Agencia de Tecnología y Certificación Electrónica

Política de Certificación de Certificados Cualificados de Autenticación de Sitios Web

Fecha: 27/06/2017	**Versión:** 4.0
Estado: APROBADO	**Nº de páginas:** 35
OID: 1.3.6.1.4.1.8149.3.3.4.0	**Clasificación: PÚBLICO**
Archivo: ACCV-CP-3V4.0-c.doc	
Preparado por: Agencia de Tecnología y Certificación Electrónica - ACCV	

Tabla de Contenido

1. INTRODUCCIÓN....7

1.1. PRESENTACIÓN....7
1.2. IDENTIFICACIÓN....7
1.3. COMUNIDAD DE USUARIOS Y ÁMBITO DE APLICACIÓN....7
1.3.1. Autoridades de Certificación....7
1.3.2. Autoridades de Registro....8
1.3.3. Usuarios Finales....8
1.3.3.1. Suscriptores....8
1.3.3.2. Partes confiantes....8
1.4. USO DE LOS CERTIFICADOS....8
1.4.1. Usos Permitidos....8
1.4.2. Usos prohibidos....8
1.5. POLÍTICA DE ADMINISTRACIÓN DE LA ACCV....8
1.5.1. Especificación de la Organización Administradora....8
1.5.2. Persona de Contacto....9
1.5.3. Competencia para determinar la adecuación de la CPS a la Políticas....9
1.6. DEFINICIONES Y ACRÓNIMOS....9
1.6.1. Definiciones....9
1.6.2. Acrónimos....9

2. PUBLICACIÓN DE INFORMACIÓN Y REPOSITORIO DE CERTIFICADOS....10

2.1. REPOSITORIO DE CERTIFICADOS....10
2.2. PUBLICACIÓN....10
2.3. FRECUENCIA DE ACTUALIZACIONES....10
2.4. CONTROLES DE ACCESO AL REPOSITORIO DE CERTIFICADOS....10

3. IDENTIFICACIÓN Y AUTENTICACIÓN....11

3.1. REGISTRO DE NOMBRES....11
3.1.1. Tipos de nombres....11
3.1.2. Significado de los nombres....11
3.1.3. Interpretación de formatos de nombres....11
3.1.4. Unicidad de los nombres....11
3.1.5. Resolución de conflictos relativos a nombres....11
3.1.6. Reconocimiento, autenticación y función de las marcas registradas....11
3.2. VALIDACIÓN INICIAL DE LA IDENTIDAD....11
3.2.1. Métodos de prueba de posesión de la clave privada....11
3.2.2. Autenticación de la identidad de una organización....11
3.2.3. Autenticación de la identidad de un individuo....11
3.3. IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE RENOVACIÓN DEL PAR DE CLAVES....12
3.3.1. Identificación y autenticación de las solicitudes de renovación rutinarias....12
3.3.2. Identificación y autenticación de las solicitudes de renovación de clave después de una revocación – Clave no comprometida....12
3.4. IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE REVOCACIÓN DEL PAR DE CLAVES....12

4. EL CICLO DE VIDA DE LOS CERTIFICADOS....13

4.1. SOLICITUD DE CERTIFICADOS....13
4.2. TRAMITACIÓN DE LA SOLICITUD DE CERTIFICADOS....13
4.3. EMISIÓN DE CERTIFICADOS....13
4.4. ACEPTACIÓN DE CERTIFICADOS....14
4.5. USO DEL PAR DE CLAVES Y DEL CERTIFICADO....14
4.6. RENOVACIÓN DE CERTIFICADOS....14
4.7. RENOVACIÓN DE CLAVES....14
4.8. MODIFICACIÓN DE CERTIFICADOS....14
4.9. REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS....14
4.9.1. Circunstancias para la revocación....14

