Agencia de Tecnología y Certificación Electrónica

Política de Certificación de Certificados Cualificados en dispositivo seguro para ciudadanos

Fecha: 20/03/2021	**Versión:** 7.0.5
Estado: APROBADO	**Nº de páginas:** 44
OID: 1.3.6.1.4.1.8149.3.6.7.0	**Clasificación: PUBLICO**
Archivo: ACCV-CP-06V7.0.5-ES-2021.doc	
Preparado por: Agencia de Tecnología y Certificación Electrónica - ACCV	

ISTEC Firmado digitalmente por ISTEC
Fecha: 2021.05.13 15:32:31 +02'00'

Cambios

Versión	Autor	Fecha	Observaciones
7.0.1	ACCV	03/05/2018	Cambios de adaptación RFC3647
7.0.2	ACCV	18/06/2019	Modificaciones por CAB/Forum
7.0.3	ACCV	20/01/2020	Modificaciones por cambio de correo
7.0.4	ACCV	10/03/2020	Cambios de adaptación RFC3647
7.0.5	ACCV	20/03/2020	Policy Notice

Tabla de Contenido

1 INTRODUCCIÓN

1.1 Presentación

El presente documento es la Política de Certificación asociada a los certificados cualificados para ciudadanos en soporte de dispositivo seguro, que contiene las reglas a las que se sujeta la gestión y 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 para ciudadanos, sobre dispositivo seguro de creación de firma –tarjeta criptográfica–. Mediante los certificados cualificados y los dispositivos seguros de creación de firma asociados a esta Política de Certificación se generarán firmas electrónicas reconocidas

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 en dispositivo seguro para ciudadanos
Calificador de la política	`Certificado cualificado para Ciudadano expedido por la ACCV (Pol. Ademuz, s/n. Burjassot, CP 46100, ESPAÑA. CIF A40573396)`
Versión de la política	7.0.5
Estado de la política	APROBADO
Referencia de la política / OID (Object Identifier)	1.3.6.1.4.1.8149.3.6.7.0
Fecha de emisión	20 de Marzo de 2021
Fecha de expiración	No aplicable.
CPS relacionada	Declaración de Prácticas de Certificación (CPS) de la ACCV. Versión 4.0. OID: 1.3.6.1.4.1.8149.2.4.0 `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

La CA que puede emitir certificados acordes con esta política es ACCVCA-120 perteneciente a la Agencia de Tecnología y Certificación Electrónica, cuya función es la emisión de certificados de entidad final para los suscriptores de ACCV. El certificado de ACCVCV-120 es válido desde el día 13 de octubre de 2011 hasta el 1 de enero de 2027.

1.3.2 Autoridades de Registro

La lista de Autoridades de Registro (Puntos de Registro de Usuario) que gestionan las solicitudes 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 cualquier persona física en posesión de los elementos de identificación requeridos (DNI, NIE, etc.).

El soporte de claves y certificados es tarjeta criptográfica Giesecke & Devrient (G&D) Sm@rtCafé Expert 3.2 o y Giesecke & Devrient (G&D) Sm@rtCafé Expert 7.0 versiones posteriores. En caso de acreditarse otros dispositivos criptográficos serán recogidos en el presente documento, en su punto 6.1.8 Hardware/software de generación de claves

Se limita el derecho de solicitud de certificados definido en la presente Política de Certificación a personas físicas. No se aceptarán solicitudes de certificación realizadas en nombre de personas jurídicas, entidades u organizaciones.

1.3.4 Partes confiantes

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

- Los usuarios de clientes de correo electrónico S/MIME en el ámbito de la verificación de la identidad del emisor de mensajes de correo electrónico y del cifrado de los mismos.
- Las aplicaciones y servicios pertenecientes a la Generalitat, a alguna de las entidades u organizaciones vinculados a la Generalitat o a Administraciones Públicas o Corporativas con las que se haya firmado convenio de certificación.
- Las aplicaciones y servicios de cualquier Administración Pública española o europea.
- Las aplicaciones o servicios de cualquier entidad publica o privada que requiera de la identificación electrónica segura o la firma digital de los ciudadanos.

