Agencia de Tecnología y Certificación Electrónica

Política de Certificación de Certificados Cualificados para servidores VPN

Fecha: 10 de Noviembre de 2019	**Versión:** 4.0.1
Estado: APROBADO	**Nº de páginas:** 42
OID: 1.3.6.1.4.1.8149.3.8.4.0	**Clasificación: PUBLICO**
Archivo: ACCV-CP-08V4.0.1_2019.odt	
Preparado por: Agencia de Tecnología y Certificación Electrónica	

ISTEC Firmado digitalmente por ISTEC
Fecha: 2020.07.02 09:21:56 +02'00'

Tabla de Contenido

1. INTRODUCCIÓN

1.1. Presentación

El presente documento es la Política de Certificación asociada a los certificados para servidores VPN, 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 para servidores VPN.

La presente Politica 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.

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

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 para servidores VPN
Calificador de la política	Certificado Cualificado para Servidores VPN expedido por la ACCV(Plaza Nápoles y Sicilia, 6. Valencia CP 46003, ESPAÑA. CIF A40573396)
Versión de la política	4.0.1
Estado de la política	APROBADO
Referencia de la política / OID (Object Identifier)	1.3.6.1.4.1.8149.3.8.4.0
Fecha de emisión	10 de noviembre de 2019
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/pdf-politicas

1.3. Comunidad y Ámbito de aplicación

1.3.1. Autoridades de Certificación

La CA que puede emitir certificados acordes con esta política es la 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 Autoridad de Registro que gestiona este tipo de certificados es la Agencia de Tecnología y Certificación Electrónica.

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

La confianza en los certificados para servidores VPN emitidos bajo esta Política no está limitada. Cualquier persona física o sistema informático puede confiar en estos certificados para la verificación de la identidad del servidor al que se conectan.

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 dotar de identidad y capacidades criptográficas avanzadas a los servidores VPN.

1.4.2. Usos prohibidos

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

1.5. Política de Administración de la ACCV

1.5.1. Especificación de la Organización Administradora

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

1.5.2. Persona de Contacto

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

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

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

1.5.4. Procedimiento de aprobación.

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

1.6. Definiciones y Acrónimos

1.6.1. Definiciones

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

1.6.2. 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

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

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 AUTENTIFICACIÓN

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. Procedimientos de resolución de disputas de 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 como solicitante.

La confirmación de la exactitud de los datos de la organización en nombre de la cual el solicitante realiza la solicitud se seguirán los mecanismo detallados en el punto 3.2.3

3.2.3. Autentificación de la identidad de un individuo

La autenticación de la identidad del solicitante de un certificado se realizará mediante el uso de su certificado cualificado personal para la firma de la solicitud del certificado para servidores VPN.

El solicitante deberá presentar además la documentación necesaria que determine los datos y características de la entidad en nombre de la cual se solicita, 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.

ACCV comprobará todos los datos (incluyendo el país del solicitante) utilizando para ello la información disponible de registros de personal y de dominio, requiriendo al solicitante o a la entidad repre-

sentada las aclaraciones o documentos adicionales que considere necesarios. ACCV guardara esta información a efectos de auditoria, permitiendo su reutilización durante un plazo no superior a 13 meses desde la ultima comprobación. La información que hace referencia a la posesión del dominio se solicitara en cada ocasión, no siendo reutilizable.

Verificación de dominio

ACCV verificara el dominio solicitado para el certificado y las direcciones asociadas proporcionadas por el solicitante utilizando la información disponible en los registros públicos, requiriendo al solicitante las explicaciones o documentación adicional que pudiera ser necesaria. ACCV conserva esta información por cuestiones de auditoría, permitiendo su reutilización, salvo en el caso de la posesión de dominio, por un periodo no superior a 13 meses. ACCV no emite certificados a direcciones IP o dominios privados. En el caso de gTLD, solo se emiten certificados con nombres gTLD aprobados y comprobables, y exclusivamente a los suscriptores con control del gTLD, como aparece en ICANN/IANA.

Concretamente, se confirma que el solicitante ,cuya identidad se ha verificado sin duda, es uno de los registradores del dominio. Para esta comprobación la ACCV debe usar al menos unos de los siguientes métodos:

* Contactando por correo-e, enviando un numero aleatorio único asociado a un enlace de un solo uso que el solicitante debe pinchar para verificarlo. Este correo se envía a la dirección de correo registrada en el dominio y comprobable en un registro publico de confianza. El mensaje de correo de confirmación tiene una vigencia de 30 días.

