



Agencia de Tecnología y Certificación Electrónica

Política de Certificación de Certificados Cualificados de Sello Electrónico de Entidad en soporte software

Fecha: 02/06/2016	Versión: 2.0
Estado: APROBADO	Nº de páginas: 41
OID: 1.3.6.1.4.1.8149.3.22.2.0	Clasificación: PUBLICO
Archivo: ACCV-CP-22V2.0-c.doc	
Preparado por: Agencia de Tecnología y Certificación Electrónica - ACCV	

Tabla de Contenido

1 INTRODUCCIÓN.....	9
1.1 PRESENTACIÓN.....	9
1.2 IDENTIFICACIÓN.....	9
1.3 COMUNIDAD DE USUARIOS Y ÁMBITO DE APLICACIÓN.....	10
1.3.1 Autoridades de Certificación.....	10
1.3.2 Autoridades de Registro.....	10
1.3.3 Usuarios Finales.....	10
1.3.3.1 Suscriptores.....	10
1.3.3.2 Partes confiantes.....	10
1.4 USO DE LOS CERTIFICADOS.....	10
1.4.1 Usos Permitidos.....	10
1.4.2 Usos Prohibidos.....	11
1.5 POLÍTICA DE ADMINISTRACIÓN DE LA ACCV.....	11
1.5.1 Especificación de la Organización Administradora.....	11
1.5.2 Persona de Contacto.....	11
1.5.3 Competencia para determinar la adecuación de la CPS a la Políticas.....	11
1.6 DEFINICIONES Y ACRÓNIMOS.....	11
1.6.1 Definiciones.....	11
1.6.2 Acrónimos.....	11
2 PUBLICACIÓN DE INFORMACIÓN Y REPOSITORIO DE CERTIFICADOS.....	12
2.1 REPOSITORIO DE CERTIFICADOS.....	12
2.2 PUBLICACIÓN.....	12
2.3 FRECUENCIA DE ACTUALIZACIONES.....	12
2.4 CONTROLES DE ACCESO AL REPOSITORIO DE CERTIFICADOS.....	12
3 IDENTIFICACIÓN Y AUTENTICACIÓN.....	13
3.1 REGISTRO DE NOMBRES.....	13
3.1.1 Tipos de nombres.....	13
3.1.2 Significado de los nombres.....	13
3.1.3 Interpretación de formatos de nombres.....	13
3.1.4 Unicidad de los nombres.....	13
3.1.5 Resolución de conflictos relativos a nombres.....	13
3.1.6 Reconocimiento, autenticación y función de las marcas registradas.....	13
3.2 VALIDACIÓN INICIAL DE LA IDENTIDAD.....	13
3.2.1 Métodos de prueba de posesión de la clave privada.....	13
3.2.2 Autenticación de la identidad de una organización.....	13

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 2

3.2.3 Autenticación de la identidad de un individuo.....	14
3.3 IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE RENOVACIÓN DE LA CLAVE.....	14
3.3.1 Identificación y autenticación de las solicitudes de renovación rutinarias.....	14
3.3.2 Identificación y autenticación de las solicitudes de renovación de clave después de una revocación – Clave no comprometida.....	15
3.4 IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE REVOCACIÓN DE LA CLAVE.....	15
4 EL CICLO DE VIDA DE LOS CERTIFICADOS.....	16
4.1 SOLICITUD DE CERTIFICADOS.....	16
4.2 TRAMITACIÓN DE LA SOLICITUD DE CERTIFICADOS.....	16
4.3 EMISIÓN DE CERTIFICADOS.....	16
4.4 ACEPTACIÓN DE CERTIFICADOS.....	17
4.5 USO DEL PAR DE CLAVES Y DEL CERTIFICADO.....	17
4.6 RENOVACIÓN DE CERTIFICADOS.....	17
4.7 RENOVACIÓN DE CLAVES.....	17
4.8 MODIFICACIÓN DE CERTIFICADOS.....	17
4.9 REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS.....	17
4.9.1 Circunstancias para la revocación.....	17
4.9.2 Entidad que puede solicitar la revocación.....	17
4.9.3 Procedimiento de solicitud de revocación.....	17
4.9.3.1 Presencial.....	17
4.9.3.2 Telemático.....	17
4.9.4 Periodo de gracia de la solicitud de revocación.....	18
4.9.5 Circunstancias para la suspensión.....	18
4.9.6 Entidad que puede solicitar la suspensión.....	18
4.9.7 Procedimiento para la solicitud de suspensión.....	18
4.9.8 Límites del periodo de suspensión.....	18
4.9.9 Frecuencia de emisión de CRLs.....	18
4.9.10 Requisitos de comprobación de CRLs.....	18
4.9.11 Disponibilidad de comprobación on-line de revocación y estado.....	18
4.9.12 Requisitos de comprobación on-line de revocación.....	18
4.9.13 Otras formas de divulgación de información de revocación disponibles.....	18
4.9.14 Requisitos de comprobación para otras formas de divulgación de información de revocación.....	18
4.9.15 Requisitos especiales de renovación de claves comprometidas.....	18
4.10 SERVICIOS DE COMPROBACIÓN DE ESTADO DE CERTIFICADOS.....	18
4.11 FINALIZACIÓN DE LA SUSCRIPCIÓN.....	19
4.12 DEPÓSITO Y RECUPERACIÓN DE CLAVES.....	19
5 CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES.....	20

