Agencia de Tecnología y Certificación Electrónica

Política de Certificación de Certificados de Autenticación de Servidor

Fecha: 20/03/2022	**Versión:** 1.0.2
Estado: APROBADO	**Nº de páginas:** 42
OID: 1.3.6.1.4.1.8149.3.36.2.0	**Clasificación: PÚBLICO**
Archivo: ACCV-CP-36V1.0.2-ES-2022.odt	
Preparado por: Agencia de Tecnología y Certificación Electrónica - ACCV	

Cambios

Versión	Autor	Fecha	Obdervaciones
1.0.1	ACCV	20/06/2021	Versión inicial
1.0.2	ACCV	20/03/2022	Se elimina el campo OU del perfil

Tabla de Contenido

1.INTRODUCCIÓN

1.1.Presentación

El presente documento es la Política de Certificación asociada a los certificados de autenticación de sitios web, 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 de autenticación de sitios web.

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.

En el ámbito del proyecto Certificate Transparency, los precertificados se publicarán en el servicio CT Log de los proveedores de servidores de registro cualificados para cumplir con los requisitos del proyecto.

1.2.Identificación

Nombre de la política	Política de Certificación de Certificados de Autenticación de Sitios Web
Calificador de la política	`Certificado de autenticación de servidor expedido por la ACCV (Pol. Ademuz, s/n. Burjassot, CP 46100, ESPAÑA. CIF A40573396)`
Versión de la política	1.0.2
Estado de la política	APROBADO
Referencia de la política / OID (Object Identifier)	1.3.6.1.4.1.8149.3.36.1.0
Fecha de emisión	20/03/2022
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 ACCVCA-120 es válido desde el día 27 de enero de 2015 hasta el 1 de enero de 2027.

1.3.2.Autoridades de Registro

La Autoridad de Registro que gestiona este tipo de certificados es la Agencia de Tecnología y Certificación Electrónica (ACCV).

1.3.3.Suscriptores

El grupo de usuarios que pueden solicitar certificados definidos por esta política está formado por los responsables de entidades públicas o privadas, en situación de representar a la entidad solicitante.

En el caso de entidades públicas, las solicitudes pueden llevarlas a cabo Jefes de Servicio o puestos organizativos equivalentes en cualquier tipo de Administración Pública (europea, estatal, autonómica y local), siendo éstos los responsables últimos de su uso dentro de los distintos proyectos o sistemas de información.

En el caso de entidades privadas, podrán solicitar los certificados aquellas personas con capacidad de representar la entidad o que hayan sido autorizadas para la gestión de este tipo de certificados.

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 por 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:

a. Los usuarios de clientes de aplicaciones en el ámbito de la verificación de la identidad de los sitios web a los que se conectan y del cifrado del canal de los datos transmitidos entre ellos.

b. Las aplicaciones y servicios con capacidades de soporte SSL y/o TLS, en el ámbito de verificación de la identidad de los sitios web a los que se conectan, y del cifrado del canal de los datos transmitidos entre ellos

1.3.5.Otros participantes

De acuerdo con 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 dotar a los sitios web de capacidades SSL/TLS. Asimismo, pueden utilizarse como mecanismo de identificación de estos sitios de forma inequívoca 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

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

Bastionado: es el proceso mediante el cual se implementa una política de seguridad específica sobre una instalación de un sistema operativo. El bastionado de un equipo intenta reducir el nivel de exposición de un equipo y, por tanto, los riesgos y vulnerabilidades asociados a éste.

SSL: Secure Sockets Layer

TLS: Transport Security Layer

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

Además de lo especificado en la Declaración de Prácticas de Certificación (CPS), ACCV proporciona páginas web de prueba que permiten a los proveedores de software de aplicación probar su software con certificados de suscriptor que se encadenan a cada certificado raíz de confianza pública.

VALID

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

REVOKED

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

EXPIRED

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

ACCV 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.Anonimización o seudoanonimización de los suscriptores

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

3.1.4.Interpretación de formatos de nombres

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

3.1.5.Unicidad de los 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.

