



# Autoritat de Certificació de la Comunitat Valenciana

## Política de Certificación de Certificados de Controlador de Dominio

<b>Fecha:</b> 12/06/2006	<b>Versión:</b> 1.0
<b>Estado:</b> APROBADO	<b>Nº de páginas:</b> 32
<b>OID:</b> 1.3.6.1.4.1.8149.3.12.1.0	<b>Clasificación:</b> PUBLICO
<b>Archivo:</b> ACCV-CP-12V1.0-c.doc	
<b>Preparado por:</b> ACCV	



**Secretaria Autònoma de Telecomunicacions i  
Societat de la Informació  
Conselleria d'Infraestructures i Transport**



## Tabla de Contenido

<b>1. INTRODUCCIÓN</b> .....	<b>8</b>
1.1. PRESENTACIÓN.....	8
1.2. IDENTIFICACIÓN.....	8
1.3. COMUNIDAD DE USUARIOS Y ÁMBITO DE APLICACIÓN.....	9
1.3.1. <i>Autoridades de Certificación</i> .....	9
1.3.2. <i>Autoridades de Registro</i> .....	9
1.3.3. <i>Usuarios Finales</i> .....	9
1.3.3.1. Suscriptores.....	9
1.3.3.2. Partes confiantes.....	9
1.4. USO DE LOS CERTIFICADOS.....	9
1.4.1. <i>Usos Permitidos</i> .....	9
1.4.2. <i>Usos prohibidos</i> .....	9
1.5. POLÍTICA DE ADMINISTRACIÓN DE LA ACCV.....	10
1.5.1. <i>Especificación de la Organización Administradora</i> .....	10
1.5.2. <i>Persona de Contacto</i> .....	10
1.5.3. <i>Competencia para determinar la adecuación de la CPS a la Políticas</i> .....	10
1.6. DEFINICIONES Y ACRÓNIMOS.....	10
1.6.1. <i>Definiciones</i> .....	10
1.6.2. <i>Acrónimos</i> .....	10
<b>2. PUBLICACIÓN DE INFORMACIÓN Y REPOSITORIO DE CERTIFICADOS</b> .....	<b>11</b>
2.1. REPOSITORIO DE CERTIFICADOS.....	11
2.2. PUBLICACIÓN.....	11
2.3. FRECUENCIA DE ACTUALIZACIONES.....	11
2.4. CONTROLES DE ACCESO AL REPOSITORIO DE CERTIFICADOS.....	11
<b>3. IDENTIFICACIÓN Y AUTENTICACIÓN</b> .....	<b>12</b>
3.1. REGISTRO DE NOMBRES.....	12
3.1.1. <i>Tipos de nombres</i> .....	12
3.1.2. <i>Significado de los nombres</i> .....	12
3.1.3. <i>Interpretación de formatos de nombres</i> .....	12
3.1.4. <i>Unicidad de los nombres</i> .....	12
3.1.5. <i>Resolución de conflictos relativos a nombres</i> .....	12
3.1.6. <i>Reconocimiento, autenticación y función de las marcas registradas</i> .....	12
3.2. VALIDACIÓN INICIAL DE LA IDENTIDAD.....	12
3.2.1. <i>Métodos de prueba de posesión de la clave privada</i> .....	12
3.2.2. <i>Autenticación de la identidad de una organización</i> .....	12
3.2.3. <i>Autenticación de la identidad de un individuo</i> .....	12