1.3.5 Otros 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

De acuerdo con lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

1.5.2 Persona de Contacto

De acuerdo con 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

De acuerdo con lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV

1.5.4 Procedimiento de aprobación de la CPS

De acuerdo con lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

1.6 Definiciones y Acrónimos

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

ACCV se ajusta a la versión actual de los "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates", publicados en https://www.cabforum.org/.In. En caso de que haya alguna incoherencia entre esta política de certificación y los requisitos del CAB Forum, éstos tendrán prioridad 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.

El derecho de solicitud de certificados definido en la presente Política de Certificación se encuentra limitado a personas físicas. No se aceptarán solicitudes de certificación realizadas en nombre de personas jurídicas, entidades u organizaciones. Por tanto, no se considera necesaria la identificación de ninguna organización.

3.2.3 Autenticación de la identidad de un individuo.

La autentificación de la identidad del solicitante de un certificado se realizará mediante su identificación ante la Autoridad de Registro correspondiente. En el caso de presentación presencial ante un Operador de Punto de Registro habilitado para la emisión de este tipo de certificados, la identidad deberá acreditarse mediante la presentación del Documento Nacional de Identidad (DNI), el pasaporte español, el Número de Identificación de Extranjero (NIE) del solicitante u otros medios admitidos en Derecho. Se podrá prescindir de la presentación presencial del solicitante mediante un poder notarial en el que se delegue expresamente la obtención del certificado en un tercero. En el caso de la identificación a distancia ante la Autoridad de Registro, el solicitante accederá al Área de Servicios de Certificación Personal (APSC) identificándose mediante un certificado personal reconocido de la ACCV o del DNIe.

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.

En este tipo de certificados se incluye la dirección de correo electrónico del suscriptor como elemento necesario para soportar el protocolo S/MIME.

Para verificar esta cuenta de correo electrónico, ACCV enviará un correo electrónico a dicha cuenta con un enlace web único. El solicitante deberá hacer clic en este enlace para confirmar la dirección y así poder continuar con el proceso de generación. Este enlace web único caducará en 30 días sin posibilidad de reutilización.

3.2.4 Información no verificada

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

3.2.5 Validación de la autoridad

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

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 puede realizar utilizando las técnicas para la autenticación e identificación inicial (descrita en el punto 3.2.3 *Autenticación de la identidad de un individuo*, de esta Política de Certificación). En el caso de identificación no presencial frente a la Autoridad de registro, el usuario accederá al Área Personal de Servicios de Certificación (APSC) identificándose mediante un certificado cualificado personal de la ACCV o el DNIe.

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

La política de identificación para las solicitudes de revocación acepta los siguientes métodos de identificación:

- Presencial. Es el mismo que para el registro inicial descrito en el punto 3.2.3. *Autenticación de la identidad de un individuo*, de esta Política de Certificación
- Telemática. Mediante la petición a través del formulario de revocación ubicado en el Área Personal de Servicios de Certificación (en http://www.accv.es).´
- Telefónica. Mediante la respuesta a las preguntas realizadas desde el servicio de soporte telefónico disponible en el número 963 866 014

.

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

4.1.1 Quien puede enviar una solicitud de certificado

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

4.1.2 Proceso de registro y responsabilidades

El ciudadano que solicite un certificado emitido bajo esta política deberá dirigirse a la Autoridad de Registro de la ACCV, presentando la documentación necesaria establecida en esta política (punto 3.2.3).

La lista de Autoridades de Registro autorizadas se encuentra en https://www.accv.es.

En el caso de las solicitudes presenciales, los datos de la solicitud se obtienen de la documentación oficial aportada por el solicitante y la consulta a los registros oficiales disponibles, y es responsabilidad de la ACCV verificar los datos y asegurar la disponibilidad de las autoridades de registro y sistemas asociados, así como informar al solicitante de los diferentes estados por los que pasa la solicitud. Es responsabilidad del solicitante proporcionar información precisa en su solicitud.

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.