* Contactando por correo-e, enviando un numero aleatorio único asociado a un enlace de un solo uso que el solicitante debe pinchar para verificarlo. Este correo se crea usando como parte local 'admin', 'administrator', 'webmaster', 'hostmaster', o 'postmaster',a continuación el caracter ("@"), y seguido por el nombre de dominio a autorizar. El mensaje de correo de confirmación tiene una vigencia de 30 días.

* Confirmando la presencia de un valor aleatorio único en un registro DNS del tipo TXT o CAA para 1) un nombre de autorización de dominio o 2)un nombre de autorización de dominio precedido por una etiqueta cuyo primer carácter sea un subrayado. Una vez comunicado el valor a incluir en el registro solo sera valido por 30 días.

* Confirmando la presencia de una valor aleatorio único contenido en un fichero de texto bajo el directorio “/.well-known/pki-validation" en servidor que responda al nombre de autorización de dominio accesible a la CA por HTTP/HTTPS por un puerto autorizado. Una vez comunicado el valor a incluir en el servidor solo sera valido por 30 días.

ACCV comprobará siempre el registro CAA justo antes de la emisión del certificado, y si el registro esta presente actuará como esta definido en el RFC-6844 y en la documentación del CAB Forum. El identificador CAA de la ACCV para los registros issue y issuewild es “accv.es”.

En el caso de certificados VPN no se admite la utilización de caracteres wildcard (*).

En presencia de cualquier irregularidad el solicitante del certificado sera notificado por la ACCV y la emisión quedará suspendida hasta su corrección. Si pasado un mes no se ha corregisdo la solicitud se denegará.

3.2.4. Información no verificada de los suscriptores

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

3.2.5. Validación de la representación

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

3.2.6. Criterios 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 de validaciones previas si no han pasado mas de 13 meses, excluyendo la información asociada a las comprobaciones de la posesión de dominio que se realiza en cada solicitud.

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. ACCV puede reutilizar la información de validaciones previas si no han pasado mas de 13 meses, excluyendo la información asociada a las comprobaciones de la posesión de dominio que se realiza en cada solicitud. ACCV puede implementar cualquier método que garantice de una forma inequívoca y segura la identidad del solicitante, teniendo en cuenta los medios técnicos disponibles y detallando todos los pasos del proceso.

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:

- Telemática. Mediante la firma electrónica de la solicitud de revocación (ubicada en el Área de Gestión de Certificados No Personales https://npsc.accv.es:8450/npsc) por parte del solicitante del certificado o del responsable del mismo en la fecha de la solicitud de revocación.
- Telefónico: Mediante llamada telefónica al número de soporte telefónico de la Agencia de Tecnología y Certificación Electrónica 902482481.

La Agencia de Tecnología y Certificación Electrónica 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 emitido al amparo de esta Política de Certificación, 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. Legitimación de la solicitud

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

4.1.2. Procedimiento de alta 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 servidor VPN 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 servidor VPN, se utilizaran los datos de Organización, Unidad Organizativa y Cargo de dicho certificado.

ACCV conserva la información asociada a la solicitud indefinidamente con un limite de al menos 15c años, incluyendo su aprobación o rechazo, y las razones del mismo.

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. Todas las comprobaciones se describen en el punto 3.2.3 de la presente politica.

4.2. Tramitación de la solicitud de certificados.

4.2.1. Ejecución de las funciones de identificación y autenticación

Tras recibir la solicitud de certificados por parte de las personas habilitadas al efecto y una vez aceptada la propuesta económica si fuera el caso, se procederá a la revisión de la solicitud.

ACCV comprobará los datos de la solicitud y acreditará al solicitante para la solicitud de certificados para servidores VPN, durante 13 meses a partir de la aprobación sin necesidad de aportar documentación adicional. En el caso de identificación con certificado de empleado público no existe limitación temporal mientras el certificado esté en vigor.

La autenticación de la identidad del solicitante se hará mediante la identificación con la Autoridad de Registro correspondiente (en este caso NPSC), utilizando los mecanismos descritos en la sección 3.2.3 *Autenticación de la identidad de un individuo*. La Autoridad de registro comprueba la documentación y valida los datos utilizando registros accesibles al público para dicha verificación.

En este proceso, ACCV comprueba que la solicitud de certificado no incluye dominios que puedan usarse para phising u otros usos fraudulentos, utilizando los mecanismo y listas disponibles.