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 3

5.1	CONTROLES DE SEGURIDAD FÍSICA.....	20
5.1.1	<i>Ubicación y construcción.....</i>	20
5.1.2	<i>Acceso físico.....</i>	20
5.1.3	<i>Alimentación eléctrica y aire acondicionado.....</i>	20
5.1.4	<i>Exposición al agua.....</i>	20
5.1.5	<i>Protección y prevención de incendios.....</i>	20
5.1.6	<i>Sistema de almacenamiento.....</i>	20
5.1.7	<i>Eliminación de residuos.....</i>	20
5.1.8	<i>Backup remoto.....</i>	20
5.2	CONTROLES DE PROCEDIMIENTOS.....	20
5.2.1	<i>Papeles de confianza.....</i>	20
5.2.2	<i>Número de personas requeridas por tarea.....</i>	20
5.2.3	<i>Identificación y autenticación para cada papel.....</i>	20
5.3	CONTROLES DE SEGURIDAD DE PERSONAL.....	20
5.3.1	<i>Requerimientos de antecedentes, calificación, experiencia, y acreditación.....</i>	21
5.3.2	<i>Procedimientos de comprobación de antecedentes.....</i>	21
5.3.3	<i>Requerimientos de formación.....</i>	21
5.3.4	<i>Requerimientos y frecuencia de actualización de la formación.....</i>	21
5.3.5	<i>Frecuencia y secuencia de rotación de tareas.....</i>	21
5.3.6	<i>Sanciones por acciones no autorizadas.....</i>	21
5.3.7	<i>Requerimientos de contratación de personal.....</i>	21
5.3.8	<i>Documentación proporcionada al personal.....</i>	21
5.3.9	<i>Controles periódicos de cumplimiento.....</i>	21
5.3.10	<i>Finalización de los contratos.....</i>	21
5.4	PROCEDIMIENTOS DE CONTROL DE SEGURIDAD.....	21
5.4.1	<i>Tipos de eventos registrados.....</i>	21
5.4.2	<i>Frecuencia de procesado de logs.....</i>	21
5.4.3	<i>Periodo de retención para los logs de auditoría.....</i>	21
5.4.4	<i>Protección de los logs de auditoría.....</i>	21
5.4.5	<i>Procedimientos de backup de los logs de auditoría.....</i>	21
5.4.6	<i>Sistema de recogida de información de auditoría (interno vs externo).....</i>	22
5.4.7	<i>Notificación al sujeto causa del evento.....</i>	22
5.4.8	<i>Análisis de vulnerabilidades.....</i>	22
5.5	ARCHIVO DE INFORMACIONES Y REGISTROS.....	22
5.5.1	<i>Tipo de informaciones y eventos registrados.....</i>	22
5.5.2	<i>Periodo de retención para el archivo.....</i>	22
5.5.3	<i>Protección del archivo.....</i>	22
5.5.4	<i>Procedimientos de backup del archivo.....</i>	22

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 4



5.5.5	Requerimientos para el sellado de tiempo de los registros.....	22
5.5.6	Sistema de recogida de información de auditoría (interno vs externo).....	22
5.5.7	Procedimientos para obtener y verificar información archivada.....	22
5.6	CAMBIO DE CLAVE.....	22
5.7	RECUPERACIÓN EN CASO DE COMPROMISO DE UNA CLAVE O DE DESASTRE.....	22
5.7.1	Alteración de los recursos hardware, software y/o datos.....	22
5.7.2	La clave pública de una entidad se revoca.....	22
5.7.3	La clave de una entidad se compromete.....	22
5.7.4	Instalación de seguridad después de un desastre natural u otro tipo de desastre.....	23
5.8	CESE DE UNA CA.....	23
6	CONTROLES DE SEGURIDAD TÉCNICA.....	24
6.1	GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES.....	24
6.1.1	Generación del par de claves.....	24
6.1.2	Entrega de la clave privada a la entidad.....	24
6.1.3	Entrega de la clave pública al emisor del certificado.....	24
6.1.4	Entrega de la clave pública de la CA a los usuarios.....	24
6.1.5	Tamaño de las claves.....	24
6.1.6	Parámetros de generación de la clave pública.....	24
6.1.7	Comprobación de la calidad de los parámetros.....	25
6.1.8	Hardware/software de generación de claves.....	25
6.1.9	Fines del uso de la clave.....	25
6.2	PROTECCIÓN DE LA CLAVE PRIVADA.....	25
6.2.1	Estándares para los módulos criptográficos.....	25
6.2.2	Control multipersona de la clave privada.....	25
6.2.3	Custodia de la clave privada.....	26
6.2.4	Copia de seguridad de la clave privada.....	26
6.2.5	Archivo de la clave privada.....	26
6.2.6	Introducción de la clave privada en el módulo criptográfico.....	26
6.2.7	Método de activación de la clave privada.....	26
6.2.8	Método de desactivación de la clave privada.....	26
6.2.9	Método de destrucción de la clave privada.....	26
6.3	OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES.....	26
6.3.1	Archivo de la clave pública.....	26
6.3.2	Periodo de uso para las claves públicas y privadas.....	26
6.4	DATOS DE ACTIVACIÓN.....	26
6.4.1	Generación y activación de los datos de activación.....	26
6.4.2	Protección de los datos de activación.....	27

