



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



# Autoritat de Certificació de la Comunitat Valenciana

## Política de Certificación de Certificados Reconocidos en soporte software para ciudadanos

<b>Fecha:</b> 11 de octubre de 2004	<b>Versión:</b> 2.0
<b>Estado:</b> APROBADO	<b>Nº de páginas:</b> 45
<b>OID:</b> 1.3.6.1.4.1.8149.3.7.2.0	<b>Clasificación:</b> PUBLICO
<b>Archivo:</b> PKIGVA-CP-07V2.0-c.doc	
<b>Preparado por:</b> ACCV	

## Tabla de Contenido

<b>1. INTRODUCCIÓN.....</b>	<b>8</b>
1.1. VISTA GENERAL.....	8
1.2. IDENTIFICACIÓN.....	9
1.3. COMUNIDAD 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>Entidades Finales</i> .....	10
1.3.4. <i>Ámbito de aplicación</i> .....	10
1.4. DATOS DE CONTACTO.....	11
1.4.1. <i>Persona de Contacto</i> .....	11
1.4.2. <i>Determinación de la adecuación de la CPS a la Política</i> .....	11
<b>2. CLÁUSULAS GENERALES.....</b>	<b>12</b>
2.1. OBLIGACIONES.....	12
2.1.1. <i>Obligaciones de la CA</i> .....	12
2.1.2. <i>Obligaciones de la RA</i> .....	12
2.1.3. <i>Obligaciones de los Suscriptores</i> .....	12
2.1.4. <i>Obligaciones de las partes confiantes</i> .....	12
2.1.5. <i>Obligaciones del repositorio</i> .....	12
2.2. RESPONSABILIDAD.....	12
2.2.1. <i>Responsabilidad de la CA</i> .....	12
2.2.2. <i>Responsabilidad de la RA</i> .....	13
2.3. RESPONSABILIDAD FINANCIERA.....	13
2.3.1. <i>Indemnización a las partes confiantes</i> .....	13
2.3.2. <i>Relaciones fiduciarias</i> .....	13
2.3.3. <i>Procesos administrativos</i> .....	13
2.4. INTERPRETACIÓN Y EJECUCIÓN.....	13
2.4.1. <i>Leyes gubernamentales</i> .....	13
2.4.2. <i>Extinción, subsistencia, fusión, y notificación</i> .....	13
2.4.3. <i>Procedimientos de resolución de disputas</i> .....	13
2.5. TARIFAS.....	14
2.5.1. <i>Tarifas de emisión de certificado o renovación</i> .....	14
2.5.2. <i>Tarifas de acceso a los certificados</i> .....	14
2.5.3. <i>Tarifas de acceso a la información de estado o revocación</i> .....	14
2.5.4. <i>Tarifas de otros servicios como información de políticas</i> .....	14
2.5.5. <i>Política de reintegros</i> .....	14
2.6. PUBLICACIÓN Y REPOSITORIOS.....	14