4.9.2. Entidad que puede solicitar la revocación *14*
4.9.3. Procedimiento de solicitud de revocación *14*
4.9.3.1. Telemático 14
4.9.4. Periodo de gracia de la solicitud de revocación *14*
4.9.5. Circunstancias para la suspensión *14*
4.9.6. Entidad que puede solicitar la suspensión *14*
4.9.7. Procedimiento para la solicitud de suspensión *14*
4.9.8. Límites del período de suspensión *15*
4.9.9. Frecuencia de emisión de CRLs *15*
4.9.10. Requisitos de comprobación de CRLs *15*
4.9.11. Disponibilidad de comprobación on-line de revocación y estado *15*
4.9.12. Requisitos de comprobación on-line de revocación *15*
4.9.13. Otras formas de divulgación de información de revocación disponibles *15*
4.9.14. Requisitos de comprobación para otras formas de divulgación de información de revocación *15*
4.9.15. Requisitos especiales de renovación de claves comprometidas *15*
4.10. SERVICIOS DE COMPROBACIÓN DE ESTADO DE CERTIFICADOS 15
4.11. FINALIZACIÓN DE LA SUSCRIPCIÓN 15
4.12. DEPÓSITO Y RECUPERACIÓN DE CLAVES 15
4.13. CADUCIDAD DE LAS CLAVES DE CERTIFICADO DE CA 15
5. CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES 17
5.1. CONTROLES DE SEGURIDAD FÍSICA 17
5.1.1. Ubicación y construcción *17*
5.1.2. Acceso físico *17*
5.1.3. Alimentación eléctrica y aire acondicionado *17*
5.1.4. Exposición al agua *17*
5.1.5. Protección y prevención de incendios *17*
5.1.6. Sistema de almacenamiento *17*
5.1.7. Eliminación de residuos *17*
5.1.8. Backup remoto *17*
5.2. CONTROLES DE PROCEDIMIENTOS 17
5.2.1. Papeles de confianza *17*
5.2.2. Número de personas requeridas por tarea *17*
5.2.3. Identificación y autenticación para cada papel *17*
5.3. CONTROLES DE SEGURIDAD DE PERSONAL 17
5.3.1. Requerimientos de antecedentes, calificación, experiencia, y acreditación *17*
5.3.2. Procedimientos de comprobación de antecedentes *18*
5.3.3. Requerimientos de formación *18*
5.3.4. Requerimientos y frecuencia de actualización de la formación *18*
5.3.5. Frecuencia y secuencia de rotación de tareas *18*
5.3.6. Sanciones por acciones no autorizadas *18*
5.3.7. Requerimientos de contratación de personal *18*
5.3.8. Documentación proporcionada al personal *18*
5.3.9. Controles periódicos de cumplimiento *18*
5.3.10. Finalización de los contratos *18*
5.4. PROCEDIMIENTOS DE CONTROL DE SEGURIDAD 18
5.4.1. Tipos de eventos registrados *18*
5.4.2. Frecuencia de procesado de logs *18*
5.4.3. Periodo de retención para los logs de auditoría *18*
5.4.4. Protección de los logs de auditoría *18*
5.4.5. Procedimientos de backup de los logs de auditoría *18*
5.4.6. Sistema de recogida de información de auditoría (interno vs externo) *18*
5.4.7. Notificación al sujeto causa del evento *18*
5.4.8. Análisis de vulnerabilidades *19*
5.5. ARCHIVO DE INFORMACIONES Y REGISTROS 19
5.5.1. Tipo de informaciones y eventos registrados *19*
5.5.2. Periodo de retención para el archivo *19*
5.5.3. Protección del archivo *19*
5.5.4. Procedimientos de backup del archivo *19*
5.5.5. Requerimientos para el sellado de tiempo de los registros *19*