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 5

6.4.3 Otros aspectos de los datos de activación.....	27
6.5 CONTROLES DE SEGURIDAD INFORMÁTICA.....	27
6.6 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA.....	27
6.7 CONTROLES DE SEGURIDAD DE LA RED.....	27
6.8 CONTROLES DE INGENIERÍA DE LOS MÓDULOS CRIPTOGRÁFICOS.....	27
7 PERFILES DE CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS.....	28
7.1 PERFIL DE CERTIFICADO.....	28
7.1.1 Identificadores de objeto (OID) de los algoritmos.....	30
7.1.2 Formatos de nombres.....	30
7.1.3 Restricciones de los nombres.....	31
7.1.4 Identificador de objeto (OID) de la Política de Certificación.....	31
7.1.5 Uso de la extensión “Policy Constraints”.....	31
7.1.6 Sintaxis y semántica de los cualificadores de política.....	31
7.1.7 Tratamiento semántico para la extensión crítica “Certificate Policy”.....	31
7.2 PERFIL DE CRL.....	31
7.2.1 Número de versión.....	31
7.2.2 CRL y extensiones.....	31
7.3 LISTAS DE CERTIFICADOS REVOCADOS.....	31
7.3.1 Limite Temporal de los certificados en las CRLs.....	31
8 AUDITORÍA DE CONFORMIDAD.....	32
8.1 FRECUENCIA DE LOS CONTROLES DE CONFORMIDAD PARA CADA ENTIDAD.....	32
8.2 IDENTIFICACIÓN/CUALIFICACIÓN DEL AUDITOR.....	32
8.3 RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA.....	32
8.4 TÓPICOS CUBIERTOS POR EL CONTROL DE CONFORMIDAD.....	32
8.5 ACCIONES A TOMAR COMO RESULTADO DE UNA DEFICIENCIA.....	32
8.6 COMUNICACIÓN DE RESULTADOS.....	32
9 REQUISITOS COMERCIALES Y LEGALES.....	33
9.1 TARIFAS.....	33
9.1.1 Tarifas de emisión de certificado o renovación.....	33
9.1.2 Tarifas de acceso a los certificados.....	33
9.1.3 Tarifas de acceso a la información de estado o revocación.....	33
9.1.4 Tarifas de otros servicios como información de políticas.....	33
9.1.5 Política de reintegros.....	33
9.2 CAPACIDAD FINANCIERA.....	33
9.2.1 Indemnización a los terceros que confían en los certificados emitidos por la ACCV.....	33
9.2.2 Relaciones fiduciarias.....	33

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 6



9.2.3	Procesos administrativos.....	33
9.3	POLÍTICA DE CONFIDENCIALIDAD.....	33
9.3.1	Información confidencial.....	33
9.3.2	Información no confidencial.....	33
9.3.3	Divulgación de información de revocación /suspensión de certificados.....	34
9.4	PROTECCIÓN DE DATOS PERSONALES.....	34
9.4.1	Plan de Protección de Datos Personales.....	34
9.4.2	Información considerada privada.....	34
9.4.3	Información no considerada privada.....	34
9.4.4	Responsabilidades.....	34
9.4.5	Prestación del consentimiento en el uso de los datos personales.....	34
9.4.6	Comunicación de la información a autoridades administrativas y/o judiciales.....	34
9.4.7	Otros supuestos de divulgación de la información.....	34
9.5	DERECHOS DE PROPIEDAD INTELECTUAL.....	34
9.6	OBLIGACIONES Y RESPONSABILIDAD CIVIL.....	34
9.6.1	Obligaciones de la Entidad de Certificación.....	34
9.6.2	Obligaciones de la Autoridad de Registro.....	34
9.6.3	Obligaciones de los suscriptores.....	34
9.6.4	Obligaciones de los terceros confiantes en los certificados emitidos por la ACCV.....	35
9.6.5	Obligaciones del repositorio.....	35
9.7	RENUNCIAS DE GARANTÍAS.....	35
9.8	LIMITACIONES DE RESPONSABILIDAD.....	35
9.8.1	Garantías y limitaciones de garantías.....	35
9.8.2	Deslinde de responsabilidades.....	35
9.8.3	Limitaciones de pérdidas.....	35
9.9	PLAZO Y FINALIZACIÓN.....	35
9.9.1	Plazo.....	35
9.9.2	Finalización.....	35
9.9.3	Supervivencia.....	35
9.10	NOTIFICACIONES.....	35
9.11	MODIFICACIONES.....	35
9.11.1	Procedimientos de especificación de cambios.....	35
9.11.2	Procedimientos de publicación y notificación.....	36
9.11.3	Procedimientos de aprobación de la Declaración de Prácticas de Certificación.....	36
9.12	RESOLUCIÓN DE CONFLICTOS.....	36
9.12.1	Resolución extrajudicial de conflictos.....	36
9.12.2	Jurisdicción competente.....	36
9.13	LEGISLACIÓN APLICABLE.....	36