En el caso de las solicitudes a distancia sin identificación de identidad interactiva, los datos se obtienen de la información disponible en el soporte digital utilizado para identificar al solicitante, y es responsabilidad de la ACCV verificar los datos y asegurar la disponibilidad de las autoridades de registro y sistemas asociados, así como informar al solicitante de los diferentes estados por los que pasa la solicitud. Es responsabilidad del solicitante proporcionar información precisa en su solicitud.

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.

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 documento de comparecencia. Una vez completa la solicitud, la Autoridad de Registro la remitirá a la Agencia de Tecnología y Certificación Electrónica.

4.2.1 Realización de las funciones de identificación y autenticación

La autentificación de la identidad del solicitante de un certificado se realizará mediante la identificación ante la Autoridad de Registro correspondiente utilizando los mecanismos descritos en el apartado 3.2.3 Autentificación de la identidad individual. El Operador de la Autoridad de Registro comprueba la documentación y valida los datos utilizando registros de acceso público para dicha verificación. En el caso de la dirección de correo electrónico, se establece un mecanismo de validación mediante el envío de un enlace único a esta dirección, bloqueando la solicitud hasta que se realice la confirmación.

4.2.2 Aprobación o rechazo de la solicitud del certificado

En caso de aceptación, la Autoridad de Registro notificará al solicitante a través de un correo electrónico firmado digitalmente a la dirección de correo electrónico que figura en la solicitud. Antes de aceptar la solicitud, el solicitante deberá haber validado la dirección de correo electrónico.

En las solicitudes presenciales, la Autoridad de Registro informará al usuario de la aceptación o el rechazo directamente.

En las solicitudes remotas el solicitante deberá acceder al Área Personal de Servicios de Certificación (Autoridad de Registro remota) con un certificado personal o el DNIe. Si el solicitante puede realizar la solicitud, se mostrará la opción correspondiente.

En caso de rechazo la Autoridad de Registro informará al solicitante mediante los mecanismos correspondientes. En las solicitudes presenciales el Operador informará directamente al usuario del rechazo y el motivo del mismo, interrumpiendo el proceso en ese momento y cancelando la solicitud en la plataforma. En las solicitudes remotas la Autoridad de Registro informará al usuario en la aplicación impidiendo la continuación del proceso.

La ACCV utilizará esta información para decidir sobre nuevas solicitudes.

4.2.3 Plazo 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 supervisión, investigación o confirmación sobre la exactitud de la información que se recoge en el certificado con posterioridad a su emisión. En caso de recibir información sobre la inexactitud o la inaplicabilidad actual de la información que se recoge en el certificado, éste podrá ser revocado.

La emisión del certificado se realizará cuando la ACCV haya realizado las comprobaciones necesarias para validar la solicitud de certificación y en presencia del solicitante. El mecanismo que determina la naturaleza y el modo de realizar dicha verificación es esta Política de Certificación.

Cuando la ACCV emita un certificado de acuerdo con una solicitud de certificación válida, enviará una copia del certificado a la Autoridad de Registro que presentó la solicitud y otra copia al depósito de la ACCV.

La Autoridad de Registro notificará al suscriptor la emisión del certificado y le proporcionará el certificado o los medios para obtenerlo.

4.3.1 Acciones de la Autoridad de Certificación durante la emisión

La emisión del certificado tiene lugar una vez que la Autoridad de Registro ha realizado las comprobaciones necesarias para validar la solicitud de certificación. El mecanismo que determina la naturaleza y forma de realizar estas comprobaciones es esta Política de Certificación.

En las solicitudes in situ los pasos son los siguientes:

- La Autoridad de Registro utiliza los datos introducidos por el Operador en el punto de registro presencial.

- La Autoridad de Registro comprueba la introducción de los datos personales

- La Autoridad de Registro realiza la generación del par de claves y la solicitud del certificado indicando los parámetros definidos en esta política.

- La Autoridad de Registro envía la CSR firmada a la Autoridad de Certificación

- La Autoridad de Certificación realiza una verificación de la firma de la Autoridad de Registro y confirma que la forma del CSR es correcta

- La Autoridad de Certificación firma el CSR y lo devuelve a la Autoridad de Registro

- La Autoridad de Registro comunica el certificado al solicitante.