4.2.2. Aprobación o rechazo de la solicitud

En caso de aceptación, la Autoridad de Registro notificará al solicitante por medio de un correo electrónico firmado digitalmente a la dirección de correo que figura en el perfil del usuario en la aplicación NPSC.

El solicitante debe acceder a NPSC con su certificado personal cualificado. Si el solicitante esta en condiciones técnicas y administrativas de llevar a cabo esta generación, la correspondiente opción le aparecerá habilitada en la aplicación.

En caso de rechazo, la Autoridad de Registro informará al solicitante mediante el correspondiente mecanismo. En las solicitudes utilizando un certificado cualificado, la Autoridad de Registro informará al usuario utilizando métodos interactivos que el proceso se detiene y el motivo que impide su continuación.
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 monitorización, investigación o confirmación de la exactitud de la información contenida en el certificado con posterioridad a su emisión. En el caso de recibir información sobre la inexactitud o la no aplicabilidad actual de la información contenida en el certificado, éste puede ser revocado.

El responsable del certificado para servidor VPN puede solicitar a la ACCV que añada a otros usuarios con capacidad para realizar los trámites asociados al ciclo de vida del certificado que tiene asociado. La Autoridad de Registro comprobará la solicitud de credenciales y comunicará mediante correo electrónico firmado al solicitante la autorización o denegación de los permisos.

ACCV puede efectuar esta autorización de oficio en los casos en los que el responsable del certificado para servidor VPN pierda la capacidad necesaria para gestionarlo y no haya otras personas autorizadas.

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

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

4.3.1. Acciones de la CA durante el proceso de emisión

La emisión del certificado se produce una vez la RA a llevado a cabo las verificaciones necesarias para validar la solicitud de certificado. El mecanismo que determina la naturaleza y forma de esas validaciones es esta Política de Certificación.

En la solicitudes realizadas con un certificado personal cualificado los pasos son los siguientes:

- El solicitante se identifica con su certificado personal cualificado correspondiente en NPSC

- Accede a la parte de solicitudes aceptadas y busca las disponibles.

- Pulsa el enlace asociado a la acción de Generar.

- La RA comprueba que no existe un registro CAA contrario asociado al dominio.

- RA pregunta al solicitante el mecanismo de generación del par de claves y la petición de certificado de entre las opciones permitidas y con los parámetros definidos en esta política..

- RA envía la petición de certificado firmada (CSR) a la CA.

- CA realiza una verificación de la firma de la RA y confirma el formato del CSR.

- CA firma el CSR y lo envía de vuelta a la RA.

- RA comunica el certificado al solicitante.

Todos estos procesos se realizan en la plataforma de generación proporcionada por la ACCV.

4.3.2. Notificación de la emisión al suscriptor

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

4.4. Aceptación de certificados

4.4.1. Conducta que constituye aceptación del certificado

La aceptación de los certificados por parte de los suscriptores se produce en el momento de la firma 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 firmado por el solicitante, y cuyo fin es vincular a la persona que solicita el certificado para servidores VPN, 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 CA

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

4.4.3. Notificación de la emisión a terceros

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

4.5. Uso del par de claves y del certificado.

4.5.1. Uso del certificado y la clave privada del suscriptor

Los usos de la clave vienen definidos en el contenido del certificado en las extensiones: keyUsage, extendedKeyUsage y basicConstraints. Estas extensiones se detallan en el apartado *7.1.2 Extensiones del certificado*.

4.5.2. Uso de la clave pública y del certificado por la parte que confía

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

4.6. Renovación de certificados.

La renovación de certificados debe ser realizada utilizando los mismos procedimientos y métodos de identificación que los establecidos para realizar la solicitud inicial.

4.6.1. Circunstancia 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 renovación

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

4.6.3. Procesamiento 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 nueva emisión de 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 un certificado de renovación

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

4.6.6. Publicación del certificado de renovación por la CA

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

4.6.7. Notificación de emisión de certificado por la CA 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. Circunstancia para la renovación de claves (re-key) certificado

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

4.7.2. Quién puede solicitar la certificación de una nueva clave pública

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

4.7.3. Procesamiento de solicitudes de cambio de claves del certificado

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

4.7.4. Notificación de nueva emisión de certificado al suscriptor

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

4.7.5. Conducta que constituye la aceptación de un certificado con nuevas claves (re-keyed)

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

4.7.6. Publicación del certificado con renovación de claves (re-keyed) por la CA

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

4.7.7. Notificación de emisión de certificado por la CA 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. Circunstancia 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 de certificados

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

4.8.4. Notificación de nueva emisión de certificado al suscriptor

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

4.8.5. Conducta que constituye la aceptación de un certificado modificado

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

4.8.6. Publicación del certificado modificado por la CA

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

4.8.7. Notificación de emisión de certificado por la CA 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. 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.