2.6.1.	<i>Publicación de información de la CA.....</i>	<i>14</i>
2.6.2.	<i>Frecuencia de publicación .....</i>	<i>15</i>
2.6.3.	<i>Controles de acceso.....</i>	<i>15</i>
2.6.4.	<i>Repositorios.....</i>	<i>15</i>
2.7.	<b>CONTROL DE CONFORMIDAD .....</b>	<b>15</b>
2.7.1.	<i>Frecuencia de los controles de conformidad.....</i>	<i>15</i>
2.7.2.	<i>Identificación/cualificación del auditor.....</i>	<i>15</i>
2.7.3.	<i>Relación entre el auditor y la entidad auditada .....</i>	<i>15</i>
2.7.4.	<i>Tópicos cubiertos por el control de conformidad.....</i>	<i>15</i>
2.7.5.	<i>Acciones a tomar como resultado de una deficiencia.....</i>	<i>15</i>
2.7.6.	<i>Comunicación de resultados.....</i>	<i>16</i>
2.8.	<b>POLÍTICA DE CONFIDENCIALIDAD .....</b>	<b>16</b>
2.8.1.	<i>Tipo de información a mantener confidencial.....</i>	<i>16</i>
2.8.2.	<i>Tipo de información no considerada confidencial .....</i>	<i>16</i>
2.8.3.	<i>Divulgación de información de revocación /suspensión de certificados.....</i>	<i>16</i>
2.8.4.	<i>Envío a la autoridad judicial y/o policial.....</i>	<i>16</i>
2.8.5.	<i>Publicación como parte de un descubrimiento civil.....</i>	<i>16</i>
2.8.6.	<i>Divulgación a petición del propietario.....</i>	<i>16</i>
2.8.7.	<i>Otras circunstancias de publicación de información .....</i>	<i>16</i>
2.9.	<b>DERECHOS DE PROPIEDAD INTELECTUAL .....</b>	<b>17</b>
<b>3.</b>	<b>IDENTIFICACIÓN Y AUTENTIFICACIÓN.....</b>	<b>18</b>
3.1.	<b>REGISTRO INICIAL .....</b>	<b>18</b>
3.1.1.	<i>Tipos de nombres.....</i>	<i>18</i>
3.1.2.	<i>Necesidad de los nombres de ser significativos.....</i>	<i>18</i>
3.1.3.	<i>Reglas para interpretar varios formatos de nombres.....</i>	<i>18</i>
3.1.4.	<i>Unicidad de los nombres .....</i>	<i>18</i>
3.1.5.	<i>Procedimientos de resolución de disputas de nombres .....</i>	<i>18</i>
3.1.6.	<i>Reconocimiento, autenticación y función de las marcas registradas.....</i>	<i>18</i>
3.1.7.	<i>Métodos de prueba de posesión de la clave privada .....</i>	<i>18</i>
3.1.8.	<i>Autenticación de la identidad de una organización .....</i>	<i>18</i>
3.1.9.	<i>Autenticación de la identidad de un individuo .....</i>	<i>19</i>
3.2.	<b>RENOVACIÓN RUTINARIA DE LA CLAVE.....</b>	<b>19</b>
3.3.	<b>RENOVACIÓN DE CLAVE DESPUÉS DE UNA REVOCACIÓN – CLAVE NO COMPROMETIDA .....</b>	<b>19</b>
3.4.	<b>SOLICITUD DE REVOCACIÓN .....</b>	<b>20</b>
<b>4.</b>	<b>REQUERIMIENTOS OPERACIONALES.....</b>	<b>21</b>
4.1.	<b>SOLICITUD DE CERTIFICADOS .....</b>	<b>21</b>
4.2.	<b>EMISIÓN DE CERTIFICADOS.....</b>	<b>21</b>
4.3.	<b>ACEPTACIÓN DE CERTIFICADOS.....</b>	<b>21</b>