En las solicitudes remotas con certificado cualificado los pasos son los siguientes:

- El solicitante se ha identificado con un certificado cualificado ACCV o con el DNIe y los datos personales asociados a la solicitud se extraen de los campos del certificado.

- El solicitante puede cambiar la dirección postal pero tanto en el caso de utilizar la misma como de cambiarla se validará mediante un enlace único enviado a esa dirección.

- La Autoridad de Registro comprueba los datos personales introducidos por el solicitante en la URL de inscripción.

- La Autoridad de Registro realiza la generación del par de claves y la solicitud del certificado indicando los parámetros definidos en esta política.

- La Autoridad de Registro envía el CSR firmado a la Autoridad de Certificación

- La Autoridad de Certificación realiza una verificación de la firma de la Autoridad de Registro y confirma que la forma del CSR es correcta

- La Autoridad de Certificación firma el CSR y lo devuelve a la Autoridad de Registro

- La Autoridad de Registro comunica el certificado al solicitante.

4.3.2 Notificación al suscriptor

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

4.4 Aceptación de certificados

4.4.1 Proceso de aceptación

La aceptación de los certificados por parte de los suscriptores se produce en el momento de la aceptación del contrato de certificación asociado a cada 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 aceptado por el solicitante, y cuya finalidad es vincular a la persona que solicita el certificado, y el conocimiento de las normas de uso y 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.

4.4.2 Publicación del certificado por la Autoridad de Certificación

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

4.4.3 Notificación de la emisión a otras entidades

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

4.5 Uso del par de claves y del certificado.

4.5.1 Clave privada del suscriptor y uso del certificado.

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

4.5.2 Uso 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.

4.6.1 Circunstancias para la renovación del certificado

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

4.6.2 Quién puede solicitar la renovación del certificado

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

4.6.3 Tramitación de solicitudes de renovación de certificados

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

4.6.4 Notificación de la emisión de un nuevo certificado al suscriptor

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

4.6.5 Conducta que constituye la aceptación de la renovación del certificado

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

4.6.6 Publicación 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.

4.6.7 Notificación 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.

4.7.1 Circunstancias para la renovación con regeneración de claves

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

4.7.2 Circunstancias para la renovación con regeneración de claves

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

4.7.3 Procesamiento de solicitudes de renovación con regeneración de claves

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

4.7.4 Notificación de la renovación con regeneración de claves

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

4.7.5 Conducta 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.

4.7.6 Publicación del certificado renovado

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

4.7.7 Notificación 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.

4.8.1 Circunstancias para la modificación del certificado

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

4.8.2 Quién puede solicitar la modificación del certificado

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

4.8.3 Procesamiento de solicitudes de modificación del certificado

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

4.8.4 Notificación de la modificación del certificado

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

4.8.5 Conducta que constituye la aceptación de la modificación del certificado

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

4.8.6 Publicación del certificado modificado

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

4.8.7 Notificación 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 suscriptor 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

Existe un formulario de solicitud de revocación de certificados en la web de ACCV, en la URL http://www.accv.es, dentro del Área Personal de Servicios de Certificación.

4.9.3.3 Telefónico

Mediante llamada telefónica al número de soporte telefónico de la Agencia de Tecnología y Certificación Electrónica 963 985 308.

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.

4.9.6 Requisitos para la comprobación de la revocación para las partes confiantes
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.7 Frecuencia de emisión de la CRL
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

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

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

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

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

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

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

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

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

4.9.16 Limite para el periodo de supensión
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.10 Servicios de comprobación de estado de certificados.

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

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

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

4.11 Finalización de la suscripción.

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

ACCV informará al firmante, mediante correo electrónico firmado digitalmente, en un momento previo anterior a la publicación del certificado en la Lista de Certificados Revocados, acerca de la suspensión o revocación de su certificado, especificando los motivos, la fecha y la hora en que su certificado quedará sin efecto, y comunicándole que no debe continuar utilizándolo

4.12 Depósito y recuperación de claves.

4.12.1 Prácticas y políticas de custodia y recuperación de claves

La ACCV realiza el depósito de certificados y claves de cifrado para permitir la recuperación de informaciones cifradas en caso de pérdida de las claves necesarias para su descifrado, por interés legítimo del titular de los certificados o por requerimiento judicial.