La autentificación de la identidad del solicitante se realiza mediante el uso de su certificado personal cualificado, firmando con el la solicitud del certificado de servidor al identificarse en la aplicación que para esta función pone a disposición de los usuarios la ACCV (NPSC https://npsc.accv.es:8450/npsc)

El solicitante debe presentar la documentación necesaria que determine

Los datos relativos a la entidad como la inclusión en el registro mercantil correspondiente, domicilio, localidad, estado o provincia, país, códigos de funcionamiento, etc.

Las capacidades de representación necesarias de la entidad propietaria del referido dominio.

La posesión del dominio

Esta presentación se realizará de forma digital utilizando las fuentes y aplicaciones que ACCV pone a disposición de los usuarios para ello.

ACCV comprobará los datos suministrados (incluyendo el país del solicitante) utilizando para ello la información disponible en:

Agencias de Protección de Datos

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

Registros de Administraciones Públicas

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

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

Registros mercantiles

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

Oficinas de Patentes y Marcas

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

Servicios de Verificación y Consulta de Identidad

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

reclamando al solicitante las subsanaciones o documentos adicionales que pudiera considerar necesarios.

Todos los organismos y registros utilizados son oficiales y de alta fiabilidad, proporcionando pruebas rastreables de todas las búsquedas.

La ACCV conserva esta información a efectos de auditoría, permitiendo su reutilización durante un periodo no superior a 13 meses desde su última comprobación.

Verificación de dominio

ACCV verificará que el dominio de los certificados y sus direcciones asociadas pertenecen a los datos del solicitante utilizando para ello la información disponible de los registros personales y de dominios, exigiendo al solicitante las explicaciones o documentos adicionales que pudiera considerar necesarios e incluyendo en el proceso mecanismos de comprobación técnicamente fiables y aprobados por la industria.

ACCV conserva la información de comprobación dominio con fines de auditoría pero no la reutiliza, verificando el dominio para cada solicitud de forma independiente. La ACCV no emitirá certificados para direcciones IP o nombres de dominio privados, y las entradas en el dNSName deben estar en la "sintaxis de nombre preferida", como se especifica en el RFC 5280, y por lo tanto no deben contener caracteres de subrayado ("_"). En el caso de los gTLD, sólo se emitirán certificados con nombres de gTLD aprobados, y sólo se emitirán a los suscriptores que tengan el control del gTLD, tal y como aparece en ICANN/IANA.

En concreto:

- Comprobación de que el solicitante, cuya identidad ha sido verificada sin lugar a dudas, es uno de los propietarios del dominio. Para esta comprobación, la ACCV debe utilizar uno o varios de los siguientes métodos:
  - Contactar por correo, enviando un número aleatorio único en el correo a la dirección confirmada del propietario del dominio, esperar un tiempo no superior a 30 días y comprobar la respuesta que debe incluir el mismo número aleatorio.
    - (CAB/Forum BR 3.2.2.4.2 Correo electrónico, fax, SMS o correo postal al contacto del dominio)
  - Contactar por correo, enviando un número aleatorio único en el correo a una o más direcciones creadas usando 'admin', 'administrator', 'webmaster', 'hostmaster', o 'postmaster' como parte local, seguido del signo de arroba ("@"), seguido de un nombre de dominio a autorizar, incluyendo un valor aleatorio en el correo electrónico, y recibiendo una respuesta de confirmación utilizando el mismo valor aleatorio del correo inicial. ACCV debe esperar la respuesta un tiempo no superior a 30 días y debe confirmar que la respuesta incluye el mismo número aleatorio.
    - (CAB/Forum BR 3.2.2.4.4 Correo electrónico construido al contacto del dominio)
  - Confirmar la presencia de un valor aleatorio incluido en el contenido de un archivo bajo el directorio "/.well-known/pki-validation" en el nombre de dominio a autorizar. Esta URL debe ser accesible por la CA a través de HTTP/HTTPS sobre un Puerto Autorizado. Una vez comunicado el valor al solicitante, sólo será válido durante 30 días. En la URL no

aparece en ningún caso el contenido del fichero y solo se considera como valor correcto de respuesta HTTP 200 (no se permiten re direcciones).