4.9.3.2. Telefónico

Mediante llamada telefónica al número de soporte telefónico de la Agencia de Tecnología y Certificación Electrónica 902482481.

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 CA debe procesar la solicitud de revocación

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

4.9.6. Requisitos de comprobación de CRLs
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. Máxima latencia de CRL
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.9. Disponibilidad de comprobación on-line de la revocación
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.10. Requisitos de la comprobación on-line de la revocación
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.11. Otras formas de divulgación de información de revocación disponibles
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.12. Requisitos especiales de revocación por compromiso de las claves
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.
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.10.1. Características operacionales
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 servidores VPN, 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. Política y prácticas clave de custodia y recuperación

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

4.12.2. Política y prácticas de encapsulado y recuperación de claves de sesión

La recuperación de las claves de sesión no esta soportado.

5. CONTROLES DE SEGURIDAD FÍSICA, PROCEDURAL Y DE PERSONAL

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. Roles 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. Procedimientos de gestión de incidencias y compromisos

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

5.7.2. Corrupción de recursos, aplicaciones o datos

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

5.7.3. Compromiso de la clave privada de la entidad

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

5.7.4. Continuidad del 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.

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 2048 bits.

6.1.6. Parámetros de generación de la clave pública

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**
sha256-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.

6.2.1. Estándares para los módulos criptográficos

Los certificados emitidos en virtud de esta política se basan en software, por lo que las normas y controles de los módulos criptográficos dependen del sistema operativo del suscriptor.

6.2.2. Control multipersona de la clave privada

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

6.2.3. Custodia de la clave privada

No se custodian claves privadas de firma, autenticación ni cifrado de los suscriptores de los certificados definidos por la presente política.

6.2.4. Copia de seguridad de la clave privada

No se custodian claves privadas de firma, autenticación y cifrado de los suscriptores de los certificados definidos por la presente política, por lo que no es aplicable.

6.2.5. Archivo de la clave privada.

No se archivan las claves privadas.

6.2.6. Introducción de la clave privada en el módulo criptográfico.

El par de claves se genera en software. No hay dispositivos criptográficos.

6.2.7. Almacenamiento de clave privada en el módulo criptográfico.

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

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 Agencia de Tecnología y Certificación Electrónica.

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 Agencia de Tecnología y Certificación Electrónica.

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 Agencia de Tecnología y Certificación Electrónica. Se podrá destruir mediante el borrado de esta siguiendo las instrucciones de la aplicación que la alberga.

6.2.11. Calificación del módulo criptográfico

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) 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. Periodo de uso para las claves públicas y privadas

Los certificados emitidos al amparo de la presente política tienen una validez de 27 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 27 meses como máximo.

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

La clave privada es generada por el solicitante y nunca está en posesión de la Agencia de Tecnología y Certificación Electrónica.

6.4.2. Protección de los datos de activación

El responsable 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. Requerimientos técnicos de seguridad informática específicos

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

6.5.2. Valoración de la 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 del sistema

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. Evaluación de la 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. TimeStamping

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

7. PERFILES DE CERTIFICADO Y CRL

7.1. Perfil de Certificado

7.1.1. Número de versión

La presente política se implementa sobre certificados X.509 versión 3 (X.509 v3).

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.
CommonName	Nombre completo del servidor VPN 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
OrganizationalUnit	Cadena fija con valor VPN
Organization	Denominación (nombre “oficial”) de la Administración, organismo o entidad de derecho público suscriptora del certificado y propietaria del dominio.
Locality	Ciudad
State	Provincia
Country	Cadena fija con el valor 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 certificado de servidores VPN
Extended Key Usage	
	Server Authentication Internet Key Exchange for IPSec
CRL Distribution Point	
	distributionPoint http://www.accv.es/fileadmin/Archivos/certificados/accvca120_der.crl

Certificate Policy Extensions		
Policy OID	{itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ovcp(7)} 0.4.0.2042.1.7	
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	1.3.6.1.4.1.8149.3.8.4.0	
Policy CPS Location	http://www.accv.es/legislacion_c.htm*	
Policy Notice	Certificado Cualificado para servidores VPN expedido por la ACCV (Plaza Nápoles y Sicilia, 6. Valencia CP 46003, 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)		
	Digital Signature Key Encipherment	
QcStatement	**Campos QC (Qualified Certificate)**	
QcCompliance		
QcType	web	
QcRetentionPeriod	15y	
QcPDS	https://www.accv.es/fileadmin/Archivos/Practicas_de_certificacion/ACCV-PDS-V1.0-EN.pdf	

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.

a) 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.