3.3.	IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE RENOVACIÓN DE LA CLAVE.....	13
3.3.1.	<i>Identificación y autenticación de las solicitudes de renovación rutinarias.....</i>	<i>13</i>
3.3.2.	<i>Identificación y autenticación de las solicitudes de renovación de clave después de una revocación – Clave no comprometida.....</i>	<i>13</i>
3.4.	IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE REVOCACIÓN DE LA CLAVE.....	13
<b>4.</b>	<b>EL CICLO DE VIDA DE LOS CERTIFICADOS.....</b>	<b>14</b>
4.1.	SOLICITUD DE CERTIFICADOS.....	14
4.2.	TRAMITACIÓN DE LA SOLICITUD DE CERTIFICADOS.....	14
4.3.	EMISIÓN DE CERTIFICADOS.....	14
4.4.	ACEPTACIÓN DE CERTIFICADOS.....	14
4.5.	USO DEL PAR DE CLAVES Y DEL CERTIFICADO.....	14
4.6.	RENOVACIÓN DE CERTIFICADOS.....	15
4.7.	RENOVACIÓN DE CLAVES.....	15
4.8.	MODIFICACIÓN DE CERTIFICADOS.....	15
4.9.	REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS.....	15
4.9.1.	<i>Circunstancias para la revocación.....</i>	<i>15</i>
4.9.2.	<i>Entidad que puede solicitar la revocación.....</i>	<i>15</i>
4.9.3.	<i>Procedimiento de solicitud de revocación.....</i>	<i>15</i>
4.9.4.	<i>Periodo de gracia de la solicitud de revocación.....</i>	<i>15</i>
4.9.5.	<i>Circunstancias para la suspensión.....</i>	<i>15</i>
4.9.6.	<i>Entidad que puede solicitar la suspensión.....</i>	<i>15</i>
4.9.7.	<i>Procedimiento para la solicitud de suspensión.....</i>	<i>15</i>
4.9.8.	<i>Límites del período de suspensión.....</i>	<i>15</i>
4.9.9.	<i>Frecuencia de emisión de CRLs.....</i>	<i>16</i>
4.9.10.	<i>Requisitos de comprobación de CRLs.....</i>	<i>16</i>
4.9.11.	<i>Disponibilidad de comprobación on-line de revocación y estado.....</i>	<i>16</i>
4.9.12.	<i>Requisitos de comprobación on-line de revocación.....</i>	<i>16</i>
4.9.13.	<i>Otras formas de divulgación de información de revocación disponibles.....</i>	<i>16</i>
4.9.14.	<i>Requisitos de comprobación para otras formas de divulgación de información de revocación... ..</i>	<i>16</i>
4.9.15.	<i>Requisitos especiales de renovación de claves comprometidas.....</i>	<i>16</i>
4.10.	SERVICIOS DE COMPROBACIÓN DE ESTADO DE CERTIFICADOS.....	16
4.11.	FINALIZACIÓN DE LA SUSCRIPCIÓN.....	16
4.12.	DEPÓSITO Y RECUPERACIÓN DE CLAVES.....	16
<b>5.</b>	<b>CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES.....</b>	<b>17</b>
5.1.	CONTROLES DE SEGURIDAD FÍSICA.....	17
5.1.1.	<i>Ubicación y construcción.....</i>	<i>17</i>
5.1.2.	<i>Acceso físico.....</i>	<i>17</i>
5.1.3.	<i>Alimentación eléctrica y aire acondicionado.....</i>	<i>17</i>



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 .....	18
5.3.1.	Requerimientos de antecedentes, calificación, experiencia, y acreditación.....	18
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.....	19
5.4.5.	Procedimientos de backup de los logs de auditoría .....	19
5.4.6.	Sistema de recogida de información de auditoría (interno vs externo).....	19
5.4.7.	Notificación al sujeto causa del evento .....	19
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.....	20
5.7.1.	Alteración de los recursos hardware, software y/o datos.....	20



