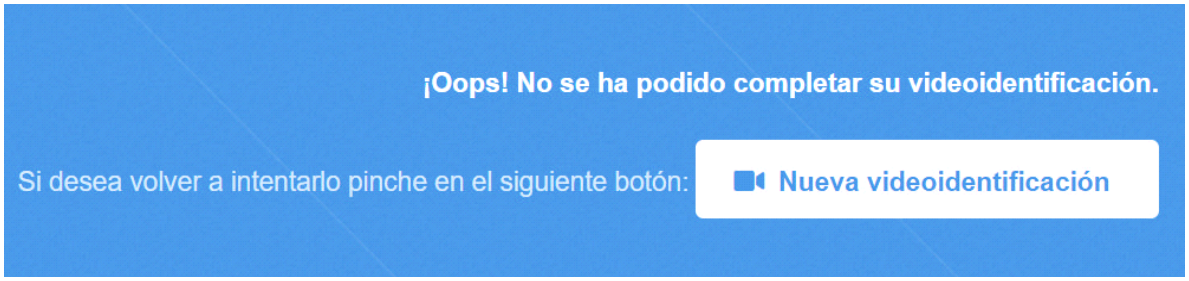


A continuación el reverso.

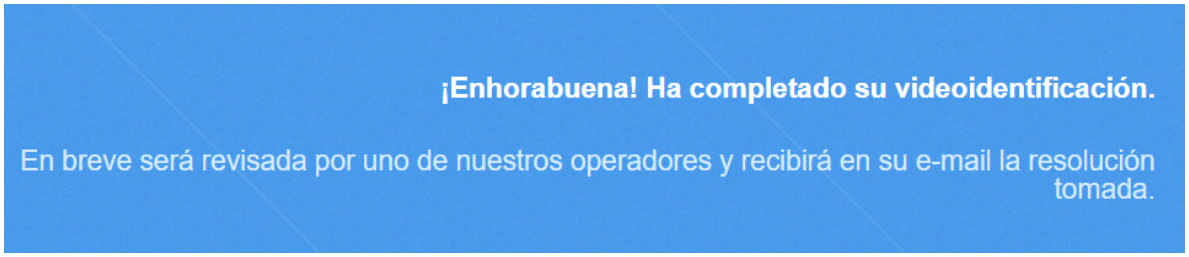
Después le solicitará que sonría a la camara y finalmente que lea una serie de caracteres aleatorios.



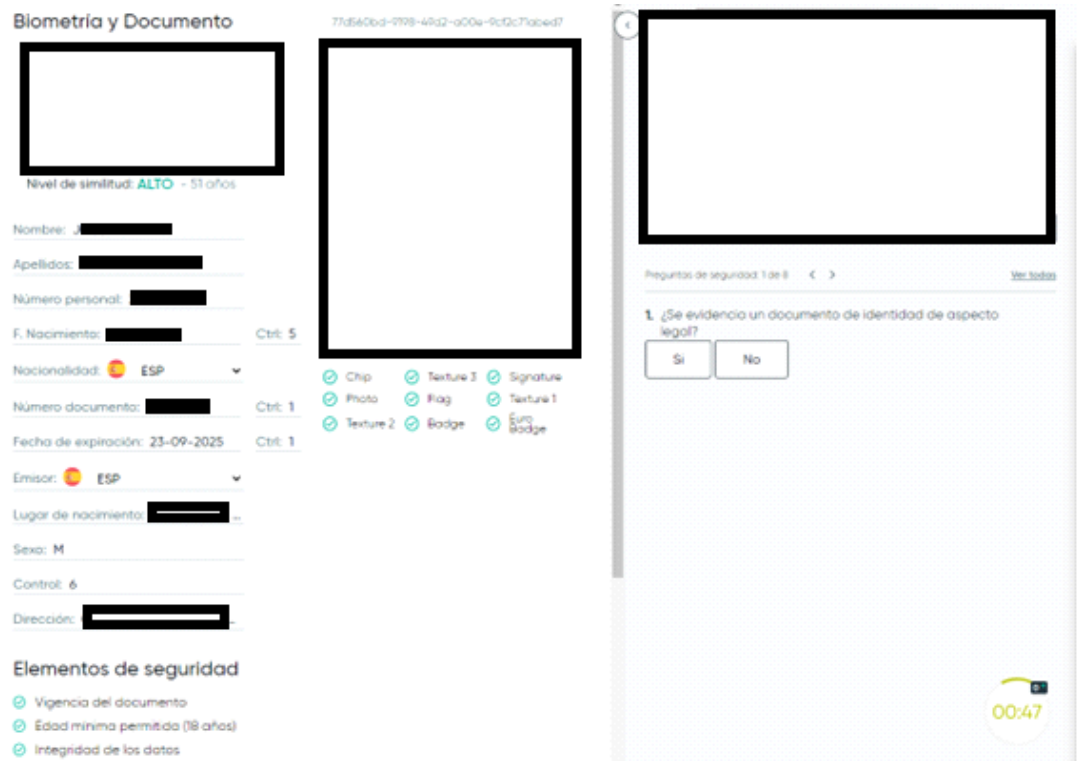
5.1. Si la videoidentificación es fallida se muestra un botón para volver a empezarla. La videoidentificación fallida crea evidencias en CouchDB.