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:

1.3.6.1.4.1.8149.3.8.3.0

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

0.4.0.194112.1.4	**Política de certificación para certificados cualificados EU emitidos a sitios web**

En este caso se añade un OID para identificar el tipo de entidad que se representa según la 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**

En este caso se añade un OID para identificar el tipo de entidad que se representa según el estandar ETSI EN 319 411-1

0.4.0.2042.1.7	**Organizational Validation Certificate Policy (OVCP)**

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 CertificatePolicy puede incluir dos campos Calificadores de Política, ambos opcionales:

CPS Pointer: Contiene la URL donde se publica la Política.

User Notice: Contiene un texto descriptivo.

7.1.9. Tratamiento semántico para la extensión “Certificate Policy”

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

7.1.10. Lista de Sellos CT firmados

Respuestas de logs cualificados conocidos, que cumplen con la política de Certificate Transparency de Chrome.

Extension OID: 1.3.6.1.4.1.11129.2.4.2

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

El numero minimo de respuestas se determina por el ciclo de vida del certificado de acuerdo con la siguiente tabla:

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 de OCSP

7.3.1. Número 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.

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

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

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

9.2. Capacidad financiera

9.2.1. Cobertura del Seguro

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. Seguro o cobertura de garantía para entidades finales

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. Responsabilidad de proteger la información confidencial

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

9.4. Privacidad de la información personal

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

9.4.1. Plan de privacidad

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. Responsabilidad de proteger la información privada

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

9.4.5. Aviso y consentimiento para usar información privada

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. Obligación y responsabilidad de terceras partes

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

9.6.5. Obligación y responsabilidad 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 se debe cambiar el OID

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

9.13. Resolución de conflictos.

9.13.1. Resolución extrajudicial de conflictos.

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

9.13.2. Jurisdicción competente.

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

9.14. Legislación aplicable

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

9.15. Conformidad con la Ley aplicable.

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

9.16. Cláusulas diversas.

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

9.16.1. Acuerdo completo

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. Separabilidad

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

9.16.4. Cumplimiento (honorarios de abogados y exención de 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.

Anexo I

CONTRATO DE CERTIFICACIÓN – CÓDIGO 1.3.6.1.4.1.8149.3.8.4.0

Sección 1 – Datos del solicitante

Apellidos: .....

Nombre: ..... DNI/NIF: .....

Organismo / Servicio: .....

Organización: .....

Dirección correo electrónico: .....

Dirección postal: ..... Tel.: .....

Sección 2 – Datos del Sistema informático a certificar

Nombre cualificado: .....

Alias (si el certificado no se emite al nombre cualificado):.....

Dirección IP: .....

Sección 4 – Fecha y Firma

Solicito el Certificado asociado a la Política de Certificación con código 1.3.6.1.4.1.8149.3.8.4.0, para Servidores VPN, 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 expuestos en **http://www.accv.es**. Declaro, asimismo, que los datos expuestos son verdaderos.

En ..... a ..... de ..... de 2.0....

Firma del solicitante

Fdo.:

CONTRATO DE CERTIFICACIÓN – CÓDIGO 1.3.6.1.4.1.8149.3.8.4.0
Condiciones de utilización de los certificados

1. Los certificados asociados a la la Política de Certificación para Certificados de Servidores VPN, emitidos por la ACCV son del tipo X.509v3 y se rigen por la Declaración de Prácticas de la ACCV, 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. El solicitante de los certificados debe ser una persona física, en posesión de un certificado cualificado.

3. El solicitante de los certificados, especialmente habilitado para la gestión de éstos por parte de una Administración o Entidad 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 de las comunicaciones o los datos transferidos utilizando este certificado.

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 ACCV y en la Política de Certificación asociada a este tipo de certificados.

8. El periodo de validez de estos certificados es de 27 meses como máximo. 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 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 cualificado personal.

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

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

13. El solicitante podrá ejercer sus derechos de acceso, rectificación 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 indicando claramente esta voluntad.

14. La Agencia de Tecnología y Certificación Electrónica ha constituido un aval bancario por un importe de tres millones de euros (3.000.000,00 €) para afrontar el riesgo por la responsabilidad por los daños y perjuicios que pudiera ocasionar el uso de los certificados expedidos y los servicios de certificación digital.

    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.