La recuperación de las claves de cifrado se puede llevar a cabo por parte del usuario a través del Área Personal de Servicios de Certificación en http://www.accv.es, donde puede descargar su certificado y claves de cifrado tras un identificación basada en el certificado de autenticación y firma.

Igualmente puede el usuario solicitar el certificado y claves de cifrado presentándose e identificándose en cualquier Punto de Registro de Usuario.

La Autoridad Judicial debe dirigir un requerimiento a la Agencia de Tecnología y Certificación Electrónica, cuyo datos de contacto se recogen en el apartado 1.5.1 de este documento.

4.12.2 Prácticas 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.

5.2.4 Papeles que requieren separación de tareas
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

Los pares de claves para los certificados emitidos bajo el ámbito de la presente Política de Certificación se generan en tarjeta criptográfica del usuario y nunca abandonan la misma.

6.1.2 Entrega de la clave privada a la entidad

Las claves privadas para los certificados emitidos bajo el ámbito de la presente Política de Certificación se encuentran contenidas en la tarjeta criptográfica que se entrega el suscriptor con su certificado en el momento de su registro.

6.1.3 Entrega de la clave pública al emisor del certificado

La clave pública a ser certificada es generada en el interior de la tarjeta criptográfica 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 el Operador de la 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 de al menos 2048 bits.

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

Las claves de la raíz ACCVRAIZ1 y de la ACCVCA-120 están creadas con el algoritmo RSA

Se utilizan los parámetros definidos en la suite criptográfica sha256-with-rsa especificada en el documento de ETSI TS 119 312 “Electronic Signatures and Infrastructures (ESI); Cryptographic Suites”. Se define ModLen=2048.

Signature suite entry name	**Signature algorithm**	**Signature algorithm parameters**	**Key generation algorithm**	**Padding method**	**Cryptographic hash function**
Sha-256-with-rsa	RSA-PKCSv1_5	MinModLen=2048	rsagen1	emsa-pkcs1-v1_5	sha-256

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 y listas de certificados revocados"*.

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.

Los sistemas donde se almacenan las claves privadas deben cumplir una serie de requisitos relacionados con la seguridad física y lógica de las mismas. ACCV puede solicitar al organismo suscriptor que evidencie los mecanismos que se utilizan para el cumplimiento de dichos requisitos, de manera discrecional. Se recomienda seguir las directrices generadas por el CCN (Centro Nacional de Criptografía) dentro de su serie CNN-STIC, específicamente orientadas a garantizar los sistemas informáticos y las comunicaciones de la Administración.

6.2.1 Estándares para los módulos criptográficos

Los dispositivos criptográficos con certificados cualificados de firma electrónica, aptos como dispositivos cualificados de creación de firma (DSCF), cumplen con los requisitos de nivel de seguridad CC EAL4+, aunque también se aceptan certificaciones que cumplan con un mínimo de criterios de seguridad ITSEC E3 o FIPS 140-2 Nivel 2 o equivalente. La norma europea de referencia para los dispositivos de abonado utilizados es la Decisión de Ejecución (UE) 2016/650 de la Comisión, de 25 de abril de 2016.

Los dispositivos cualificados de creación de firma (DSCF) que pueden dar soporte a este tipo de certificados son los siguientes:

• G&D Smart Cards:

− Giesecke & Devrient (G&D) SmartCafe Expert 3.2 72K FIPS 140-2 Level 2

− Giesecke & Devrient (G&D) SmartCafe Expert 7.0 215K FIPS 140-2 Level 2

6.2.2 Control multipersona de la clave privada

Las claves privadas para los certificados de firma 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

Se hace custodia de las claves vinculadas a los certificados de cifrado. No se custodian claves privadas de firma de los suscriptores de los certificados definidos por la presente política.

6.2.4 Copia de seguridad de la clave privada

Para la custodia de las claves vinculadas a los certificados de cifrado la Agencia de Tecnología y Certificación Electrónica realiza una copia de seguridad de dichas claves. No se se realiza copia de seguridad de las claves privadas de firma de los suscriptores de los certificados definidos por la presente política.