5.2. Una vez concluida con éxito se muestra un mensaje al usuario, que en este punto acaba su intervención. Si el NIF obtenido en la videoidentificación difiere del introducido en la solicitud se marca esta como "revisable por operador". También se marca como "revisable por operador" si el nombre y apellidos de la solicitud (obtenidos por SVDRI o introducidos por el usuario) no son iguales a los que devuelve la videoidentificación. En los dos casos advierte de esta circunstancia en un correo a todos los operadores.



6. Un operador verifica la videoidentificación:



6.1. Si se rechaza por alguno de los motivos ofrecidos: se envía correo al usuario informando que accediendo al mismo lugar del punto 1 e introduciendo su DNI puede volver a intentarlo. Todas estas acciones crean evidencias en la aplicación.

6.2. La acepta: la solicitud se guarda como preaceptada. Un proceso revisa periodicamente estas solicitudes:

6.2.1. Si la solicitud se encuentra "revisable por operador" no hace nada. En las revisiones diarias por parte de los operadores se debe comprobar, en ese momento se le muestra en NIF de la misma así como la foto del documento para que pueda determinar si los números son diferentes o no. Si son diferentes la solicitud es rechazada. Si son iguales se revisa nombre y apellidos, pudiendo ser modificados por el operador de acuerdo a lo que se vea en la foto y se desmarca el flag "revisable por operador".

6.2.2. Si la solicitud no se encuentra "revisable por operador" se crean las evidencias en CouchDB y se llama a ARCA para generar una petición web que continua si tramite normal. A ARCA se le pasan como evidencias el contrato que se mostró en el punto 2.2 y la respuesta del SVDRI.

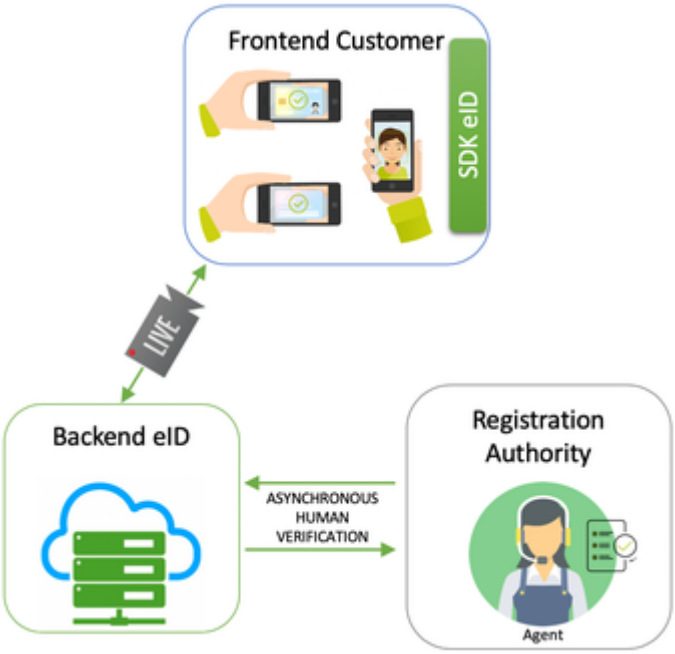
A continuación, adjuntamos un documento proporcionado por el fabricante que explica el funcionamiento de la solución VideoID High

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:

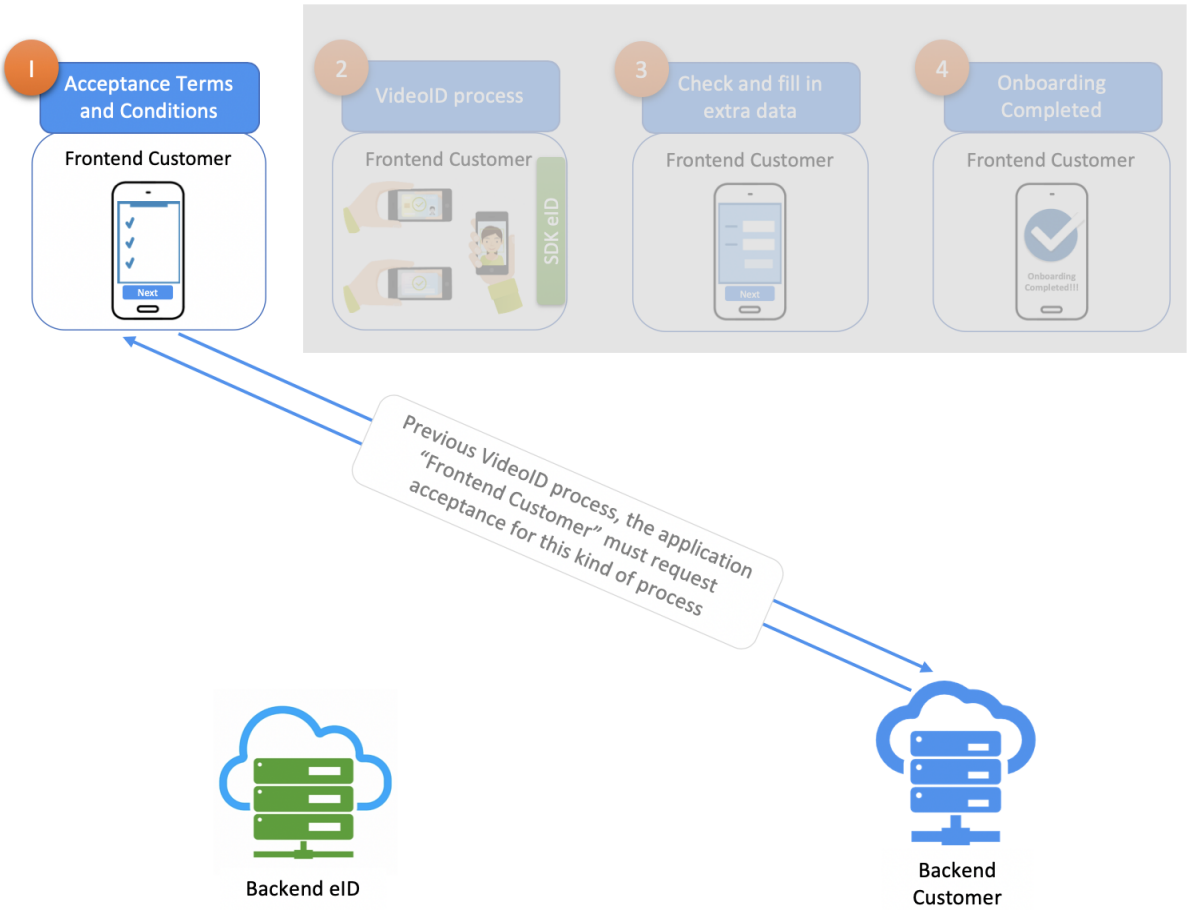
1. Acceptance of terms and conditions before starting the process
2. VideoID Process
3. Additional data and checks

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.