- (CAB/Forum BR 3.2.2.4.18 Cambio acordado en el sitio web v2)

◦ Confirmar la presencia de un valor aleatorio en un registro DNS CNAME, TXT o CAA para 1) un Nombre de Dominio de Autorización; o 2) un Nombre de Dominio de Autorización que tenga como prefijo una etiqueta que comience con un carácter de subrayado. Una vez comunicado el valor al solicitante, sólo será válido durante 30 días.

- (CAB/Forum BR 3.2.2.4.7 Cambio de DNS)

ACCV comprobará la existencia de registros CAA justo antes de emitir el certificado, actuando como se define en el rfc 6844 y en los documentos del CAB/Forum si el registro está presente. El identificador asociado a ACCV como registros CAA *issue* e *issuewild* es "accv.es".

Además de la consulta de WHOIS, se realizarán pruebas de conexión con el dominio dado y pruebas de respuesta de DNS mediante protocolo seguro (por ejemplo, HTTPS).

Si se trata de un certificado con carácter comodín (*), la aplicación para realizar la petición (NPSC) sólo permite colocar el carácter en una posición válida (nunca se permite en una primera posición a la izquierda de una etiqueta "controlada por el registro" o sufijo público).

Ante cualquier irregularidad el solicitante del certificado será notificado por la ACCV y se suspenderá su emisión hasta su corrección. Si dicha corrección no se produce en un mes, la solicitud será denegada.

3.2.3.Autenticación de la identidad de un individuo

La autentificación de la identidad del solicitante de un certificado se realizará mediante el uso de su certificado cualificado personal admitido para la firma de la solicitud del certificado de servidor.

El solicitante deberá presentar además la documentación necesaria que determine la capacidad de representar a la entidad propietaria del dominio al que hace referencia y la posesión del dominio mismo. Esta presentación se realizará de manera telemática utilizando los medios y aplicaciones que a tal efecto la ACCV ponga a disposición de los usuarios (3.2.2.).

ACCV comprobará los datos suministrados (incluyendo el país del solicitante) utilizando para ello la información disponible en:

Agencias de Protección de Datos

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

Registros de Administraciones Públicas

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

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

Registros mercantiles

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

Oficinas de Patentes y Marcas

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

Servicios de Verificación y Consulta de Identidad

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

reclamando al solicitante las subsanaciones o documentos adicionales que pudiera considerar necesarios.

Todos los organismos y registros utilizados son oficiales y de alta fiabilidad, proporcionando pruebas rastreables de todas las búsquedas.

La ACCV conserva esta información a efectos de auditoría, permitiendo su reutilización durante un periodo no superior a 13 meses desde su última comprobación.

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 del par de claves.

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). ACCV puede reutilizar la información almacenada en comprobaciones previas si no han pasado mas de 13 meses desde la ultima verificación de los datos, exceptuando la información de comprobación de dominio que no se reutiliza. Existe, por tanto, un mecanismo para la renovación:

- Formularios web en el Área de Gestión de Certificados No Personales, disponible en https://npsc.accv.es:8450/npsc.

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, pudiendo reutilizar la información en posesión de la ACCV si no han pasado mas de 13 meses desde la ultima verificación de los datos, exceptuando la información de comprobación de dominio que no se reutiliza.

ACCV, por cuestiones técnicas y detallando todos los pasos, puede emplear 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 del par de claves

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

•Telemática. Mediante formulario de revocación (ubicado en el Área de Gestión de Certificados No Personales https://npsc.accv.es:8450/npsc) accediendo por parte del solicitante del certificado o del responsable del mismo en la fecha de la solicitud de revocación mediante certificado cualificado personal.

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 asociada al certificado de autenticación de sitios web, 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

Este tipo de solicitud de certificados es responsabilidad de entidades privadas o públicas. Una solicitud de certificado puede ser presentada por el sujeto del certificado o por un representante autorizado del mismo.