6.2.5 Archivo de la clave privada.

Para la custodia de las claves vinculadas a los certificados de cifrado la Agencia de Tecnología y Certificación Electrónica almacena la copia de seguridad de dichas claves referida en el punto anterior. No se se realiza archivo de las claves privadas de firma de los suscriptores de los certificados definidos por la presente política.

6.2.6 Introducción de la clave privada en el módulo criptográfico.

La generación de las claves vinculadas al certificado de firma se realiza en tarjeta criptográfica por el propio chip criptográfico de la misma y nunca la abandonan.

La generación de las claves vinculadas al certificado de cifrado y la importación en la tarjeta criptográfica del suscriptor se realiza por el software de la Autoridad de Certificación

6.2.7 Almacenamiento de la clave privada en el módulo criptográfico

La generación de las claves vinculadas al certificado de firma se realiza en tarjeta criptográfica por el propio chip criptográfico de la misma y nunca la abandonan.

La generación de las claves vinculadas al certificado de cifrado y la importación en la tarjeta criptográfica del suscriptor se realiza por el software de la Autoridad de Certificación

6.2.8 Método de activación de la clave privada.

La clave privada del suscriptor se activa mediante la introducción del PIN de la tarjeta que la contiene.

6.2.9 Método de desactivación de la clave privada

La desactivación de la clave privada del suscriptor se consigue mediante la extracción de la tarjeta que la contiene del lector PC/SC.

6.2.10 Método 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 destrucción del Token puede producirse cuando la información impresa en él pierde su validez y hay que emitir una nueva tarjeta.

La tarea a realizar consiste en la Destrucción Segura del Token de carácter físico.

6.2.11 Clasificación 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.

El certificado de “ACCVCA-120” es válido desde el día 13 de octubre de 2011 hasta el 1 de enero de 2027.

6.4 Datos de activación

6.4.1 Generación y activación de los datos de activación

Los datos de activación de la clave privada consisten en el PIN de la tarjeta que la contiene y que se proporciona al suscriptor del certificado con el mismo.

La generación del PIN de la tarjeta se realiza en el momento de la inicialización de la misma. El PIN, junto con el código de desbloqueo –PUK–, se entregará al suscriptor.

Es responsabilidad y obligación del suscriptor la custodia de ese PIN (y PUK). Se aconseja al suscriptor el cambio de ese PIN preconfigurado por uno de su exclusivo conocimiento.

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 considerar.

6.5 Controles de Seguridad Informática

6.5.1 Requisitos 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.

6.6.1 Controles 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 el uso de dos certificados distintos; uno de ellos para firma digital y autenticación del titular, y el otro certificado para cifrado de datos. El perfil de ambos certificados es idéntico excepto por los usos de la clave, como se refleja en el apartado 7.1.2 *Extensiones del certificado* de esta Política. En dicho punto se especifica cuando existen diferencias entre ambos certificados

7.1.2 Extensiones del certificado

Las extensiones utilizadas por los certificados emitidos bajo el amparo de la presente política son:

Campo	**Valor**	
Subject		
SerialNumber	NIF del suscriptor. 9 caracteres completados a ceros por la izquierda.	
GivenName	Nombre del suscriptor , tal como aparece en el DNI	
SurName	Apellidos del suscriptor, tal como aparece en el DNI	
CommonName	Cadena compuesta de la forma: NOMBRE APELLIDO1 APELLIDO2 – NIF:NIFDELSUSCRIPTOR	
OrganizationalUnit	Ciudadanos	
Organization	ACCV	
Country	ES	
Version	V3	
SerialNumber	Identificador único del certificado. Menor de 32 caracteres hexadecimales.	
Algoritmo de firma	sha256withRSAEncryption	
Issuer (Emisor)		
CommonName	ACCVCA-120	
OrganizationalUnit	PKIACCV	
Organization	ACCV	
Country	ES	
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	