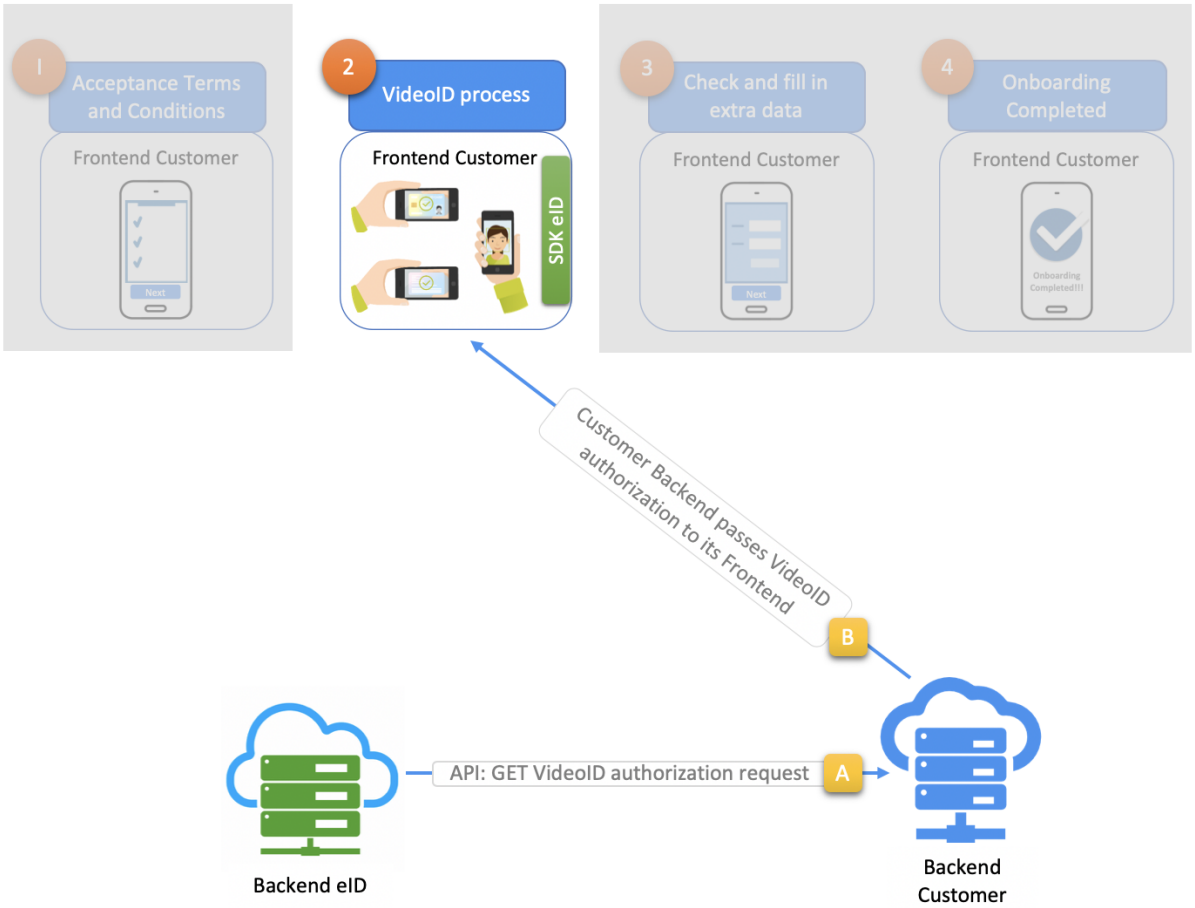


2) VideoID Process

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.