4.1.2.Proceso de registro y responsabilidades

El proceso comienza por acceder al Área de gestión de certificados no personales (NPSC) ubicada en https://npsc.accv.es:8450/npsc. Si se solicita por primera vez el certificado de autenticación de servidor asociado a una entidad el usuario debe adjuntar el documento que lo acredita como capacitado para efectuar esa solicitud (documento de toma de posesión en el puesto o diario oficial donde se recoge el nombramiento correspondiente, poderes notariales e inscripción en los registros correspondientes), en formato pdf firmado electrónicamente. Si el acceso se ha efectuado con un certificado que acredita la capacidad necesaria para gestionar los certificados de autenticación de servidor, se utilizaran los datos de Organización, Unidad Organizativa y Cargo de dicho certificado.

ACCV comprobará los datos de la solicitud y acreditará al solicitante para la solicitud de certificados de autenticación de servidor, durante 13 meses a partir de la aprobación sin necesidad de aportar documentación adicional, exceptuando la información de comprobación de dominio que no se reutiliza. En el caso de identificación con certificado de empleado público no existe limitación temporal mientras el certificado esté en vigor.

Ademas de comprobar las credenciales asociados a la entidad, ACCV comprobará en los registros autorizados la posesión del dominio o dominios que aparecen en la solicitud de certificado, de forma que no exista duda de dicha posesión. ACCV dejará constancia de estas búsquedas y comprobaciones de forma que puedan reproducirse en todos los pasos. Para esta comprobación ACCV utilizara los correos y teléfonos suministrados en el proceso de alta, siendo necesaria una vinculación directa entre estos datos y los dominios incluidos en la solicitud.

4.2.Tramitación de la solicitud de certificados.

4.2.1.Realización de las funciones de identificación y autenticación

El solicitante se identifica con un certificado personal cualificado en el Área de Gestión de Certificados No Personales (NPSC) ubicada en https://npsc.accv.es:8450/npsc, utilizando los datos del certificado para realizar las funciones de identificación y autenticación.

Una vez recibida la solicitud de certificado en formato electrónico a través de la plataforma por parte de las personas autorizadas y una vez aceptada la proposición económica, la ACCV procede a la revisión de la solicitud.

La ACCV comprueba los datos de la solicitud y acredita al solicitante de la solicitud de certificado de autenticación de sitios web, durante 13 meses desde la aprobación sin necesidad de presentar ninguna documentación adicional. En el caso de identificarse con certificado de empleado público o representante no existe límite temporal mientras el certificado esté vigente.

Además de comprobar las credenciales asociadas a la entidad, la ACCV verifica en los registros autorizados la posesión del dominio o dominios que aparecen en la solicitud del certificado, para que no haya dudas sobre la existencia de esta posesión, tal y como se detalla en los apartados 3.2.2 y 3.2.3 de esta política. ACCV proporciona registros de estas búsquedas y comprobaciones para que puedan ser reproducidas en cada paso. Para esta comprobación ACCV utiliza los correos y teléfonos que se presentaron en el proceso de registro, siendo necesaria una conexión directa entre estos datos y los dominios que se incluyen en la solicitud.

En este proceso, ACCV comprueba que las solicitudes de certificados no incluyen dominios que puedan ser utilizados para phishing u otros usos fraudulentos, utilizando los mecanismos y listas disponibles.

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.

En caso de rechazo, la Autoridad de Registro notificará al solicitante mediante un correo electrónico firmado digitalmente a la dirección de correo electrónico que figura en la solicitud. La solicitud queda anulada y no puede ser reutilizada, aunque es posible reutilizar la documentación aportada marcada como correcta durante un periodo no superior a 13 meses.

Este proceso lo lleva a cabo un miembro de la ACCV diferente al responsable de realizar la verificación de los datos. La diferenciación de funciones se realiza utilizando las capacidades establecidas en la aplicación de gestión.

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

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. El mecanismo que determina la naturaleza y forma de realizar estas comprobaciones es esta Política de Certificación.

Cuando el solicitante recibe el correo electrónico de aprobación, debe entrar de nuevo en NPSC, identificándose con un certificado personal cualificado para generar y descargar el certificado.

La organización responsable del certificado de autenticación de los sitios web puede solicitar a la ACCV que añada otros usuarios con capacidad para realizar las transacciones que están asociadas al ciclo de vida de los certificados. La Autoridad de Registro comprobará la solicitud de credencial y notificará al solicitante la autorización o denegación del permiso, a través de un correo electrónico firmado.