5.5.6. Sistema de recogida de información de auditoría (interno vs externo)....19
5.5.7. Procedimientos para obtener y verificar información archivada....19
5.6. Cambio de Clave....19
5.7. Recuperación en caso de compromiso de una clave o de desastre....19
5.7.1. Alteración de los recursos hardware, software y/o datos....19
5.7.2. La clave pública de una entidad se revoca....19
5.7.3. La clave de una entidad se compromete....19
5.7.4. Instalación de seguridad después de un desastre natural u otro tipo de desastre....19
5.8. Cese de una CA....20
6. CONTROLES DE SEGURIDAD TÉCNICA....21
6.1. Generación e Instalación del par de claves....21
6.1.1. Generación del par de claves....21
6.1.2. Entrega de la clave privada a la entidad....21
6.1.3. Entrega de la clave pública al emisor del certificado....21
6.1.4. Entrega de la clave pública de la CA a los usuarios....21
6.1.5. Tamaño de las claves....21
6.1.6. Parámetros de generación de la clave pública....21
6.1.7. Comprobación de la calidad de los parámetros....22
6.1.8. Hardware/software de generación de claves....22
6.1.9. Fines del uso del par de claves....22
6.2. Protección de la Clave Privada....22
6.2.1. Estándares para los módulos criptográficos....22
6.2.2. Características del servidor bastionado....22
6.2.3. Control multipersona de la clave privada....22
6.2.4. Custodia de la clave privada....22
6.2.5. Copia de seguridad de la clave privada....23
6.2.6. Archivo de la clave privada....23
6.2.7. Introducción de la clave privada en el módulo criptográfico....23
6.2.8. Método de activación de la clave privada....23
6.2.9. Método de desactivación de la clave privada....23
6.2.10. Método de destrucción de la clave privada....23
6.3. Otros Aspectos de la Gestión del par de claves....23
6.3.1. Archivo de la clave pública....23
6.3.2. Periodo de uso para las claves públicas y privadas....23
6.3.3. Los certificados emitidos al amparo de la presente política tienen una validez de tres (3) años....23
6.4. Datos de activación....23
6.4.1. Generación y activación de los datos de activación....23
6.4.2. Protección de los datos de activación....23
6.4.3. Otros aspectos de los datos de activación....23
6.5. Controles de Seguridad Informática....24
6.6. Controles de Seguridad del Ciclo de Vida....24
6.7. Controles de Seguridad de la Red....24
6.8. Controles de Ingeniería de los Módulos Criptográficos....24
7. PERFILES DE CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS....25
7.1. Perfil de Certificado....25
7.1.1. Número de versión....25
7.1.2. Extensiones del certificado....25
7.1.3. Identificadores de objeto (OID) de los algoritmos....27
7.1.4. Formatos de nombres....27
7.1.5. Restricciones de los nombres....27
7.1.6. Identificador de objeto (OID) de la Política de Certificación....27
7.1.7. Uso de la extensión "Policy Constraints"....27
7.1.8. Sintaxis y semántica de los cualificadores de política....27
7.1.9. Tratamiento semántico para la extensión "Certificate Policy"....27
7.2. Perfil de CRL....28
7.2.1. Número de versión....28
7.2.2. CRL y extensiones....28
7.3. Listas de Certificados Revocados....28

7.3.1. Límite Temporal de los certificados en las CRLs....28

8. AUDITORÍA DE CONFORMIDAD....29

8.1. Frecuencia de los controles de conformidad para cada entidad....29
8.2. Identificación/cualificación del auditor....29
8.3. Relación entre el auditor y la entidad auditada....29
8.4. Tópicos cubiertos por el control de conformidad....29
8.5. Acciones a tomar como resultado de una deficiencia....29
8.6. Comunicación de resultados....29