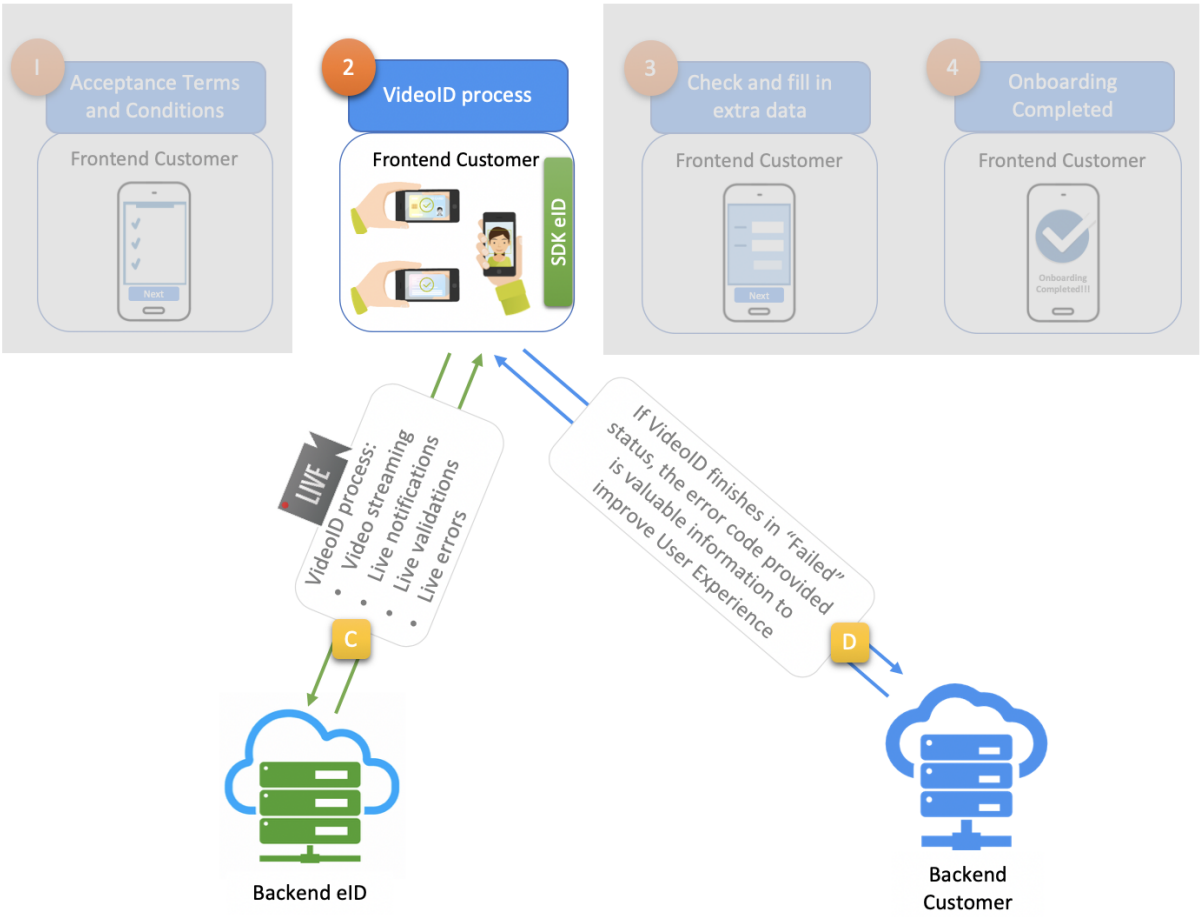
Note: see diagram below.



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.

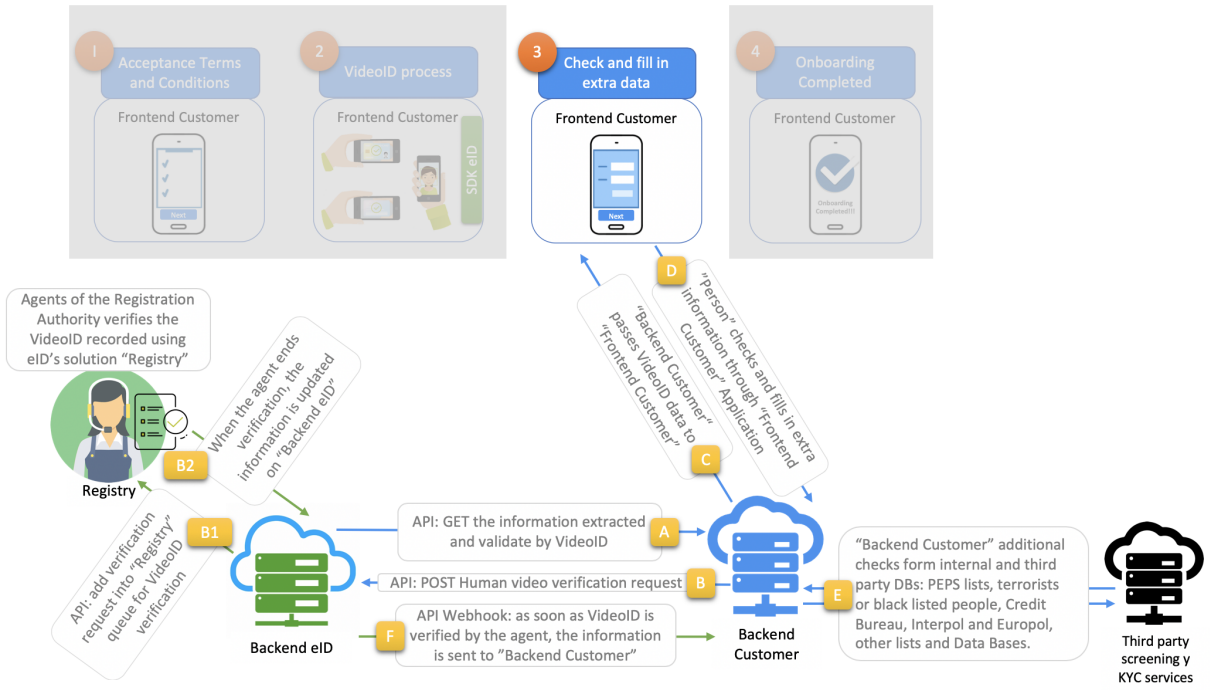
Note: only VideoIDs completed in "Completed" status can be sent for verification by human agents.