5.7.2.	<i>La clave pública de una entidad se revoca</i> .....	20
5.7.3.	<i>La clave de una entidad se compromete</i> .....	20
5.7.4.	<i>Instalación de seguridad después de un desastre natural u otro tipo de desastre</i> .....	20
5.8.	CESE DE UNA CA.....	20
<b>6.</b>	<b>CONTROLES DE SEGURIDAD TÉCNICA</b> .....	<b>21</b>
6.1.	GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES .....	21
6.1.1.	<i>Generación del par de claves</i> .....	21
6.1.2.	<i>Entrega de la clave privada a la entidad</i> .....	21
6.1.3.	<i>Entrega de la clave pública al emisor del certificado</i> .....	21
6.1.4.	<i>Entrega de la clave pública de la CA a los usuarios</i> .....	21
6.1.5.	<i>Tamaño de las claves</i> .....	21
6.1.6.	<i>Parámetros de generación de la clave pública</i> .....	21
6.1.7.	<i>Comprobación de la calidad de los parámetros</i> .....	22
6.1.8.	<i>Hardware/software de generación de claves</i> .....	22
6.1.9.	<i>Fines del uso de la clave</i> .....	22
6.2.	PROTECCIÓN DE LA CLAVE PRIVADA .....	22
6.2.1.	<i>Estándares para los módulos criptográficos</i> .....	22
6.2.2.	<i>Control multipersona de la clave privada</i> .....	22
6.2.3.	<i>Custodia de la clave privada</i> .....	22
6.2.4.	<i>Copia de seguridad de la clave privada</i> .....	22
6.2.5.	<i>Archivo de la clave privada</i> .....	23
6.2.6.	<i>Introducción de la clave privada en el módulo criptográfico</i> .....	23
6.2.7.	<i>Método de activación de la clave privada</i> .....	23
6.2.8.	<i>Método de desactivación de la clave privada</i> .....	23
6.2.9.	<i>Método de destrucción de la clave privada</i> .....	23
6.3.	OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES .....	23
6.3.1.	<i>Archivo de la clave pública</i> .....	23
6.3.2.	<i>Periodo de uso para las claves públicas y privadas</i> .....	23
6.4.	DATOS DE ACTIVACIÓN .....	23
6.4.1.	<i>Generación y activación de los datos de activación</i> .....	23
6.4.2.	<i>Protección de los datos de activación</i> .....	23
6.4.3.	<i>Otros aspectos de los datos de activación</i> .....	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
<b>7.</b>	<b>PERFILES DE CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS</b> .....	<b>25</b>
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.....	26
7.1.4.	Formatos de nombres.....	26
7.1.5.	Restricciones de los nombres.....	26
7.1.6.	Identificador de objeto (OID) de la Política de Certificación.....	26
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 crítica “Certificate Policy”.....	27
7.2.	PERFIL DE CRL.....	27
7.2.1.	Número de versión.....	27
7.2.2.	CRL y extensiones.....	27
7.3	LISTAS DE CERTIFICADOS REVOCADOS.....	27
7.3.1	Limite Temporal de los certificados en las CRLs.....	27
<b>8.</b>	<b>AUDITORÍA DE CONFORMIDAD.....</b>	<b>28</b>
8.1.	FRECUENCIA DE LOS CONTROLES DE CONFORMIDAD PARA CADA ENTIDAD.....	28
8.2.	IDENTIFICACIÓN/CUALIFICACIÓN DEL AUDITOR.....	28
8.3.	RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA.....	28
8.4.	TÓPICOS CUBIERTOS POR EL CONTROL DE CONFORMIDAD.....	28
8.5.	ACCIONES A TOMAR COMO RESULTADO DE UNA DEFICIENCIA.....	28
8.6.	COMUNICACIÓN DE RESULTADOS.....	28
<b>9.</b>	<b>REQUISITOS COMERCIALES Y LEGALES.....</b>	<b>29</b>
9.1.	TARIFAS.....	29
9.1.1.	Tarifas de emisión de certificado o renovación.....	29
9.1.2.	Tarifas de acceso a los certificados.....	29
9.1.3.	Tarifas de acceso a la información de estado o revocación.....	29
9.1.4.	Tarifas de otros servicios como información de políticas.....	29
9.1.5.	Política de reintegros.....	29
9.2.	CAPACIDAD FINANCIERA.....	29
9.2.1.	Indemnización a los terceros que confían en los certificados emitidos por la ACCV.....	29
9.2.2.	Relaciones fiduciarias.....	29
9.2.3.	Procesos administrativos.....	29
9.3.	POLÍTICA DE CONFIDENCIALIDAD.....	29
9.3.1.	Información confidencial.....	29
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.....	30
9.4.1.	Plan de Protección de Datos Personales.....	30



9.4.2.	<i>Información considerada privada.</i>	30
9.4.3.	<i>Información no considerada privada.</i>	30
9.4.4.	<i>Responsabilidades.</i>	30
9.4.5.	<i>Prestación del consentimiento en el uso de los datos personales.</i>	30
9.4.6.	<i>Comunicación de la información a autoridades administrativas y/o judiciales.</i>	30
9.4.7.	<i>Otros supuestos de divulgación de la información.</i>	30
9.5.	DERECHOS DE PROPIEDAD INTELECTUAL	30
9.6.	OBLIGACIONES Y RESPONSABILIDAD CIVIL	30
9.6.1.	<i>Obligaciones de la Entidad de Certificación.</i>	30
9.6.2.	<i>Obligaciones de la Autoridad de Registro.</i>	31
9.6.3.	<i>Obligaciones de los suscriptores.</i>	31
9.6.4.	<i>Obligaciones de los terceros confiantes en los certificados emitidos por la ACCV.</i>	31
9.6.5.	<i>Obligaciones del repositorio.</i>	31
9.7.	RENUNCIAS DE GARANTÍAS	31
9.8.	LIMITACIONES DE RESPONSABILIDAD	31
9.8.1.	<i>Garantías y limitaciones de garantías.</i>	31
9.8.2.	<i>Deslinde de responsabilidades.</i>	31
9.8.3.	<i>Limitaciones de pérdidas.</i>	31
9.9.	PLAZO Y FINALIZACIÓN.	31
9.9.1.	<i>Plazo.</i>	31
9.9.2.	<i>Finalización.</i>	31
9.9.3.	<i>Supervivencia.</i>	31
9.10.	NOTIFICACIONES.	31
9.11.	MODIFICACIONES.	32
9.11.1.	<i>Procedimientos de especificación de cambios.</i>	32
9.11.2.	<i>Procedimientos de publicación y notificación.</i>	32
9.11.3.	<i>Procedimientos de aprobación de la Declaración de Prácticas de Certificación.</i>	32
9.12.	RESOLUCIÓN DE CONFLICTOS.	32
9.12.1.	<i>Resolución extrajudicial de conflictos.</i>	32
9.12.2.	<i>Jurisdicción competente.</i>	32
9.13.	LEGISLACIÓN APLICABLE	32
9.14.	CONFORMIDAD CON LA LEY APLICABLE.	32
9.15.	CLÁUSULAS DIVERSAS.	32