ACCV podrá realizar esta autorización de oficio en el caso de que el responsable del sitio web pierda su capacidad de gestión y no exista otra persona autorizada.

ACCV realizará revisiones frecuentes de las muestras de los certificados de autentificación de la web para garantizar la exactitud de los datos y el efecto. Si en el transcurso de estos muestreos se confirma un cambio de datos que pueda implicar la pérdida de la posesión del dominio, la ACCV revocará los certificados implicados. En caso de inexactitud de los datos que figuran en el certificado o de su inaplicabilidad se aplicará el mismo proceso. ACCV dejará constancia documental de todas estas revisiones y actuaciones.

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 cuyo fin es vincular a la persona que solicita el certificado de autenticación de servidor, 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.

4.4.2.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

4.9.1.1.Razones para revocar un certificado de usuario
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.1.2.Razones para revocar un certificado de AC subordinada (intermedia)

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.Telemático

Accediendo al Área de Gestión de certificados no personales (NPSC) ubicada en https://npsc.accv.es:8450/npsc el usuario puede revocar los certificados que ha solicitado o de los que tiene permiso para ello.

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.Plazo de tiempo para procesar la solicitud de revocación

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

4.9.6.Obligación de verificar las revocaciones por las partes que confían

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

4.9.7.Frecuencia de emisión de CRLs

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

4.9.8.Latencia máxima para la publicación de CRLs

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

4.9.9.Disponibilidad del sistema de verificación online 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 en línea de la revocación

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

4.9.11.Otras formas de aviso de revocación disponibles

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

4.9.12.Requisitos especiales de revocación de claves comprometidas

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

4.9.13.Circunstancias para la suspensión

Se suspenderá un certificado si así lo dispone una autoridad judicial o administrativa, por el tiempo que la misma establezca.

ACCV no soporta la suspensión de certificados como operación independiente sobre sus certificados.

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.Límites del período de suspensión

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 responsable del certificado de autenticación de servidor, 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 los certificados en los cuales aparezca como suscriptor o responsable, 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

ACCV no realiza el depósito de claves de ningún tipo asociadas a este tipo de certificados.

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.

4.13.Caducidad de las claves de certificado de CA.

ACCV evitará generar certificados de autenticación de servidor que caduquen con posterioridad a los certificados de CA. Para ello no se emitirán certificados de autenticación de servidor cuyo periodo de validez exceda el del certificado de CA en cuestión y se generarán con el nuevo certificado de CA, con el fin de evitar la notificación a los subscriptores para que procedan a la renovación de su certificado, en el supuesto que el certificado de CA caducara con anterioridad.

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.Plan de recuperación de desastres

5.7.1.Procedimientos de gestión de incidentes y vulnerabilidades
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.7.2.Alteración de los recursos hardware, software y/o datos
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.7.3.Procedimiento de actuación ante la vulnerabilidad de la clave privada de una entidad de ACCV
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.7.4.Continuidad de negocio después de un 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 generan en software por el suscriptor del certificado.

6.1.2.Entrega de la clave privada a la entidad

La clave privada se genera por el subscriptor, por tanto, no procede hacerle entrega de la misma.

6.1.3.Entrega de la clave pública al emisor del certificado

La clave pública a ser certificada es generada por el suscriptor 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 suscriptor.

Si se detecta que la clave pública de la solicitud no cumple los requisitos (clave débil, etc.) será rechazada.

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

Las claves de la raíz ACCVRAIZ1 y de la ACCVCA-120 son claves RSA de 4096 bits de longitud.

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 el documento ETSI TS 119 312 "Electronic Signatures and Infrastructures (ESI);Cryptographic Suites" (6 - Esquemas de firma).El esquema de relleno utilizado es emsa-pkcs1-v2.1 (según RFC 3447 sección 9.2).

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

6.1.7.Usos admitidos de la clave (campo KeyUsage de X.509v3)

Las claves definidas en la presente política se utilizarán para los usos descritos en la sección 1.3 Comunidad de usuarios y ámbito de aplicación de este documento. La definición detallada del perfil de certificado y el uso de las claves se encuentra en la sección 7 de este documento "Perfiles de certificado, CRL y OCSP".