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 7

9.14 CONFORMIDAD CON LA LEY APLICABLE.....	36
9.15 CLÁUSULAS DIVERSAS.....	36
10 ANEXO I.....	37
11 ANEXO II – FORMULARIO DE SOLICITUD DE REVOCACIÓN DE CERTIFICADO.....	40

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 8

1 INTRODUCCIÓN

1.1 Presentación

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

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

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

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

1.2 Identificación

Nombre de la política	Política de Certificación de Certificados Cualificados de Sello Electrónico de Entidad en soporte software
Calificador de la política	Certificado Cualificado de Sello Electrónico de Entidad en soporte software expedido por la Agencia de Tecnología y Certificación Electrónica IVF (Pl. Napoles y Sicilia, 6. CIF Q9650010C). CPS y CP en http://www.accv.es
Versión de la política	2.0
Estado de la política	APROBADO
Referencia de la política / OID (Object Identifier)	1.3.6.1.4.1.8149.3.22.2.0
Fecha de emisión	2 de junio de 2016
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

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 9

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-110 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-110 es válido desde el día 13 de octubre de 2011 hasta el 1 de enero de 2027.

1.3.2 Autoridades de Registro

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

1.3.3 Usuarios Finales

1.3.3.1 Suscriptores

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

La custodia de los datos de creación de firma asociados a cada certificado de sello electrónico de entidad será responsabilidad de la persona física solicitante, cuya identificación se incluirá en el certificado electrónico.

El soporte de claves y certificados es software (disquete, disco duro, CDROM u otros medios de almacenamiento no criptográficos).

1.3.3.2 Partes confiantes

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

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

1.4 Uso de los certificados

1.4.1 Usos Permitidos

Los certificados emitidos por la Agencia de Tecnología y Certificación Electrónica bajo esta Política de Certificación, pueden utilizarse para la realización de sellos electrónicos y cifrado de cualquier información o documento. Asimismo, pueden utilizarse como mecanismo de identificación ante servicios y aplicaciones informáticas.

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 10

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	<i>Agencia de Tecnología y Certificación Electrónica IVF</i>
Dirección de email	<i>accv@accv.es</i>
Dirección	<i>Plaza Napoles y Sicilia , 6 –46003 Valencia (Spain)</i>
Número de teléfono	<i>+34 902 482 481</i>
Número de fax	<i>+34-961 971 771</i>

1.5.2 Persona de Contacto

Nombre	<i>Agencia de Tecnología y Certificación Electrónica IVF</i>
Dirección de email	<i>accv@accv.es</i>
Dirección	<i>Plaza Napoles y Sicilia , 6 –46003 Valencia (Spain)</i>
Número de teléfono	<i>+34 902 482 481</i>
Número de fax	<i>+34-961 971 771</i>

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

No estipulado

1.6.2 Acrónimos

No estipulado

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 11

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.

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 12

3 Identificación y Autenticación

3.1 Registro de nombres

3.1.1 Tipos de nombres

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

3.1.2 Significado de los nombres

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

3.1.3 Interpretación de formatos de nombres

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

3.1.4 Unicidad de los nombres

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

3.1.5 Resolución de conflictos relativos a nombres

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

3.1.6 Reconocimiento, autenticación y función de las marcas registradas.

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

3.2 Validación Inicial de la Identidad

3.2.1 Métodos de prueba de posesión de la clave privada.

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

3.2.2 Autenticación de la identidad de una organización.

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

- Para solicitar el certificado de sello electrónico de entidad para una Administración Pública (estatal, autonómica o local) deberá solicitarlo la persona responsable y con autoridad en la entidad a nivel de Director General, Gerente, Alcalde o Teniente Alcalde, Presidente o Vicepresidente de la Diputación, acompañado del Diario o Boletín Oficial donde conste la publicación de su nombramiento.
- Para solicitar certificado de Sello Electrónico de una sociedad mercantil o cualquier sociedad de inscripción obligatoria en el Registro Mercantil (Sociedad Anónima, Sociedad de Responsabilidad Limitada, Sociedad Laboral, Sociedad Deportiva, Sociedades Colectivas, Comanditarias o Cooperativas, Agrupaciones de Interés Económico, UTE, otras..), se deberá aportar certificado del Registro Mercantil relativo a la constitución, personalidad jurídica y nombramiento y vigencia del cargo de administrador o representante legal, expedido durante los 10 días anteriores a la fecha de presentación del certificado en la ACCV. Si no se aportara

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 13

se entiende que presta el consentimiento a la ACCV para la consulta en registro público donde consten inscritos los documentos de constitución y apoderamiento. Si la representación es voluntaria, se sustituirá el certificado de nombramiento y vigencia del cargo por el poder notarial bastante, con la cláusula especial para poder solicitar el Certificado de Persona Jurídica.