# 1. INTRODUCCIÓN

## 1.1. Presentación

La Generalitat se constituyó en *Prestador de Servicios de Certificación o Autoridad de Certificación* en virtud de lo dispuesto en el Decreto 87/2002, de 30 de mayo, del Gobierno Valenciano, por el que se regula la utilización de la firma electrónica avanzada en la Generalitat Valenciana.

El presente documento es la Política de Certificación asociada a los certificados emitidos para sistemas controladores de dominio en sistemas operativos windows, 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 Autoridad de Certificación de la Comunidad Valenciana 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 Autoridad de Certificación de la Comunidad Valenciana.

La Política de Certificación referida en este documento se utilizará para la emisión de certificados para habilitar a los sistemas controladores de dominio la aceptación de los certificados de inicio de sesión en windows por usuarios de sistemas operativos Windows. Los certificados que se emiten bajo la presente Política son certificados electrónicos, que no tienen el carácter de certificados reconocidos, pero que van firmados por la Autoridad de Certificación de la Comunitat Valenciana y que vinculan unos datos de verificación de firma a un firmante y confirma su identidad.

La presente Declaración de Políticas 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 de Controladores de Dominio en Sistemas Operativos Windows.
Calificador de la política	Certificado no reconocido de Controlador de Dominio en sistemas operativos windows expedido por la Autoridad de Certificación de la Comunidad Valenciana (Pl. Manises 1. CIF S4611001A). CPS y CP en <a href="http://www.accv.es">http://www.accv.es</a>
Versión de la política	1.0
Estado de la política	APROBADO
Referencia de la política / OID (Object Identifier)	1.3.6.1.4.1.8149.3.12.1.0
Fecha de emisión	12 de junio de 2006
Fecha de expiración	No aplicable.
CPS relacionada	Declaración de Prácticas de Certificación (CPS) de la ACCV. Versión 1.7. OID: 1.3.6.1.4.1.8149.2.1.7 Disponible en <a href="http://www.accv.es/pdf-politicas">http://www.accv.es/pdf-politicas</a>
Localización	Esta Política de Certificación se puede encontrar en: <a href="http://www.accv.es/pdf-politicas">http://www.accv.es/pdf-politicas</a>



## 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 ACCV-CA3 perteneciente a la Autoridad de Certificación de la Comunidad Valenciana, cuya función es la emisión de certificados de entidad final de Controlador de Dominio en sistemas operativos Windows para los suscriptores de ACCV. El certificado de ACCV-CA3 es válido desde el día 17 de junio de 2006 hasta el 14 de junio de 2016

### 1.3.2. Autoridades de Registro

Las Autoridad de Registro para los certificados emitidos bajo la presente política es la propia ACCV, delegando su operación en los Administradores de Dominio para sus respectivos dominios.

### 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 Dominio de los respectivos dominios que sean titulares de un certificado reconocido en dispositivo seguro de creación de firma para ciudadanos expedido por la ACCV, válido y en vigor.

El soporte de claves y certificados es software (se almacenan en el disco duro de los correspondientes controladores de dominio)

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

#### 1.3.3.2. Partes confiantes

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

- Los usuarios de dominios en sistemas operativos windows
- Los responsables de los entornos de red windows.
- Los servicios y aplicaciones que quieran hacer uso de este tipo de certificados para identificar a los controladores de dominio de su organización.

## 1.4. Uso de los certificados

### 1.4.1. Usos Permitidos

Los certificados emitidos por la Autoridad de Certificación de la Comunidad Valenciana bajo esta Política de Certificación se utilizará para garantizar la confianza de los controladores de dominio en los certificados de inicio de sesión emitidos por la Autoridad de Certificación firmante (ACCV-CA2) y permitir el inicio de sesión en sistemas operativos windows con dichos certificados. Quedan al arbitrio de los responsables de las aplicaciones informáticas la utilización de este tipo de certificados para otros usos distintos, además de éste.