6.1.8.Hardware/software de generación de claves

La generación de las claves se realiza en software por el suscriptor del certificado.

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

Este punto está siempre referido a las claves que se generan para los certificados emitidos bajo el ámbito de la Política de Certificación vigente. La información sobre los estándares y controles del módulo criptográfico de las entidades que componen las Autoridades de Certificación se encuentra en el apartado 6.2.1 de la Declaración de Prácticas de Certificación (DPC) de la ACCV.

Los módulos criptográficos se encuentran en software en el equipo del usuario 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 ni se realizan copias de seguridad de las claves privadas de los suscriptores de los certificados definidos por la presente política.

6.2.5.Archivo de la clave privada

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

6.2.6.Introducción de la clave privada en el módulo criptográfico

No aplicable en el ámbito de la presente Política.

6.2.7.Almacenamiento de la clave privada en el módulo criptográfico

No aplicable en el ámbito de la presente Política.

6.2.8.Método de activación de la clave privada.

La clave privada es generada por el solicitante y nunca está en posesión de la ACCV.

6.2.9.Método de desactivación de la clave privada

La clave privada es generada por el solicitante y nunca está en posesión de la ACCV.

6.2.10.Método de destrucción de la clave privada

La clave privada es generada por el solicitante y nunca está en posesión de la ACCV. Se podrá destruir mediante el borrado de esta siguiendo las instrucciones de la aplicación que la alberga.

6.2.11.Clasificación de los módulos criptográficos

La clave privada es generada por el solicitante y nunca está en posesión de la ACCV.

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.Periodos de operación del certificado y periodos de uso del par de claves

Los certificados emitidos al amparo de la presente política tienen una validez de 12 meses como máximo.

La clave utilizada para la emisión de los certificados se crea para cada emisión, y por tanto también tienen una validez de 12 meses como máximo. Esa es la fecha máxima de validez que se admite en la solicitud de los certificados emitidos en virtud de esta política.

El certificado de ACCVCA-120 es válido desde el día 27 de enero de 2015 hasta el 1 de enero de 2027.

6.4.Datos de activación

6.4.1.Generación e instalación de datos de activación

La clave privada es generada por el solicitante y nunca está en posesión de la ACCV.

6.4.2.Protección de los datos de activación

El suscriptor 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

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

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. Sellos 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

ACCV admite y utiliza certificados X.509 versión 3 (X.509 v3)

Esta política de certificación especifica el uso de un certificado con dos usos distintos; firma digital, y cifrado de clave.

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 de la Administración, organismo o entidad de derecho público o privado suscriptora del certificado, a la que se encuentra vinculado el sitio web.
CommonName	Denominación de nombre de dominio (DNS) donde residirá el certificado.
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
Organization	Denominación (nombre “oficial”) de la Administración, organismo o entidad de derecho público suscriptora del certificado y propietaria del dominio.
Jurisdiction Country	ES
Business Category	Uno de las siguientes cadenas fijas "PRIVATE ORGANIZATION", "GOVERNMENT ENTITY", "BUSINESS ENTITY”, o "NON-COMMERCIAL ENTITY”, dependiendo del tipo de organización.
Locality	Ciudad
State	Provincia
Country	ES (code ISO 3166-1)
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 certificado
Extended Key Usage	

	Server Authentication Client Authentication	
CRL Distribution Point		
	distributionPoint	http://www.accv.es/fileadmin/Archivos/certificados/accvca120_der.crl
SubjectAlternativeName		
	dnsName	Nombre Dominio DNS 1 (coincide con el dominio en el common name)
Opcional	dnsName	Nombre Dominio DNS 2
Opcional	dnsName	Nombre Dominio DNS 3
Opcional	dnsName	Nombre Dominio DNS 4
Opcional	dnsName	Nombre Dominio DNS 5
Certificate Policy Extensions		
Policy OID	{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)} 2.23.140.1.2.2	
Policy OID	1.3.6.1.4.1.8149.3.36.1.0	
Policy CPS Location	http://www.accv.es/legislacion_c.htm*	
Policy Notice	Certificado de autenticación de servidor 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-caIssuers
	Access Location	http://www.accv.es/gestcert/ACCVCA120SHA2.cacert.crt
Fingerprint issuer	48 72 a4 c3 df 17 4c ef 34 d7 7f e6 a3 b4 e7 be 7d f2 d2 5d	
Algoritmo de hash	SHA-256	
KeyUsage (críticos)		
	Digital Signature Key Encipherment	
SCT List1.3.6.1.4.1.11129.2.4.2	Signed Certificate Timestamp List	Respuestas SCT de Logs cualificados. Al menos tres respuestas diferentes.
CA/Browser Forum	cabfOrganizationIdentifier (OID: 2.23.140.3.1) {joint-iso-itu-t(2) international-organizations(23)	