9. REQUISITOS COMERCIALES Y LEGALES....30

9.1. Tarifas....30
9.1.1. Tarifas de emisión de certificado o renovación....30
9.1.2. Tarifas de acceso a los certificados....30
9.1.3. Tarifas de acceso a la información de estado o revocación....30
9.1.4. Tarifas de otros servicios como información de políticas....30
9.1.5. Política de reintegros....30
9.2. Capacidad financiera....30
9.2.1. Indemnización a los terceros que confían en los certificados emitidos por la ACCV....30
9.2.2. Relaciones fiduciarias....30
9.2.3. Procesos administrativos....30
9.3. Política de Confidencialidad....30
9.3.1. Información confidencial....30
9.3.2. Información no confidencial....30
9.3.3. Divulgación de información de revocación /suspensión de certificados....30
9.4. Protección de datos personales....31
9.4.1. Plan de Protección de Datos Personales....31
9.4.2. Información considerada privada....31
9.4.3. Información no considerada privada....31
9.4.4. Responsabilidades....31
9.4.5. Prestación del consentimiento en el uso de los datos personales....31
9.4.6. Comunicación de la información a autoridades administrativas y/o judiciales....31
9.4.7. Otros supuestos de divulgación de la información....31
9.5. Derechos de propiedad Intelectual....31
9.6. Obligaciones y Responsabilidad Civil....31
9.6.1. Obligaciones de la Entidad de Certificación....31
9.6.2. Obligaciones de la Autoridad de Registro....31
9.6.3. Obligaciones de los suscriptores....31
9.6.4. Obligaciones de los terceros confiantes en los certificados emitidos por la ACCV....31
9.6.5. Obligaciones del repositorio....31
9.7. Renuncias de garantías....32
9.8. Limitaciones de responsabilidad....32
9.8.1. Garantías y limitaciones de garantías....32
9.8.2. Deslinde de responsabilidades....32
9.8.3. Limitaciones de pérdidas....32
9.9. Plazo y finalización....32
9.9.1. Plazo....32
9.9.2. Finalización....32
9.9.3. Supervivencia....32
9.10. Notificaciones....32
9.11. Modificaciones....32
9.11.1. Procedimientos de especificación de cambios....32
9.11.2. Procedimientos de publicación y notificación....32
9.11.3. Procedimientos de aprobación de la Declaración de Prácticas de Certificación....32
9.12. Resolución de conflictos....33
9.12.1. Resolución extrajudicial de conflictos....33
9.12.2. Jurisdicción competente....33
9.13. Legislación aplicable....33
9.14. Conformidad con la Ley aplicable....33
9.15. Cláusulas diversas....33

10. ANEXO I.....34

1. INTRODUCCIÓN

1.1. Presentación

El presente documento es la Política de Certificación asociada a los certificados cualificados 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 cualificados 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.

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 de Autenticación de Sitios Web
Calificador de la política	Certificado cualificados de autenticación de sitios web expedido por el Instituto Valenciano de Finanzas - ACCV (Plaza Nápoles y Sicilia, 6. Valencia CP 46003, ESPAÑA. CIF Q9650010C). CPS y CP en http://www.accv.es
Versión de la política	4.0
Estado de la política	APROBADO
Referencia de la política / OID (Object Identifier)	1.3.6.1.4.1.8149.3.3.4.0
Fecha de emisión	01/06/2017
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 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 IVF (ACCV).

1.3.3. Usuarios Finales

1.3.3.1. 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.

1.3.3.2. 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.

1.4. 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

Nombre	*Agencia de Tecnología y Certificación Electrónica IVF*
Dirección de email	*accv@accv.es*
Dirección	*Plaza Nápoles y Sicilia , 6 –46003 Valencia (Spain)*
Número de teléfono	*+34 902 482 481*
Número de fax	*+34·961 971 771*

1.5.2. Persona de Contacto

Nombre	*Agencia de Tecnología y Certificación Electrónica IVF*
Dirección de email	*accv@accv.es*
Dirección	*Plaza Nápoles y Sicilia , 6 –46003 Valencia (Spain)*
Número de teléfono	*+34 902 482 481*
Número de fax	*+34·961 971 771*

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

La entidad competente para determinar la adecuación de esta CPS a las diferentes Políticas de Certificación de la ACCV, es la Subdirección de Entidades Financieras y Certificación Electrónica - IVF de conformidad con los Estatutos del Instituto Valenciano de Finanzas (IVF).