4.4.	SUSPENSIÓN Y REVOCACIÓN DE CERTIFICADOS .....	22
4.4.1.	<i>Circunstancias para la revocación</i> .....	22
4.4.2.	<i>Quién puede solicitar la revocación</i> .....	22
4.4.3.	<i>Procedimiento de solicitud de revocación</i> .....	22
4.4.4.	<i>Periodo de gracia de la solicitud de revocación</i> .....	23
4.4.5.	<i>Circunstancias para la suspensión</i> .....	23
4.4.6.	<i>Quien puede solicitar la suspensión</i> .....	24
4.4.7.	<i>Procedimiento para la solicitud de suspensión</i> .....	24
4.4.8.	<i>Limites del periodo de suspensión</i> .....	24
4.4.9.	<i>Frecuencia de emisión de CRLs</i> .....	24
4.4.10.	<i>Requisitos de comprobación de CRLs</i> .....	24
4.4.11.	<i>Disponibilidad de comprobación on-line de revocación/estado</i> .....	24
4.4.12.	<i>Requisitos de comprobación on-line de revocación</i> .....	24
4.4.13.	<i>Otras formas de divulgación de revocación disponibles</i> .....	25
4.4.14.	<i>Requisitos de comprobación para otras formas de divulgación de revocación</i> .....	25
4.4.15.	<i>Requisitos especiales de renovación de claves comprometidas</i> .....	25
4.5.	PROCEDIMIENTOS DE CONTROL DE SEGURIDAD.....	25
4.5.1.	<i>Tipos de eventos registrados</i> .....	25
4.5.2.	<i>Frecuencia de procesado de logs</i> .....	25
4.5.3.	<i>Periodo de retención para los logs de auditoría</i> .....	25
4.5.4.	<i>Protección de los logs de auditoría</i> .....	25
4.5.5.	<i>Procedimientos de backup de los logs de auditoría</i> .....	26
4.5.6.	<i>Sistema de recogida de información de auditoría (interno vs externo)</i> .....	26
4.5.7.	<i>Notificación al sujeto causa del evento</i> .....	26
4.5.8.	<i>Análisis de vulnerabilidades</i> .....	26
4.6.	ARCHIVO DE REGISTROS .....	26
4.6.1.	<i>Tipo de eventos registrados</i> .....	26
4.6.2.	<i>Periodo de retención para el archivo</i> .....	26
4.6.3.	<i>Protección del archivo</i> .....	26
4.6.4.	<i>Procedimientos de backup del archivo</i> .....	26
4.6.5.	<i>Requerimientos para el sellado de tiempo de los registros</i> .....	27
4.6.6.	<i>Sistema de recogida de información de auditoría (interno vs externo)</i> .....	27
4.6.7.	<i>Procedimientos para obtener y verificar información archivada</i> .....	27
4.7.	CAMBIO DE CLAVE.....	27
4.8.	RECUPERACIÓN EN CASO DE COMPROMISO DE UNA CLAVE O UN DESASTRE .....	27
4.8.1.	<i>Alteración de los recursos hardware, software y/o datos</i> .....	27
4.8.2.	<i>La clave publica de una entidad se revoca</i> .....	27
4.8.3.	<i>La clave de una entidad se compromete</i> .....	27
4.8.4.	<i>Instalación de seguridad después de un desastre natural u otro tipo de desastre</i> .....	27
4.9.	CESE DE UNA CA.....	28

<b>5.</b>	<b>CONTROLES DE SEGURIDAD FÍSICA, PROCEDURAL Y DE PERSONAL .....</b>	<b>29</b>
5.1.	CONTROLES DE SEGURIDAD FÍSICA .....	29
5.1.1.	<i>Ubicación y construcción .....</i>	29
5.1.2.	<i>Acceso físico .....</i>	29
5.1.3.	<i>Alimentación eléctrica y aire acondicionado .....</i>	29
5.1.4.	<i>Exposición al agua .....</i>	29
5.1.5.	<i>Protección y prevención de incendios .....</i>	29
5.1.6.	<i>Sistema de almacenamiento.....</i>	29
5.1.7.	<i>Eliminación de residuos .....</i>	29
5.1.8.	<i>Backup remoto.....</i>	30
5.2.	CONTROLES PROCEDIMENTALES .....	30
5.2.1.	<i>Papeles de confianza .....</i>	30
5.2.2.	<i>Numero de personas requeridas por tarea .....</i>	30
5.2.3.	<i>Identificación y autenticación para cada papel .....</i>	30
5.3.	CONTROLES DE SEGURIDAD DE PERSONAL .....	30
5.3.1.	<i>Requerimientos de antecedentes, calificación, experiencia, y acreditación.....</i>	30
5.3.2.	<i>Procedimientos de comprobación de antecedentes .....</i>	30
5.3.3.	<i>Requerimientos de formación .....</i>	30
5.3.4.	<i>Requerimientos y frecuencia de la actualización de la formación .....</i>	31
5.3.5.	<i>Frecuencia y secuencia de rotación de tareas.....</i>	31
5.3.6.	<i>Sanciones por acciones no autorizadas.....</i>	31
5.3.7.	<i>Requerimientos de contratación de personal .....</i>	31
5.3.8.	<i>Documentación proporcionada al personal.....</i>	31
<b>6.</b>	<b>CONTROLES DE SEGURIDAD TÉCNICA .....</b>	<b>32</b>
6.1.	GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES .....	32
6.1.1.	<i>Generación del par de claves .....</i>	32
6.1.2.	<i>Entrega de la clave privada a la entidad.....</i>	32
6.1.3.	<i>Entrega de la clave pública al emisor del certificado .....</i>	32
6.1.4.	<i>Entrega de la clave pública de la CA a los usuarios.....</i>	32
6.1.5.	<i>Tamaño de las claves.....</i>	32
6.1.6.	<i>Parámetros de generación de la clave pública.....</i>	33
6.1.7.	<i>Comprobación de la calidad de los parámetros.....</i>	33
6.1.8.	<i>Hardware/software de generación de claves.....</i>	33
6.1.9.	<i>Fines del uso de la clave.....</i>	33
6.2.	PROTECCIÓN DE LA CLAVE PRIVADA .....	34
6.2.1.	<i>Estándares para los módulos criptográficos .....</i>	34
6.2.2.	<i>Control multipersona de la clave privada .....</i>	34
6.2.3.	<i>Custodia de la clave privada .....</i>	34
6.2.4.	<i>Copia de seguridad de la clave privada.....</i>	34