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).

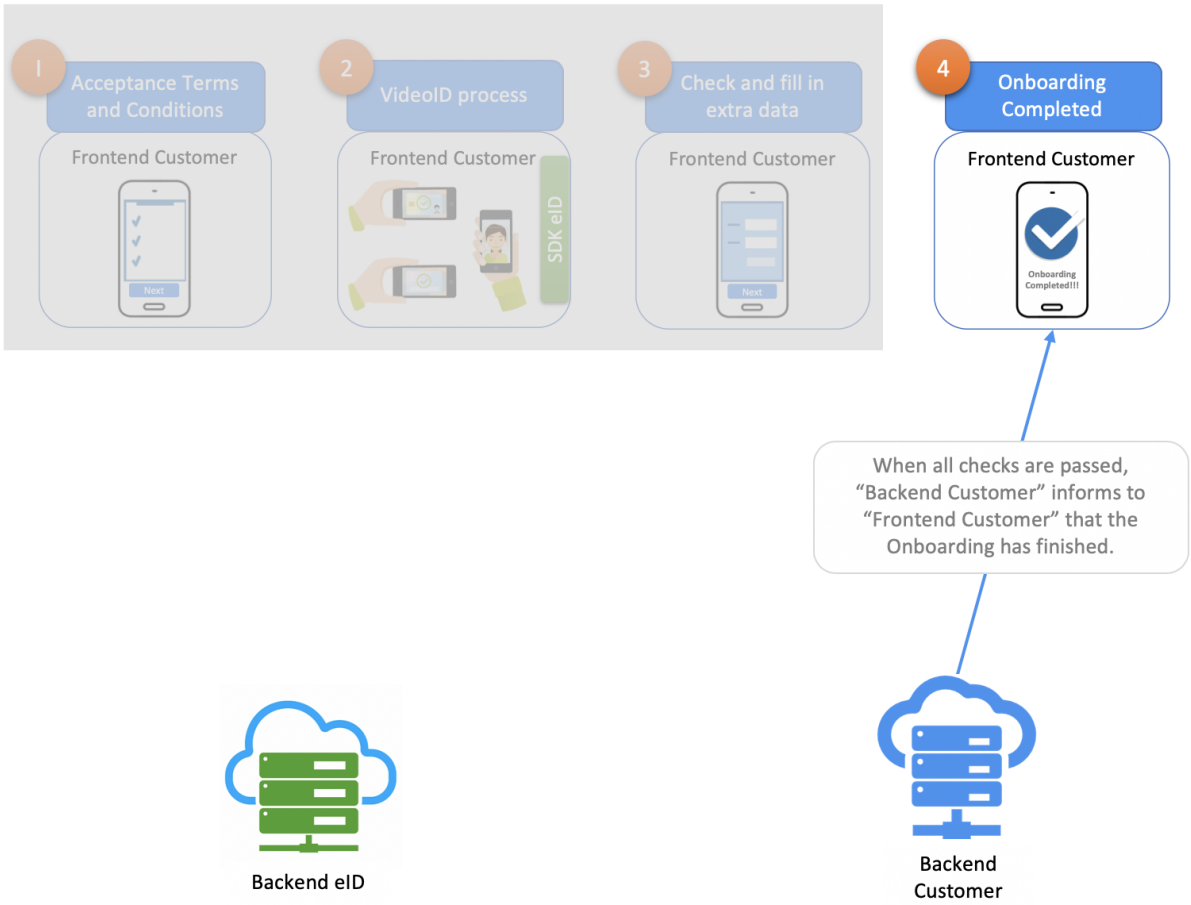
C: once the data collected by VideoID is retrieved, the Customer can show it to the user through the "Frontend Customer" to pre-fill the form and ask him to fill in the remaining fields, improving the user experience.

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 avalaible for Costumers

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.