1.6. Definiciones y Acrónimos

1.6.1. Definiciones

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.

1.6.2. Acrónimos

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

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 Autenticación

3.1. Registro de nombres

3.1.1. Tipos de nombres

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

3.1.2. Significado de los nombres

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

3.1.3. Interpretación de formatos de nombres

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

3.1.4. Unicidad de los nombres

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

3.1.5. Resolución de conflictos relativos a nombres

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

3.1.6. Reconocimiento, autenticación y función de las marcas registradas.

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

3.2. Validación inicial de la identidad

3.2.1. Métodos de prueba de posesión de la clave privada.

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

3.2.2. Autenticación de la identidad de una organización.

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

3.2.3. Autenticación de la identidad de un individuo.

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

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.

ACCV comprobará ambos datos utilizando para ello la información disponible de registros de personal y de dominio, requiriendo al solicitante o a la entidad representada 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.

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. 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. 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

La solicitud de este tipo de certificados es responsabilidad de entidades publicas o privadas.

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 sitio web 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 sitio web, 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 sitio web, 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.

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.

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 aprobación de la solicitud. Tras la aprobación, la Autoridad de Registro lo notificará al solicitante mediante el envío de un correo electrónico firmado a la dirección que figure en la solicitud. El usuario deberá entrar en el Área de gestión de certificados no personales (NPSC) ubicada en https://npsc.accv.es:8450/npsc identificándose con un certificado cualificado personal para generar y descargar el certificado.

Esta aprobación se realizara por un miembro de la ACCV distinto del responsable de realizar la verificación de los datos. La diferenciación de los roles se realizará utilizando las capacidades establecidas en la aplicación de gestión.

4.3. Emisión de certificados

ACCV realizará revisiones periódicas sobre muestreos de los certificados de autenticación web para garantizar la exactitud y vigencia de los datos. Si en el transcurso de estos muestreos se confirmara un cambio de los datos que implicara la perdida de posesión del dominio, la ACCV revocará de oficio los certificados implicados. Se procederá de igual manera en el caso de recibir información sobre la inexactitud o la no aplicabilidad actual de la información contenida en el certificado. ACCV dejará constancia documental de todas estas revisiones y actuaciones.

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

El responsable del certificado de autenticación de sitios web 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 de autenticación de sitio web pierda la capacidad necesaria para gestionarlo y no haya otras personas autorizadas.

4.4. Aceptación de certificados

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 sitio web, 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.

4.5. Uso del par de claves y del certificado.

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

4.6. Renovación de certificados.

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.

4.8. Modificación de certificados.

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.

4.9.4. 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. 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.

4.9.6. Entidad que puede solicitar la suspensión

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

4.9.7. Procedimiento para la solicitud de suspensión

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

4.9.8. Límites del período de suspensión

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

4.9.9. Frecuencia de emisión de CRLs

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

4.9.10. Requisitos de comprobación de CRLs

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

4.9.11. Disponibilidad de comprobación on-line de revocación y estado

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

4.9.12. Requisitos de comprobación on-line de revocación

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

4.9.13. Otras formas de divulgación de información de revocación disponibles

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

4.9.14. Requisitos de comprobación para otras formas de divulgación de información de revocación

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

4.9.15. Requisitos especiales de renovación de claves comprometidas

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.

4.11. 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 sitio web, 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.

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

4.13. Caducidad de las claves de certificado de CA.

ACCV evitará generar certificados de autenticación de sitio web que caduquen con posterioridad a los certificados de CA. Para ello no se emitirán certificados de autenticación de sitio web 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.

5.3. 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
No estipulado.