### 1.4.2. Usos prohibidos

No estipulado.

Clf.: <b>PUBLICO</b>	Ref.: ACCV-CP-12V1.0-c.doc	Versión: 1.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.12.1.0	Pág. 9



## 1.5. Política de Administración de la ACCV

### 1.5.1. Especificación de la Organización Administradora

Nombre	<i>Secretaria Autònica de Telecomunicacions i Societat de la Informació Conselleria d'Infraestructures i Transport</i>
Dirección de email	<i>satsi@gva.es</i>
Dirección	<i>C/ Colón, 66 –46004 Valencia (Spain)</i>
Número de teléfono	<i>+34-961 961 130</i>
Número de fax	<i>+34-961 961 001</i>

### 1.5.2. Persona de Contacto

Nombre	<i>Secretària Autònica de Telecomunicacions i Societat de la Informació Conselleria d'Infraestructures i Transport</i>
Dirección de email	<i>accv@accv.es</i>
Dirección	<i>C/ Colón, 66 – 46004 Valencia (Spain)</i>
Número de teléfono	<i>+34-902 482 481</i>
Número de fax	<i>+34- 961 961 001</i>

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

La Secretaria Autonómica de Telecomunicaciones y Sociedad de la Información de la Conselleria de Infraestructuras y Transporte de la Generalitat es el Órgano competente para determinar la adecuación de esta Política de Certificación a la Declaración de Prácticas de Certificación (CPS) de la ACCV, de conformidad con lo dispuesto en el Decreto 87/2002, de 30 de mayo, del Gobierno Valenciano, por el que se regula la utilización de la firma electrónica avanzada en la Generalitat Valenciana, y en el Decreto 114/2003, de 11 de junio, por el que se aprueba el Reglamento Orgánico y Funcional de la Conselleria de Infraestructuras y Transporte.

## 1.6. Definiciones y Acrónimos

### 1.6.1. Definiciones

No estipulado

### 1.6.2. Acrónimos

No estipulado



## 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.: <b>PUBLICO</b>	Ref.: ACCV-CP-12V1.0-c.doc	Versión: 1.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.12.1.0	Pág. 11



## 3. Identificación y Autenticación

### 3.1. Registro de nombres

#### 3.1.1. Tipos de nombres

Todos los suscriptores de certificados requieren un nombre *distintivo* (distinguished name) conforme con el estándar X.500.

En el *distinguished name* se incluye el campo common name, que se corresponde con el nombre cualificado (FQDN) utilizado por el controlador de dominio en el dominio de windows correspondiente.

#### 3.1.2. Significado de los nombres

El nombre que aparece en el certificado esta compuesto por el nombre cualificado (FQDN) dentro del dominio de windows al que pertenece.

#### 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

El formato de los nombres esta definido por el nombre del controlador de dominio en ese dominio de windows junto con el dominio, separados por el carácter '.'. Este nombre es unico dentro de un determinado dominio.

#### 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 autenticación de la identidad del solicitante de un certificado se realizará identificandose la persona autorizada (usualmente el Administrador de Dominio) frente a la aplicación de gestión de certificados de inicio de sesión en Windows y de Controlador de Dominio mediante su certificado reconocido en dispositivo seguro de creación de firma, válido y en vigor, que garantiza de manera

Clf.: <b>PUBLICO</b>	Ref.: ACCV-CP-12V1.0-c.doc	Versión: 1.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.12.1.0	Pág. 12



fiable e inequívoca su identidad. El Administrador de Dominio podrá delegar esta tarea, teniendo que informar a la ACCV de los datos de los usuarios que efectuaran esta labor. La ACCV, previamente, habrá introducido en el sistema de autorización la vinculación entre los usuarios y los dominios sobre los que tienen potestad.

### 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.

Para la identificación y autenticación para la renovación del certificado se utilizarán 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)

#### 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

Debido a la vinculación directa entre el certificado de Controlador de Dominio y el acceso a los servicios de información por parte de los usuarios, de forma que la revocación del primero inhabilita el segundo, la revocación de este tipo de certificados queda en manos del Administrador del Dominio o de los usuarios en los que el delegue. La identificación del Administrador del Dominio se efectuará tal y como se contempla en el punto 3.2.3 *Autenticación de la identidad de un individuo*, de esta Política de Certificación.

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

Clf.: <b>PUBLICO</b>	Ref.: ACCV-CP-12V1.0-c.doc	Versión: 1.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.12.1.0	Pág. 13



## 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

Para efectuar una solicitud de certificado emitido bajo la presente política, el responsable por parte de la organización que posea el dominio en el que se encuentra el controlador se identificara frente a la aplicación de gestión de certificados de inicio de sesión en Windows y de Controlador de Dominio mediante su certificado reconocido en dispositivo seguro de creación de firma, válido y en vigor, que garantiza de manera fiable e inequívoca su identidad.