6.2.5.	<i>Archivo de la clave privada</i> .....	34
6.2.6.	<i>Introducción de la clave privada en el módulo criptográfico</i> .....	34
6.2.7.	<i>Método de activación de la clave privada</i> .....	34
6.2.8.	<i>Método de desactivación de la clave privada</i> .....	35
6.2.9.	<i>Método de destrucción de la clave privada</i> .....	35
6.3.	OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES .....	35
6.3.1.	<i>Archivo de la clave pública</i> .....	35
6.3.2.	<i>Periodo de uso para las claves públicas y privadas</i> .....	35
6.4.	DATOS DE ACTIVACIÓN .....	35
6.4.1.	<i>Generación y activación de los datos de activación</i> .....	35
6.4.2.	<i>Protección de los datos de activación</i> .....	35
6.4.3.	<i>Otros aspectos de los datos de activación</i> .....	35
6.5.	CONTROLES DE SEGURIDAD INFORMÁTICA .....	36
6.5.1.	<i>Requerimientos técnicos de seguridad informática específicos</i> .....	36
6.5.2.	<i>Valoración de la seguridad informática</i> .....	36
6.6.	CONTROLES DE SEGURIDAD DEL CICLO DE VIDA .....	36
6.6.1.	<i>Controles de desarrollo del sistema</i> .....	36
6.6.2.	<i>Controles de gestión de la seguridad</i> .....	36
6.6.3.	<i>Evaluación de la seguridad del ciclo de vida</i> .....	36
6.7.	CONTROLES DE SEGURIDAD DE LA RED .....	36
6.8.	CONTROLES DE INGENIERÍA DE LOS MÓDULOS CRIPTOGRÁFICOS .....	36
<b>7.</b>	<b>PERFILES DE CERTIFICADO Y CRL .....</b>	<b>37</b>
7.1.	PERFIL DE CERTIFICADO.....	37
7.1.1.	<i>Número de versión</i> .....	37
7.1.2.	<i>Extensiones del certificado</i> .....	37
7.1.3.	<i>Identificadores de objeto (OID) de los algoritmos</i> .....	38
7.1.4.	<i>Formatos de nombres</i> .....	38
7.1.5.	<i>Restricciones de los nombres</i> .....	39
7.1.6.	<i>Identificador de objeto (OID) de la Política de certificación</i> .....	39
7.1.7.	<i>Uso de la extensión “Policy Constraints”</i> .....	39
7.1.8.	<i>Sintaxis y semántica de los cualificadores de política</i> .....	39
7.1.9.	<i>Tratamiento semántico para la extensión crítica “Certificate Policy”</i> .....	39
7.2.	PERFIL DE CRL .....	39
7.2.1.	<i>Número de versión</i> .....	39
7.2.2.	<i>CRL y extensiones</i> .....	39
<b>8.</b>	<b>ESPECIFICACIÓN DE LA ADMINISTRACIÓN .....</b>	<b>40</b>
8.1.	PROCEDIMIENTOS DE ESPECIFICACIÓN DE CAMBIOS .....	40
8.2.	PROCEDIMIENTOS DE PUBLICACIÓN Y NOTIFICACIÓN .....	40