Organization Identifier Field	ca-browser-forum(140) certificate-extensions(3) cabf-organization-identifier(1) }	
	registrationSchemeIdentifier	3 carácter Identificador del esquema de registro (VAT)
	registrationCountry	2 carácter ISO 3166 código de país (ES)
	registrationStateOrProvince	Provincia (opcional)
	registrationReference	Referencia de registro asignada de acuerdo con el esquema de registro identificado (CIF)

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 (DN) X.500 del emisor del certificado y del suscriptor del mismo en los campos de nombre del emisor y nombre del sujeto, respectivamente.

Para los certificados emitidos bajo esta política

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

Todos los campos del certificado incluidos en el Subject, excepto los que están referidos al nombre DNS, dirección de correo electrónico o definidos explícitamente, se rellenan necesariamente en mayúsculas, sin acentos.

SubjectAlternativeName contiene al menos una entrada. Cada entrada de SubjectAlternativeName es un dNSName que contiene el nombre de dominio totalmente calificado de un servidor.

Subject:

commonName (obligatorio). Debe coincidir con uno de los campos DNSName del subjectAlternativeName

serialNumber (obligatorio). NIF de la Administración, tal y como se define en el Real Decreto 1065/2007, de 27 de julio.

OrganizationIdentifier (requerido) NIF de la entidad, según se define en la norma europea ETSI EN 319 412-1

jurisdictionCountry (requerido) Código de país ISO 3166-1

BusinessCategory (requerido) Una de las siguientes cadenas fijas

"Private Organization"

"Govennment Entity"

"Business Entity"

"Non-Commercial Entity"

en función del tipo de organización

Organization (obligatorio) Designación (nombre "oficial") de la Administración, organismo o entidad suscriptora del certificado y titular del dominio.

locality (requerido) Localidad, ciudad o pueblo

state (requerido) Estado o provincia

country (requerido) 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.

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:

1.3.6.1.4.1.8149.3.36.1.0

En este caso se añade un OID para identificar el tipo de entidad que se representa siguiendo las guias del CAB/Forum

2.23.140.1.2.2 Certificates issued in accordance with the CA/Browser Forum's Baseline Requirements - Organization identity asserted

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. Además, la extensión puede contener un calificador de política.

7.1.10.Signed Certificate Timestamp (SCT) List

Respuestas de registros calificados bien conocidos, que actualmente cumplen con la política de transparencia de certificados de Chrome.

Extension OID: 1.3.6.1.4.1.11129.2.4.2

RFC 6962 (Certificate Transparency): https://tools.ietf.org/html/rfc6962

Para los certificados con un valor notBefore mayor o igual al 21 de abril de 2021 (2021-04-21T00:00:00Z), el número de SCT incrustados se basa en la vida útil del certificado:

Certificate lifetime	**# of SCTs from separate logs**	**Maximum # of SCTs per log operator which count towards the SCT requirement**
180 days or less	2	1
181 to 398 days	3	2

Para los certificados con un valor notBefore inferior al 21 de abril de 2021 (2021-04-21T00:00:00Z), el número de SCT incrustados se basa en la vida útil del certificado:

Lifetime of Certificate	Number of SCTs from distinct logs
< 15 months	2
>= 15, <= 27 months	3
> 27, <= 39 months	4
> 39 months	5

7.2.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 OCSP

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

7.3.1.Número de versión

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

7.3.2.Extensiones OCSP

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

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.

8.7.Auto auditorias

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.