Una vez autorizado, podrá solicitar los certificados para los Controladores de Dominio en los dominios en los que dicha autorización se lo permita.

### 4.2. Tramitación de la solicitud de certificados.

Compete a la Autoridad o Entidad de Registro la comprobación de la identidad del solicitante y la corrección formal de los datos introducidos. 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 la Autoridad de Registro para esta Política de Certificación 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.

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

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

### 4.4. Aceptación de certificados

La aceptación de los certificados por parte de los solicitantes se produce en el momento de la recogida del certificado. La aplicación de gestión de certificados de inicio de sesión en Windows y de Controlador de Dominio proporcionara los mecanismos correspondientes para la grabación de los mismos.

### 4.5. Uso del par de claves y del certificado.

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

Clf.: <b>PUBLICO</b>	Ref.: ACCV-CP-12V1.0-c.doc	Versión: 1.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.12.1.0	Pág. 14



## 4.6. Renovación de certificados.

Para la renovación de los certificados emitidos bajo la presente política se efectuarán los mismos pasos descritos en los puntos 4.1, 4.2 y 4.3 de este documento.

## 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

Además de lo estipulado en la CPS, pueden solicitar la revocación los responsables asociados a la concesión de acceso a los sistemas de información de la organización cuyo dominio aparece en el certificado.

### 4.9.3. Procedimiento de solicitud de revocación

La solicitud de revocación de los certificados emitidos bajo la presente política se efectúa mediante la aplicación de gestión de certificados de inicio de sesión en Windows y de Controlador de Dominio, siendo el responsable por parte de la organización que posea el dominio donde reside el controlador el encargado de efectuarla. Dicho responsable se identificará frente a la aplicación mediante su certificado reconocido en dispositivo seguro de creación de firma, válido y en vigor, que garantiza de manera fiable e inequívoca su identidad.

Una vez identificado y autorizado, podrá efectuar la solicitud de revocación de los certificados de Controlador de Dominio que le permita dicha autorización.

### 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

No se contempla la suspensión de los certificados emitidos bajo la presente política.

### 4.9.6. Entidad que puede solicitar la suspensión

No se contempla la suspensión de los certificados emitidos bajo la presente política.

### 4.9.7. Procedimiento para la solicitud de suspensión

No se contempla la suspensión de los certificados emitidos bajo la presente política.

### 4.9.8. Límites del período de suspensión

No se contempla la suspensión de los certificados emitidos bajo la presente política.

Clf.: <b>PUBLICO</b>	Ref.: ACCV-CP-12V1.0-c.doc	Versión: 1.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.12.1.0	Pág. 15



#### 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 de una dirección de correo electrónico, devuelve los certificados vinculados a esa dirección y el estado de éstos. Este formulario se encuentra en el sitio web de la Autoridad de Certificación en la URI <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.

### 4.11. Finalización de la suscripción.

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

### 4.12. Depósito y recuperación de claves.

La ACCV no guarda en depósito las claves privadas de los certificados electrónicos emitidos bajo la presente Política, por lo que si el firmante pierde su clave privada, no se podrá recuperar.

Clf.: <b>PUBLICO</b>	Ref.: ACCV-CP-12V1.0-c.doc	Versión: 1.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.12.1.0	Pág. 16



## 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.

Clf.: <b>PUBLICO</b>	Ref.: ACCV-CP-12V1.0-c.doc	Versión: 1.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.12.1.0	Pág. 17



### 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.

Clf.: <b>PUBLICO</b>	Ref.: ACCV-CP-12V1.0-c.doc	Versión: 1.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.12.1.0	Pág. 18



#### 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.

Clf.: <b>PUBLICO</b>	Ref.: ACCV-CP-12V1.0-c.doc	Versión: 1.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.12.1.0	Pág. 19



## 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.

Clf.: <b>PUBLICO</b>	Ref.: ACCV-CP-12V1.0-c.doc	Versión: 1.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.12.1.0	Pág. 20



## 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 Autoridad de Certificación de la Comunidad Valenciana.

#### 6.1.1. Generación del par de claves

Los pares de claves para los certificados emitidos bajo el ámbito de la presente Política de Certificación se generan en el servidor de la ACCV.

#### 6.1.2. Entrega de la clave privada a la entidad

La clave privada se encuentra en el fichero en formato PKCS#12 que recoge el subscritor en la aplicación de gestión de certificados de inicio de sesión en Windows y de Controlador de Dominio. Este fichero contiene las claves y el certificado de Controlador de Dominio en un fichero cifrado. Una vez efectuada la entrega, los datos de creación de firma se eliminan de los sistemas de la ACCV.