- Para solicitar un certificado de Sello Electrónico para Asociaciones, Fundaciones, Clubes, Partidos Políticos, Sindicatos o Cooperativas no inscribibles en el Registro Mercantil, se aportará certificado del registro público donde consten inscritas, relativo a la constitución, personalidad jurídica y nombramiento y vigencia del cargo de administrador o representante legal, expedido durante los 10 días anteriores a la fecha de presentación del certificado en la ACCV. Si la representación es voluntaria, se sustituirá el certificado de nombramiento y vigencia del cargo por el poder notarial bastante, con la cláusula especial para poder solicitar el Certificado de Persona Jurídica.
- Para solicitar un certificado de Sello Electrónico para Sociedades Civiles y Comunidades de Bienes, se aportará el Título Constitutivo de la Sociedad Civil o Estatutos, el NIF, el certificado del nombramiento del Presidente u órgano de administración y la manifestación responsable del Presidente (u órgano de administración) sobre la vigencia de su cargo, o bien poder notarial bastante con cláusula especial para la solicitud del certificado de sello electrónico, otorgado por el Presidente u órgano de administración al representante voluntario.

La ACCV guardará copia de la documentación presentada por el solicitante.

3.2.3 Autenticación de la identidad de un individuo.

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

Es necesario hacer notar que en este tipo de certificados se incluye la dirección de correo electrónico, bien de la entidad, bien del solicitante del certificado (custodio) como elemento necesario para soportar el protocolo S/MIME, pero que la Agencia de Tecnología y Certificación Electrónica no garantiza que esta dirección de correo esté vinculada con la entidad o el custodio del certificado, por lo que la confianza o no en que esta dirección sea la del titular del certificado corresponde únicamente a la parte confiante. La Agencia de Tecnología y Certificación Electrónica únicamente garantiza que la dirección de correo que consta en el certificado fue la aportada por el suscriptor en el momento de la formalización de su solicitud.

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

3.3.1 Identificación y autenticación de las solicitudes de renovación rutinarias.

La identificación y autenticación para la renovación del certificado se realizará utilizando las técnicas y procedimientos recogidos en el punto 3.2 *Validación Inicial de la Identidad*.

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 14

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

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

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

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

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

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

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 15

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

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

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

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

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

Asimismo, y de conformidad con lo establecido en el art. 13.4 b) de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica en el caso de la solicitud de certificado mediante medios telemáticos se exigirá que haya transcurrido un período de tiempo desde la identificación presencial menor a los cinco años.

4.2 Tramitación de la solicitud de certificados.

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

4.3 Emisión de certificados

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

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

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.

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 16

4.4 Aceptación de certificados

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

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

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.

Los certificados emitidos bajo la presente política no se renuevan, siendo necesaria realizar una nueva solicitud, tal y como se detalla en el punto 4.1.

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 Presencial

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

4.9.3.2 Telemático

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

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 17

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

Sólo 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

La autoridad judicial o administrativa competente.

4.9.7 Procedimiento para la solicitud de suspensión

Por Resolución de la autoridad judicial o administrativa competente.

4.9.8 Límites del período de suspensión

El límite será el que se establezca en la Resolución de la autoridad judicial o administrativa competente.

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

Además de la consulta de revocados por medio de Listas de Certificados Revocados (CRL) y por medio del servicio OCSP, es posible comprobar la validez de los certificados por medio de un formulario web que, a partir del nombre de la entidad (completo o parcial), devuelve los certificados vinculados que cumplan ese criterio y el estado de éstos. Este formulario se encuentra en el sitio web de la Agencia de Tecnología y Certificación Electrónica, en la URL <http://www.accv.es>

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.

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 18

4.11 Finalización de la suscripción.

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

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

4.12 Depósito y recuperación de claves.

La ACCV no realiza depósito de las claves asociadas a los certificados cualificados de entidad

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 19

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.

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 20

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 procesamiento 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.

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 21

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.

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 22

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.

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 23

6 Controles de seguridad técnica

6.1 Generación e Instalación del Par de Claves

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

6.1.1 Generación del par de claves

El par de claves para el certificado emitido bajo el ámbito de la presente Política de Certificación se pueden generar en dos ubicaciones; el equipo del usuario en un proceso de autogeneración sin salir nunca del mismo equipo, y alternativamente, en casos excepcionales, podrán generarse las claves en la aplicación ARCA, de gestión de certificados digitales.

6.1.2 Entrega de la clave privada a la entidad

La clave privada para los certificados emitidos bajo el ámbito de la presente Política de Certificación se encuentra en el equipo del usuario donde se generó el par de claves o, en caso de generación en la aplicación ARCA, se entregará al usuario y no se dejará copia ni rastro alguno en el Punto de Registro de Usuario.

6.1.3 Entrega de la clave pública al emisor del certificado

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

En el caso de que el par de claves sea generado en el PRU, se construirá igualmente una solicitud de certificado según el formato PKCS#10 para ser firmado por la CA.