9.1.5.Política de reintegros

No se prevén reintegros de las cantidades entregadas para el pago de este tipo de certificados.

9.2.Responsabilidades financieras

9.2.1.Seguro de responsabilidad civil

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

9.2.2.Otros activos

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

9.2.3.Seguros y garantías para entidades finales

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

9.3.Confidencialidad de la información

9.3.1.Alcance de la 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.Responsabilidad para proteger la información confidencial

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

9.4.Protección de datos personales

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 Garantias

9.6.1.Obligaciones de la Autoridad 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 de otros participantes
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 1.3.6.1.4.1.8149.3.36
Sección 1 – Datos del solicitante *Apellidos*: *Nombre*: NIF: Tel.: Puesto o cargo: Administración-Organización: CIF de la Organización: *Dirección correo electrónico*: Dirección postal:
Sección 2 – Datos del dominio Nombre cualificado: Alias: Dirección de correo de contacto:
Sección 3 – *Fecha y Firma* *Suscribo el presente contrato de certificación asociado a la Política de Certificación de Certificados de Autenticación de Sitios Web con código 1.3.6.1.4.1.8149.3.36, 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 solicitante* Firmat/*Firmado*:

CONTRATO DE CERTIFICACIÓN – CÓDIGO 1.3.6.1.4.1.8149.3.36

Condiciones de utilización de los certificados

1. Los certificados asociados a la la Política de Certificación de certificados para servidores con soporte SSL , 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 Valenciana.

2. El solicitante de los certificados debe ser una persona física, en posesión de un certificado cualificado de la ACCV o del DNIe. El solicitante deberá aportar los datos relativos a su relación con el Organismo o Empresa en nombre del que solicita el certificado utilizando las herramientas puestas a su disposición por la ACCV.

3. El solicitante de los certificados, especialmente habilitado para la gestión de éstos por parte de un Organismo o Empresa determinada, 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 suscriptor 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 suscriptor 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 funcionamiento de los servidores informáticos que hacen uso de los certificados 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 12 meses como máximo. Para su renovación deberá 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 suscriptor 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 certificados.

10. La identificación de los solicitantes se hará en base a su certificado digital personal expedido por la Agencia de Tecnología y Certificación Electrónica o su DNIe.

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 este fichero es servir a los usos relacionados con los servicios de certificación que presta la Agencia de Tecnología y Certificación Electrónica. El suscriptor autoriza expresamente el uso de sus datos personales que contiene el fichero, en la medida en que sean necesarios 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 o cancelación 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.

Motivos de revocación

Estos son los motivos que podrá utilizar para revocar su certificado:

Sin motivo o sin especificar

El suscriptor no está obligado a proporcionar un motivo de revocación, a menos que su clave privada se haya visto comprometida.

Cambio de los datos de filiación

Se DEBERÍA elegir este motivo de revocación cuando el nombre de su organización u otra información de la organización en el certificado haya cambiado.

Reemplazo

Se DEBERÍA elegir este motivo de revocación cuando se solicita un nuevo certificado para reemplazar un certificado existente.

Cambio de la propiedad de los dominios

Se DEBERÍA elegir este motivo de revocación cuando ya no sea propietario de todos los nombres de dominio en el certificado o cuando ya no vaya a utilizar el certificado porque el sitio web vaya a dejar de estar operativo.

Compromiso de la clave

Se DEBE elegir este motivo de revocación cuando el suscriptor tenga conocimiento o tenga motivos para creer que la clave privada de su certificado se ha visto comprometida. Por ejemplo si una persona no autorizada ha tenido acceso a la clave privada de su certificado. Si se selecciona este motivo SE REVOCARÁN TODOS LOS CERTIFICADOS DEL ORGANISMO EMITIDOS CON LAS MISMAS CLAVES y la ACCV puede contactar con el solicitante para recabar mas información y requerir evidencias adicionales.

Privilegio retirado

La CA detecta que ha habido una infracción del lado del suscriptor que no ha resultado en compromiso de clave, como que el suscriptor del certificado proporcionó información engañosa en su solicitud de certificado o no ha cumplido con sus obligaciones materiales bajo el acuerdo del suscriptor o los términos de uso.

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.