5.7. Recuperación en caso de compromiso de una clave o de desastre
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

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

5.7.2. La clave pública de una entidad se revoca
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.7.3. La clave de una entidad se compromete
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.7.4. Instalación de seguridad después de un desastre natural u otro tipo de desastre
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.8. Cese de una CA

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

6. Controles de seguridad técnica

6.1. Generación e Instalación del par de claves

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

6.1.1. Generación del par de claves

El par de claves para el certificado emitido bajo el ámbito de la presente Política de Certificación se 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

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

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

Se utilizan los parámetros definidos en la suite criptográfica 001 especificada en el documento de ETSI TS 102 176-1 “Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signature”. Se define ModLen=2048.

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

6.1.7. Comprobación de la calidad de los parámetros

Se utilizan los parámetros definidos en la suite criptográfica 001 especificada en el documento de ETSI TS 102 176-1 “Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signature”. Se define ModLen=2048.

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

6.1.8. Hardware/software de generación de claves

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

6.1.9. Fines del uso del par de claves

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

No aplicable en el ámbito de la presente Política.

6.2.2. Características del servidor bastionado

Los sistemas donde se almacenen las claves privadas deben cumplir una serie de requisitos relativos a la seguridad física y lógica de los mismos. ACCV podrá, de manera discrecional, solicitar al organismo suscriptor que evidencie los mecanismos utilizados para el bastionado de dichos sistemas.

Se recomienda seguir las guías generadas por el CCN (Centro Criptológico Nacional) dentro de su serie CCN-STIC, orientadas específicamente a garantizar la seguridad de los sistemas de las tecnologías de la información y la comunicaciones de la Administración.

6.2.3. 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.

6.2.4. Custodia de la clave privada

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

6.2.5. Copia de seguridad de la clave privada

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

6.2.6. Archivo de la clave privada.

No se archivan las claves privadas.

6.2.7. Introducción 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 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

No estipulado.

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 estipulado.

6.5. Controles 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.

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. Controles de Ingeniería de los Módulos Criptográficos

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

7. Perfiles de certificados y listas de certificados revocados

7.1. Perfil de Certificado

7.1.1. Número de versión

Esta política de certificación especifica el uso de un certificado con tres usos distintos; firma digital, autenticación del suscriptor y cifrado de datos.

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
OrganizationalUnit	Cadena fija con el valor SERVIDORES
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
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

CRL Distribution Point		
	distributionPoint	http://www.accv.es/fileadmin/Archivos/certificados/accvca120_der.crl
	distributionPoint	http://www.accv.es/gestcert/accvca120_der.crl
SubjectAlternativeName		
	dnsName	Nombre Dominio DNS 1 (coincide con el dominio en el common name)
	dnsName	Nombre Dominio DNS 2
	dnsName	Nombre Dominio DNS 3
Certificate Policy Extensions		
Policy OID	QCP-w Certificado cualificado de sitio web acorde al Reglamento UE 910/2014 itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-web (4)	
Policy OID	1.3.6.1.4.1.8149.3.3.4.0	
Policy CPS Location	http://www.accv.es/legislacion_c.htm*	
Policy Notice	Certificado cualificados de autenticación de sitios web expedido por el Instituto Valenciano de Finanzas - ACCV (Plaza Nápoles y Sicilia, 6. Valencia CP 46003, ESPAÑA. CIF Q9650010C). CPS y CP en http://www.accv.es	
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		El certificado es cualificado
QcType	web	Tipo particular de certificado cualificado
QcRetentionPeriod	15y	Periodo de retención de la información material
QcPDS	https://www.accv.es/fileadmin/Archivos/Practicas_de_certificacion/ACCV-PDS-V1.0-EN.pdf	Ubicación de PKI Disclosure Statement

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.

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:

1.3.6.1.4.1.8149.3.3.4.0

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**

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

No estipulado

7.1.9. Tratamiento semántico para la extensión “Certificate Policy”

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

7.2. Perfil de CRL

7.2.1. Número de versión

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

7.2.2. CRL y extensiones

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

7.3. Listas de Certificados Revocados

7.3.1. Límite Temporal de los certificados en las CRLs

Los números de serie de los certificados revocados aparecerán en las CRL hasta que alcance su fecha de expiración.