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-110 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-110 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	Signature algorithm	Signature algorithm	Key generation algorithm	Padding method	Cryptographic hash function
-----------------------	---------------------	---------------------	--------------------------	----------------	-----------------------------

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 24

name		parameters			
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 el equipo del usuario o, alternativamente, en el sistema de gestión de certificados ARCA.

6.1.9 Fines del uso de la clave

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

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

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.

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 25

6.2.3 Custodia de la clave privada

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

6.2.4 Copia de seguridad de la clave privada

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

6.2.5 Archivo de la clave privada.

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

6.2.6 Introducción de la clave privada en el módulo criptográfico.

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

6.2.7 Método de activación de la clave privada.

En el caso de autogeneración de la clave por parte del usuario el mecanismo de activación lo impone el usuario en el momento de la generación. Si la clave privada se ha generado en la aplicación ARCA, la activación se realizará a través de la introducción de la palabra de paso de acceso a esta clave, contenida en el fichero PKCS#12.

6.2.8 Método de desactivación de la clave privada

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

6.2.9 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 cinco (5) años.

El par de claves utilizado para la emisión de los certificados se crea para cada emisión, y por tanto también tienen una validez de cinco (5) años.

El certificado de "ACCVCA-110" 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

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

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 26

Si la generación se efectúa en el PRU se proporcionará al suscriptor la palabra de paso de acceso a la clave privada o de protección del fichero que contiene el PKCS#12. Igualmente es responsabilidad y obligación del suscriptor la modificación de esa palabra de paso preconfigurada por una de su exclusivo conocimiento de forma inmediata a la recepción del fichero PKCS#12 y previa a su primer uso.

6.4.2 Protección de los datos de activación

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

6.4.3 Otros aspectos de los datos de activación

No 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.

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 27

7 Perfiles de certificados y listas de certificados revocados

7.1 Perfil de Certificado

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

Campo	Valor
Subject	
SerialNumber	NIF de la entidad o equivalente Opcionalmente se podrá utilizar la semántica propuesta por la norma ETSI EN319 412-1
GivenName	Nombre del representante , tal como aparece en el DNI
SurName	Apellidos del representante, tal como aparece en el DNI
1.3.6.1.4.1.18838.1.1	NIF del representante
OrganizationIdentifier 2.5.4.97	Identificador de la entidad utilizando la semántica propuesta por la norma ETSI EN319 412-1
Description (2.5.4.13)	Codificación del documento público que acredita los datos de la entidad (facultades del firmante o los datos registrales). Ver posibles descripciones en el apartado 7.1.2
CommonName	Nombre descriptivo de la entidad
OrganizationName	Razón social de la entidad, tal y como aparece en los documentos acreditativos.
Country	ES
Version	V3
SerialNumber	Identificador único del certificado. Menor de 32 caracteres hexadecimales.
Algoritmo de firma	sha256withRSAEncryption
Issuer (Emisor)	
CommonName	ACCVCA-110
OrganizationalUnit	PKIACCV
Organization	ACCV
Country	ES
Válido desde	Fecha de Emisión
Válido hasta	Fecha de Caducidad
Clave Pública	Octet String conteniendo la clave pública del suscriptor
Extended Key Usage	
	Client Authentication

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 28



	Email Protection	
CRL Distribution Point	HTTP URI: http://www.accv.es/fileadmin/Archivos/certificados/accvca110_der.crl	
SubjectAlternativeName		
RFC822Name	Correo electrónico del representante	
DirectoryName		
	CN=Nombre del representante Apellido1 del representante Apellido2 del representante	
	UID=NIF del representante	
Certificate Policy Extensions		
Policy OID	1.3.6.1.4.1.8149.3.22.2.0	Política de Certificación de Certificados Cualificados de Sello Electrónico de Entidad en Soporte Software
Policy CPS Location	http://www.accv.es/legislacion_c.htm	
Policy Notice	Certificado cualificado de Sello Electrónico de Entidad en soporte software expedido por la Agencia de Tecnología y Certificación Electrónica IVF (Pl. Napoles y Sicilia, 6. CIF Q9650010C). CPS y CP en http://www.accv.es	
Policy OID	QCP-1: certificate policy for EU qualified certificates issued to legal persons; itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal (1)	
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/ACCVCA110SHA2.cacert.crt	
Fingerprint issuer	67 7c df 63 b9 5e 9e ae ae 69 6f 44 50 67 18 fe 0d 2f 6e 41	
Algoritmo de hash	SHA-256	
KeyUsage (críticos)		
	Non Repudiation Digital Signature Key Encipherment Key Agreement	
QcStatement	Campos QC (Qualified Certificate)	

Cif: PUBLICO

Ref... ACCV-CP-22V2.0-c.doc

Versión: 1.0

Est: APROBADO

OID: 1.3.6.1.4.1.8149.3.22.2.0

Pág. 29

QcCompliance		El certificado es cualificado
QcType	eSeal	Tipo particular de certificado cualificado
QcRetentionPeriod	15y	Periodo de retención de la información material
QcPDS	http://www.accv.es/fileadmin/Archivos/Practicas_d_e_certificacion/ACCV-PDS-V1.0-EN.pdf	Ubicación de PKI Disclosure Statement