#### 6.1.3. Entrega de la clave pública al emisor del certificado

La clave pública se encuentra en el fichero en formato PKCS#12 que recoge el responsable por parte de la organización en la aplicación de gestión de certificados de inicio de sesión en Windows y de Controlador de Dominio. Este fichero contiene las claves y el certificado de Controlador de Dominio en un fichero cifrado. Una vez efectuada la entrega, los datos de creación de firma se eliminan de los sistemas de la ACCV.

#### 6.1.4. Entrega de la clave pública de la CA a los usuarios

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

#### 6.1.5. Tamaño de las claves

El tamaño de las claves para los certificados emitidos bajo el ámbito de la presente Política de Certificación es de 1024 bits.

#### 6.1.6. Parámetros de generación de la clave pública

Se utilizan los parámetros definidos en la suite criptográfica 001 especificada en el documento de ETSI SR 002 176 "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signature". Se define ModLen=1024.

Signature suite entry index	Signature algorithm	Signature algorithm parameters	Key generation algorithm	Padding method	Cryptographic hash function	Valid until (signing)
001	rsa	MinModLen=1020	rsagen1	emsa-pkcs1-v1_5	sha1	31.12.2005



### 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 SR 002 176 "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signature". Se define ModLen=1024.

Signature suite entry index	Signature algorithm	Signature algorithm parameters	Key generation algorithm	Padding method	Cryptographic hash function	Valid until (signing)
001	rsa	MinModLen=1020	rsagen1	emsa-pkcs1-v1_5	sha1	31.12.2005

### 6.1.8. Hardware/software de generación de claves

La generación de las claves se realiza en un sistema perteneciente al núcleo protegido de la Infraestructura de Clave Pública de la ACCV.

El almacenamiento de las claves será de forma definitiva en los medios físicos disponibles por el Controlador de Dominio al que va asignado el certificado.

### 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 Autoridad de Certificación de la Comunidad Valenciana.

### 6.2.1. Estándares para los módulos criptográficos

No aplicable para la presente política.

### 6.2.2. Control multipersona de la clave privada

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

### 6.2.3. Custodia de la clave privada

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

### 6.2.4. Copia de seguridad de la clave privada

No estipulado

Clf.: <b>PUBLICO</b>	Ref.: ACCV-CP-12V1.0-c.doc	Versión: 1.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.12.1.0	Pág. 22



#### 6.2.5. Archivo de la clave privada.

No estipulado

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

No aplicable para la presente política.

#### 6.2.7. Método de activación de la clave privada.

La activación de la clave privada se realizará a través de la introducción de la palabra de paso de acceso a esta clave, contenida en el fichero con formato PKCS#12.

#### 6.2.8. Método de desactivación de la clave privada

La desactivación de la clave privada se consigue mediante el apagado del Controlador de Dominio donde se encuentra instalada.

#### 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 tres (3) años.

El par de claves utilizado para la emisión de los certificados se crea para cada emisión, y por tanto también tienen una validez de tres (3) años.

### 6.4. Datos de activación

#### 6.4.1. Generación y activación de los datos de activación

El responsable por parte de la organización que posee el dominio determina en el momento de la solicitud de certificado la palabra de paso de acceso a la clave privada o de protección del fichero que contiene el PKCS#12.

#### 6.4.2. Protección de los datos de activación

Es responsabilidad del Administrador del Dominio bajo cuya gestión esta el Controlador del Dominio al que va dirigido el certificado la custodia o, si la política interna de la organización lo requiere, la modificación de dicha palabra de paso.

#### 6.4.3. Otros aspectos de los datos de activación

No estipulado.

Clf.: <b>PUBLICO</b>	Ref.: ACCV-CP-12V1.0-c.doc	Versión: 1.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.12.1.0	Pág. 23



### 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.

Clf.: <b>PUBLICO</b>	Ref.: ACCV-CP-12V1.0-c.doc	Versión: 1.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.12.1.0	Pág. 24