	Email Protection	
CRL Distribution Point	http://www.accv.es/fileadmin/Archivos/certificados/accvca120_der.crl	
SubjectAlternativeName		
RFC822Name	Correo electrónico del suscriptor	
DirectoryName		
	CN=Nombre|Apellido1|Apellido2	
	UID=NIF	
Certificate Policy Extensions		
	QCP-n-qscd: certificate policy for EU qualified certificates issued to natural persons with private key related to the certified public key in a QSCD; Itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2)	
Policy OID	1.3.6.1.4.1.8149.3.6.7.0	
Policy CPS Location	http://www.accv.es/legislacion_c.htm*	
Policy Notice	Certificado cualificado para Ciudadano expedido 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	http://www.accv.es/gestcert/ACCVCA120SHA2.cacert.crt	
Fingerprint issuer	48 72 a4 c3 df 17 4c ef 34 d7 7f e6 a3 b4 e7 be 7d f2 d2 5d	
Algoritmo de hash	SHA-256	
KeyUsage (críticos)		
Certificado de Firma	Digital Signature Non-repudiation	
Certificado de Cifrado	Key Encipherment Data Encipherment	
QcStatement (sólo cert. de firma)	**Campos QC (Qualified Certificate)**	**QcStatement**
QcCompliance		El certificado es cualificado
QcType	eSign	Tipo particular de certificado cualificado

QcSSCD		La clave privada esta en un dispositivo seguro
QcRetentionPeriod	15y	Periodo de retención de la información material
QcPDS	https://www.accv.es/fileadmin/Archivos/Practicas_de_certificacion/ACCV-PDS-V1.0-EN.pdf	Ubicación de PKI Disclosure Statement

** Hay que destacar la existencia de certificados válidos que fueron emitidos con la URL pki.gva.es en lugar de accv.es. El cambio de una URL a otra es un proceso gradual que no implica diferencias significativas en el perfil ni tampoco en la funcionalidad o uso de los certificados.*

7.1.3 Identificadores de objeto (OID) de los algoritmos

Identificador de Objeto (OID) de los algoritmos Criptográficos:

- SHA1withRSA (1.2.840.113549.1.1.5)
- SHA256withRSA (1.2.840.113549.1.1.11)

7.1.4 Formatos de nombres

Los certificados emitidos por ACCV contienen el distinguished name X.500 del emisor y el subscriptor del certificado en los campos issuer name y subject name respectivamente.

Para certificados emitidos bajo esta politica:

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

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.

SubjectAlternativeName contiene al menos la dirección de correo (RFC822Name) y el nombre y apellidos del suscriptor separados por el caracter "|" (DirectoryName).

Subject:

commonName (obligatorio). Cadena construida de la siguiente manera NOMBRE APELLIDO1 APELLIDO2 – NIF:Suscriptor NIF

GivenName Nombre del suscriptor, como aparece en el DNI o NIE

SurName Apellidos del suscriptor, como aparece en el DNI o NIE

serialNumber (required). DNI o NIE del suscriptor. 9 caracteres completados con ceros a la izquierda.

OrganizationalUnit (required) cadena fija “CIUDADANOS”

Organization (required) cadena fija “ACCV”.

country (required) Código de país ISO 3166-1

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 ACCV para identificar la presente política es el siguiente:

1.3.6.1.4.1.8149.3.6.7.0

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

0.4.0.194112.1.2 Política de certificación para certificados cualificados EU en dispositivo seguro 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 critica "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

El formato de las CRLs utilizadas en la presente política es el especificado en la versión 2 (X509 v2).

7.2.2 CRL y extensiones

La presente Política de Certificación soporta y utiliza CRLs conformes al estándar X.509.

7.3 Perfil OCSP

7.3.1 Numero 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

El acceso a los certificados emitidos bajo esta política, dada su naturaleza pública, es libre y gratuito y por tanto no hay ninguna tarifa de aplicación sobre el mismo.

9.1.3 Tarifas de acceso a la información de estado o revocación

El acceso a la información de estado o revocación de los certificados es libre y gratuita y por tanto no se aplicará ninguna tarifa.

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.

9.1.5 Política 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

9.3.1 Información 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.

9.9 Indemnizaciones

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.

Todos los correos que la ACCV envíe a los suscriptores de los certificados emitidos bajo esta Política de Certificación, en el ejercicio de la prestación del servicio de certificación, serán firmados digitalmente para garantizar su autenticidad e integridad.