7.1.1 Identificadores de objeto (OID) de los algoritmos

Identificador de Objeto (OID) de los algoritmos Criptográficos:

- a) SHA1withRSA (1.2.840.113549.1.1.5)
- b) SHA256withRSA (1.2.840.113549.1.1.11)

7.1.2 Formatos de nombres

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

Subject name: serialNumber=*CIF*, givenName=*Nombre del representante*, surname=*Apellido1 del representante Apellido2 del representante*, 1.3.6.1.4.1.18838.1.1=NIF del representante, OrganizationIdentifier(2.5.4.97)=Identificador de la entidad utilizando la semántica propuesta por la norma ETSI EN319 412-1, cn=Nombre descriptivo de la entidad, o=Razón Social de la entidad tal y como aparece en los registros, c=ES

Issuer name: cn=ACCVCA-110, ou=PKIACCV o=ACCV, c=ES

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

- Registro mercantil o similar

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

- Documento notarial

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

- Boletín oficial

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

- Otros

Texto libre detallando la fuente de datos que acredita la representación

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

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 30

7.1.3 Restricciones de los nombres

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

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

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

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

1.3.6.1.4.1.8149.3.22.2.0

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

0.4.0.194112.1.1

**Política de certificación para certificados cualificados EU
emitidos a entidades**

7.1.5 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.

7.1.6 Sintaxis y semántica de los cualificadores de política

No estipulado

7.1.7 Tratamiento semántico para la extensión crítica “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.

7.37.3 Listas de Certificados Revocados

7.3.17.3.1 Limite 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,

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 31

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.

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 32

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

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

9.2 Capacidad financiera

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

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.

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 33

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.

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 34

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

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

9.6.5 Obligaciones del repositorio

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

9.7 Renuncias de garantías

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

9.8 Limitaciones de responsabilidad

9.8.1 Garantías y limitaciones de garantías

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

9.8.2 Deslinde de responsabilidades

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

9.8.3 Limitaciones de pérdidas

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

9.9 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, irán firmados para garantizar su autenticidad, integridad y confidencialidad.

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.

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 35

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.

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 36

10 Anexo I

CONTRATO DE CERTIFICACIÓN – CÓDIGO 1.3.6.1.4.1.8149.3.22

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

Nom de l'Entitat/Nombre de la Entidad:

CIF de l'Entitat/CIFde la Entidad:

Raó Social/Razón Social:

Secció 2 – Dades del sol.licitant / Sección 2 – Datos del solicitante

Cognoms/Apellidos:

Nom/Nombre:

DNI/NIF:

Tel.:

Adreça de correu electrònic/Dirección correo electrónico:

Adreça postal/Dirección postal:

PIN :

Tel. suport/ tel. soporte **902 482 481**

www.accv.es

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

Nom i cognoms/Nombre y Apellidos:

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

Subscribo el present contracte de certificació associat a la Política de Certificació de Certificats Qualificats de Segell Electrònic d'Entitat suport software amb codi 1.3.6.1.4.1.8149.3.22, emés per la Agencia de Tecnología y Certificación Electrónica. Declare que conec i accepto les normes d'utilització d'este tipus de certificats que es troben exposades en <http://www.accv.es>. Declare, així mateix, que les dades posades de manifest són certes.

Suscribo el presente contrato de certificación asociado a la Política de Certificación de Certificados Cualificados de Sello Electrónico de Entidad en soporte software con código 1.3.6.1.4.1.8149.3.22, emitido por la la Agencia de Tecnología y Certificación Electrónica. Declaro conocer y aceptar las normas de utilización de este tipo de certificados que se encuentran expuestas en <http://www.accv.es>. Declaro, asimismo, que los datos puestos de manifiesto son ciertos.

Firma del sol.licitant

Firma i segell del Punt de Registre

Firma del solicitante

Firma y sello del Punto de Registro

Firmat/Firmado:

Firmat/Firmado:

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

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 37

CONTRATO DE CERTIFICACIÓN – CÓDIGO 1.3.6.1.4.1.8149.3.22
Condiciones de utilización de los certificados