## 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 del certificado .

#### 7.1.2. Extensiones del certificado

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

Campo	Valor
<b>Subject</b>	
CommonName	Nombre Cualificado Completo del Controlador de Dominio (FQDN)
OrganizationalUnit	Logon
Organization	Generalitat Valenciana
Country	ES
<b>Version</b>	V3
<b>SerialNumber</b>	Identificador único del certificado. Menor de 32 caracteres hexadecimales.
<b>Algoritmo de firma</b>	sha1withRSAEncryption
<b>Issuer (Emisor)</b>	
CommonName	ACCV-CA3
OrganizationalUnit	PKIGVA
Organization	Generalitat Valenciana
Country	ES
<b>Válido desde</b>	Fecha de Emisión
<b>Válido hasta</b>	Fecha de Caducidad
<b>Clave Pública</b>	Octet String conteniendo la clave pública del suscriptor
<b>Extended Key Usage</b>	
	Client Authentication
	Server Authentication
<b>CRL Distribution Point</b>	<a href="http://www.accv.es/gestcert/cagva-logon_der.crl">http://www.accv.es/gestcert/cagva-logon_der.crl</a>
<b>SubjectAlternativeName</b>	
Other (1.3.6.1.4.1.311.25.1) Name	Identificador Unico Global (GUID) del Controlador de Dominio en el Directorio Activo del Dominio
DNS Name	Nombre Cualificado Completo del Controlador de Dominio (FQDN)
<b>Certificate Policy Extensions</b>	



Policy OID	1.3.6.1.4.1.8149.3.12.1.0
Policy CPS Location	http://www.accv.es/legislacion_c.htm
Policy Notice	Certificado no reconocido de Controlador de Dominio expedido por la Autoridad de Certificación de la Comunidad Valenciana (Pl. Manises 1. CIF S4611001A). CPS y CP en http://www.accv.es
<b>Authority Information Access</b>	http://ocsp.accv.es
<b>Fingerprint issuer</b>	714C 0354 F272 6B5C 8D1E 71D4 5882 0DD7 1F57 B7DD
<b>Algoritmo de hash</b>	SHA-1
<b>Certificate Template Extension</b>	DomainController
<b>KeyUsage (críticos)</b>	
	Digital Signature
	Key Encipherment

### 7.1.3. Identificadores de objeto (OID) de los algoritmos

Identificador de Objeto (OID) de los algoritmos Criptográficos:

- md5withRSAEncryption (1.2.840.113549.1.1.4)
- SHA1withRSAEncryption (1.2.840.113549.1.1.5)

### 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.

El campo cn del subject name se cumplimenta obligatoriamente en mayúsculas, prescindiendo de acentos y sustituyendo la letra "Ñ" por la "N" y la letra "Ç" por la "C". Esta característica se da únicamente en el atributo CommonName.

### 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 la ACCV para identificar la presente política es el siguiente:

1.3.6.1.4.1.8149.3.12.1.0

Clf.: <b>PUBLICO</b>	Ref.: ACCV-CP-12V1.0-c.doc	Versión: 1.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.12.1.0	Pág. 26



#### 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 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.

### 7.3 Listas de Certificados Revocados

#### 7.3.1 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,

Clf.: <b>PUBLICO</b>	Ref.: ACCV-CP-12V1.0-c.doc	Versión: 1.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.12.1.0	Pág. 27



## 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.

Clf.: <b>PUBLICO</b>	Ref.: ACCV-CP-12V1.0-c.doc	Versión: 1.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.12.1.0	Pág. 28



## 9. Requisitos comerciales y legales

### 9.1. Tarifas

#### 9.1.1. Tarifas de emisión de certificado o renovación

No se aplica ninguna tarifa sobre la emisión o renovación de certificados bajo el amparo de la presente política de certificación.

#### 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 emitido por la Caja de Ahorros de Valencia, Castellón y Alicante, Bancaja, 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 Autoridad de Certificación, 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.

Clf.: <b>PUBLICO</b>	Ref.: ACCV-CP-12V1.0-c.doc	Versión: 1.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.12.1.0	Pág. 29



### 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.

Clf.: <b>PUBLICO</b>	Ref.: ACCV-CP-12V1.0-c.doc	Versión: 1.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.12.1.0	Pág. 30



### 9.6.2. Obligaciones de la Autoridad de Registro

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

### 9.6.3. Obligaciones de los suscriptores

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

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

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

### 9.6.5. Obligaciones del repositorio

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

## 9.7. Renuncias de garantías

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

## 9.8. Limitaciones de responsabilidad

### 9.8.1. Garantías y limitaciones de garantías

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

### 9.8.2. Deslinde de responsabilidades

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

### 9.8.3. Limitaciones de pérdidas

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

## 9.9. 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.

Clf.: <b>PUBLICO</b>	Ref.: ACCV-CP-12V1.0-c.doc	Versión: 1.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.12.1.0	Pág. 31



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.

### 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.

Clf.: <b>PUBLICO</b>	Ref.: ACCV-CP-12V1.0-c.doc	Versión: 1.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.12.1.0	Pág. 32