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 Circunstancias en las que el OID debe ser cambiado

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

9.13 Resolución de conflictos.

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.

9.16.1 Acuerdo integro

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

9.16.2 Asignación

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

9.16.3 Severabilidad

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

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

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

9.16.5 Fuerza Mayor

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

9.17 Otras estipulaciones

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

10 Anexo I

CONTRATO DE CERTIFICACIÓN – CÓDIGO 1.3.6.1.4.1.8149.3.6
Secció 1 – Dades del subscriptor / *Sección 1 – Datos del suscriptor* Cognoms/*Apellidos*: Nom/*Nombre*: DNI/NIF: Tel.: Adreça de correu electrònic/*Dirección correo electrónico*: Adreça postal/Dirección postal:
PIN : Tel. suport/ tel. soporte **963 866 014** **www.accv.es**
Secció 2 – Dades del operador del Punt de Registre / *Sección 2 – Datos del operador del Punto de Registro* Nom i cognoms/*Nombre y Apellidos*:
Secció 3 - Data i Firma / Sección 3 – *Fecha y Firma* Subscric el present contracte de certificació associat a la Política de Certificació de Certificats Qualificats en dispositiu segur per a ciutadans amb codi 1.3.6.1.4.1.8149.3.6, 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 Cualificados en* dispositivo seguro *para Ciudadanos con código 1.3.6.1.4.1.8149.3.6, emitido por 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 subscriptor *Firma del suscriptor* Firma i segell del Punt de Registre *Firma y sello del Punto de Registro* Firmat/*Firmado*: Firmat/*Firmado:*

Exemplar per al subscriptor - Anvers / *Ejemplar para el suscriptor - Anverso*

CONTRATO DE CERTIFICACIÓN – CÓDIGO 1.3.6.1.4.1.8149.3.6

Condiciones de utilización de los certificados

1. Los certificados asociados a la Política de Certificación para Certificados Cualificados en dispositivo seguro para Ciudadanos, emitidos por la Agencia de Tecnología y Certificación Electrónica 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.

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.

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 y por fallecimiento del titular del certificado. Otras condiciones para la pérdida de eficicacia 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 para la identificación de los solicitantes será el Documento Nacional de Identidad, NIE o Pasaporte español, válido y vigente.

11. En cumplimiento de la ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal, 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. La finalidad de dicho fichero es la 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, cancelación, portabilidad y limitación de tratamiento 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 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 1.3.6.1.4.1.8149.3.6

Secció 1 – Dades del subscriptor / *Sección 1 – Datos del suscriptor*
Cognoms/*Apellidos*:
Nom/*Nombre*:
DNI/NIF: Tel.:

Adreça de correu electrònic/*Dirección correo electrónico*:

Adreça postal/Dirección postal:

Secció 2 – Dades del operador del Punt de Registre / *Sección 2 – Datos del operador del Punto de Registro*
Nom i cognoms/*Nombre y Apellidos*:

Secció 3 - Data i Firma / Sección 3 – *Fecha y Firma*
Subscric el present contracte de certificació associat a la Política de Certificació de Certificats Qualificats en dispositiu segur per a ciutadans amb codi 1.3.6.1.4.1.8149.3.6, 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 Cualificados en dispositivo seguro *para Ciudadanos con código 1.3.6.1.4.1.8149.3.6, emitido por 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 subscriptor
Firma del suscriptor

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*

11 Anexo II – Formulario de solicitud de revocación de certificado

SOLICITUD DE REVOCACIÓ DE CERTIFICAT ***SOLICITUD DE REVOCACIÓN DE CERTIFICADO*** V3.0
Fecha:.....
Sección 1 – Dades del subscriptor del certificat / *Sección 1 – Datos del subscriptor del certificado* Cognoms/*Apellidos*: Nom/*Nombre*: DNI/NIF:
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 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 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

V3.0

Fecha:.....

Sección 1 – Dades del subscriptor del certificat / *Sección 1 – Datos del subscriptor del certificado*

Cognoms/*Apellidos*:
Nom/*Nombre*:
DNI/NIF:

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 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*