1. Los certificados asociados a la Política de Certificación de Certificados Cualificados de Sello Electrónico de Entidad en soporte software, emitidos por la la Agencia de Tecnología y Certificación Electrónica son del tipo X.509v3 y se rigen por la Declaración de Prácticas de Certificación 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. Los solicitantes deberán ser personas físicas, en posesión de un NIF, un NIE u otro documento de identificación válido en Derecho, con poder bastante para representar a la Entidad que suscribe el certificado.
3. El solicitante es responsable de la veracidad de los datos aportados en todo momento a lo largo del proceso de solicitud y registro. Será responsable de comunicar cualquier variación de los datos aportados para la obtención del certificado.
4. La persona física solicitante del certificado es responsable de la custodia de la clave privada y de comunicar a la mayor brevedad posible cualquier pérdida o sustracción de esta clave.
5. La persona física solicitante del certificado es responsable de limitar el uso del certificado a lo dispuesto en la Política de Certificación asociada, que es un documento público y que se encuentra disponible en <http://www.accv.es>. En especial, este certificado de Entidad podrá ser utilizado cuando se admita en las relaciones entre la Entidad y las Administraciones Públicas o en la contratación de bienes o servicios que sean propios o concernientes a su giro o tráfico ordinario.
6. La Agencia de Tecnología y Certificación Electrónica no se responsabiliza del contenido de los documentos firmados haciendo uso de los certificados por ella emitidos.
7. La Agencia de Tecnología y Certificación Electrónica es responsable del cumplimiento de las legislaciones Europea, Española y Valenciana, por lo que a Firma Electrónica se refiere. Es, asimismo, responsable del cumplimiento de lo dispuesto en la Declaración de Prácticas de Certificación de la ACCV y en la Política de Certificación asociada a este tipo de certificados.
8. El periodo de validez de estos certificados es de cinco (5) años. Para su renovación deberán seguirse el mismo procedimiento que para la primera solicitud o bien los procedimientos previstos en la Política de Certificación asociada.
9. Los certificados emitidos perderán su eficacia, además de al vencimiento del periodo de validez, cuando se produzca una revocación, cuando se inutilice el soporte del certificado, ante resolución judicial o administrativa que ordene la pérdida de eficacia, por inexactitudes graves en los datos aportados por el solicitante, por extinción o disolución de la personalidad jurídica de la Entidad, por alteración de las condiciones de custodia del certificado. Otras condiciones para la pérdida de eficacia se recogen en la Declaración de Prácticas de Certificación y en la Política de Certificación asociada a este tipo de certificados.
10. La documentación a aportar para la identificación de la persona física solicitante del certificado será el Documento Nacional de Identidad, NIE o Pasaporte válido y vigente. El solicitante deberá aportar los datos relativos a la constitución de la entidad y la extensión y facultades de representación del solicitante.
11. El 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. La finalidad de dicho fichero es la servir a los usos relacionados con los servicios de certificación prestados por la 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 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 la Agencia de Tecnología y Certificación Electrónica, a través de cualquiera de los Registros de Entrada de la Generalitat e indicando claramente esta voluntad.
14. Se aconseja al usuario realizar el cambio del PIN inicial que aparece en el presente contrato a través de las herramientas que pone a su disposición la la Agencia de Tecnología y Certificación Electrónica.
15. 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.

Ejemplar para el solicitante – Reverso

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 38

11 Anexo II – Formulario de solicitud de revocación de certificado

SOLICITUD DE REVOCACIÓN DE CERTIFICAT SOLICITUD DE REVOCACIÓN DE CERTIFICADO		V3.0
Fecha:.....		
Secció 1 – Dades del subscriptor / Sección 1 – Datos del suscriptor		
Nom de l'Entitat/ <i>Nombre de la Entidad</i> :		
CIF de l'Entitat/ <i>CIF de la Entidad</i> :		
Raó Social/ <i>Razón Social</i> :		
Secció 2 – Dades del sol.licitant / Sección 2 – Datos del solicitante		
Cognoms/ <i>Apellidos</i> :		
Nom/ <i>Nombre</i> :		
DNI/NIF:	Tel.:	
Secció 2 – Identificació del certificat* / Sección 2 – Identificación del certificado*		
Certificado personal:	Nº de petición del certificado:	
Secció 3 - Motiu de la revocació* / Sección 3 – Motivo de la revocación*		
<p>* La simple voluntad de revocación del suscriptor o del solicitante del certificado es un motivo válido para la solicitud de la misma.</p>		
Secció 4 – Autorització* / Sección 2 – Autorización*		
Subscriptor del certificat <i>Subscriptor del certificado</i>		
<i>Firma</i>		
Solicitat al operador del Punt de Registre d'Usuari / Solicitado al operador de Punto de Registro de Usuario:		
Firma:		

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

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 40

SOLICITUD DE REVOCACIÓ DE CERTIFICAT
SOLICITUD DE REVOCACIÓN DE CERTIFICADO

V3.0

Fecha:.....

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

Nom de l'Entitat/*Nombre de la Entidad*:

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

Raó Social/*Razón Social*:

Secció 2 – Dades del sol.licitant / Sección 2 – Datos del solicitante

Cognoms/*Apellidos*:

Nom/*Nombre*:

DNI/NIF:

Tel.:

Secció 2 – Identificació del certificat* / Sección 2 – Identificación del certificado*

Certificado personal:

Nº de petición del certificado:

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

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

Secció 4 – Autorització* / Sección 2 – Autorización*

Subscriptor del certificat

Subscriptor del certificado

Firma

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

Firma:

Exemplar per al sol·licitant / *Ejemplar para el solicitante*

Cif: PUBLICO	Ref... ACCV-CP-22V2.0-c.doc	Versión: 1.0
Est: APROBADO	OID: 1.3.6.1.4.1.8149.3.22.2.0	Pág. 41