8. Auditoría de conformidad

8.1. Frecuencia de los controles de conformidad para cada entidad

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

8.2. Identificación/cualificación del auditor

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

8.3. Relación entre el auditor y la entidad auditada

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

8.4. Tópicos cubiertos por el control de conformidad

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

8.5. Acciones a tomar como resultado de una deficiencia.

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

8.6. Comunicación de resultados

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

9. Requisitos comerciales y legales

9.1. Tarifas

9.1.1. Tarifas de emisión de certificado o renovación

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

9.1.2. Tarifas de acceso a los certificados

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

9.1.3. Tarifas de acceso a la información de estado o revocación

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

9.1.4. Tarifas de otros servicios como información de políticas

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

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

Tal y como se especifica en la Declaración de Prácticas de Certificación (CPS), la ACCV dispone de garantía de cobertura suficiente de responsabilidad civil a través de aval bancario por importe de Tres Millones de Euros (3.000.000 €) que cubre el riesgo de la responsabilidad por los daños y perjuicios que pudiera ocasionar el uso de los certificados expedidos por esta Agencia, cumpliendo así con la obligación establecida en el artículo 20.2 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

9.2.2. Relaciones fiduciarias

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

9.2.3. Procesos administrativos

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

9.3. Política de Confidencialidad

9.3.1. Información confidencial.

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

9.3.2. Información no confidencial

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

9.3.3. Divulgación de información de revocación /suspensión de certificados

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

9.4. Protección de datos personales

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

9.4.1. Plan de Protección de Datos Personales.

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

9.4.2. Información considerada privada.

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

9.4.3. Información no considerada privada.

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

9.4.4. Responsabilidades.

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

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

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

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

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

9.4.7. Otros supuestos de divulgación de la información.

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

9.5. Derechos de propiedad Intelectual

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

9.6. Obligaciones y Responsabilidad Civil

9.6.1. Obligaciones de la Entidad de Certificación

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

9.6.2. Obligaciones de la Autoridad de Registro

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

9.6.3. Obligaciones de los suscriptores

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

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

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

9.6.5. Obligaciones del repositorio

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

9.7. Renuncias de garantías

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

9.8. Limitaciones de responsabilidad

9.8.1. Garantías y limitaciones de garantías

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

No obstante no existen límites económicos asociados a las transacciones que se realicen con este tipo de certificados por parte de los suscriptores.

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. Plazo y finalización.

9.9.1. Plazo.

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

9.9.2. Finalización.

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

9.9.3. Supervivencia.

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

9.10. 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.

9.11. Modificaciones.

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

9.11.1. Procedimientos de especificación de cambios

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

9.11.2. Procedimientos de publicación y notificación.

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

9.11.3. Procedimientos de aprobación de la Declaración de Prácticas de Certificación

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

9.12. Resolución de conflictos.

9.12.1. Resolución extrajudicial de conflictos.

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

9.12.2. Jurisdicción competente.

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

9.13. Legislación aplicable

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

9.14. Conformidad con la Ley aplicable.

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

9.15. Cláusulas diversas.

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

10. Anexo I

CONTRATO DE CERTIFICACIÓN – CÓDIGO 1.3.6.1.4.1.8149.3.3
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 Cualificados de Autenticación de Sitios Web con código 1.3.6.1.4.1.8149.3.3, 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 1.3.6.1.4.1.8149.3.3

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 la Administración Pública, Ente Instrumental de la Administración o Entidad Corporativa de Derecho Público 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 una Administración o Entidad pública 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 27 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 15/1.999, de 13 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, denominado "Usuarios de firma electrónica". La finalidad de dicho fichero es la servir a los usos relacionados con los servicios de certificación prestados por la Agencia de Tecnología y Certificación Electrónica. El suscriptor consiente expresamente la utilización de sus datos de carácter personal contenidos en dicho fichero, en la medida en que sea necesario para llevar a cabo las acciones previstas en la Política de Certificación.

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

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

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.