8.3. PROCEDIMIENTOS DE APROBACIÓN DE LA CPS.....	40
<b>ANEXO I.....</b>	<b>41</b>
<b>ANEXO II – FORMULARIO DE SOLICITUD DE REVOCACIÓN DE CERTIFICADO.....</b>	<b>44</b>

Clf.: <b>PUBLICO</b>	Ref.: PKIGVA-CP-07V2.0-c.doc	Versión: 2.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.7.2.0	Pág. 7 de 44

# 1. INTRODUCCIÓN

La presente Política de Certificación es conforme con la especificación del RFC 2527 “*Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*” propuesto por S. Chokhani y W. Ford, del Internet Engineering Task Force (IETF), para este tipo de documentos. Se incluyen todas las secciones de la especificación a fin de dotar de consistencia al documento. Cuando no exista ninguna disposición o limitación respecto de una sección aparecerá la frase “No estipulado” contenida en dicha sección.

Esta Política de Certificación asume que el lector conoce los conceptos básicos de PKI, 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.

## 1.1. Vista General

Esta Política de certificación 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 Generalitat Valenciana y las reglas de solicitud, adquisición gestión y uso de los certificados.

La Política de Certificación referida en este documento se utilizará para la emisión de certificados reconocidos en soporte software para ciudadanos de la Comunidad Valenciana según la legislación vigente. Para la redacción de esta política se han considerado las siguientes normas:

- Decreto del Consell 87/2002, de 30 de mayo, por el que se regula la utilización de la firma electrónica avanzada en la Generalitat Valenciana
- Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario par la firma electrónica.
- Ley 59/2003, de 19 de diciembre, de Firma electrónica.

La entidad involucrada en el uso de los certificados emitidos bajo el amparo de la presente política es la propia Generalitat Valenciana así como las entidades y organismos vinculados a ella, y las Administraciones Públicas o Corporativas con la que haya establecido convenio de certificación.

Clf.: <b>PUBLICO</b>	Ref.: PKIGVA-CP-07V2.0-c.doc	Versión: 2.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.7.2.0	Pág. 8 de 45



## 1.2. Identificación

Nombre de la política	Política de Certificación de Certificados Reconocidos en soporte software para ciudadanos
Calificador de la política	Certificado reconocido para Ciudadanos expedido por la Autoridad de Certificación de la Generalitat Valenciana (Pl. Manises 1. CIF S4611001A). CPS y CP en <a href="http://www.pki.gva.es">http://www.pki.gva.es</a>
Versión de la política	2.0
Estado de la política	BORRADOR
Referencia de la política / OID (Object Identifier)	1.3.6.1.4.1.8149.3.7.2.0
Fecha de emisión	PENDIENTE DE EMISIÓN
Fecha de expiración	No aplicable.
CPS relacionada	Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalitat Valenciana. Versión 1.0.  OID: 1.3.6.1.4.1.8149.2.1.0  Disponible en <a href="http://www.pki.gva.es/pdf-politicas/PKIGVA-CPS.pdf">http://www.pki.gva.es/pdf-politicas/PKIGVA-CPS.pdf</a>
Localización	Esta Política de certificación se puede encontrar en: <a href="http://www.pki.gva.es/legislacion_c.htm">http://www.pki.gva.es/legislacion_c.htm</a>

## 1.3. Comunidad y Ámbito de aplicación

### 1.3.1. Autoridades de Certificación

La CA que puede emitir certificados acordes con esta política es “**CAGVA**” perteneciente a la Autoridad de Certificación de la Comunidad Valenciana.

### 1.3.2. Autoridades de Registro

La lista de Autoridades de Registro que gestionan las solicitudes de certificados definidos en esta política se encuentra en la URL [http://www.pki.gva.es/puntreg\\_c.htm](http://www.pki.gva.es/puntreg_c.htm).

Clf.: <b>PUBLICO</b>	Ref.: PKIGVA-CP-07V2.0-c.doc	Versión: 2.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.7.2.0	Pág. 9 de 45

### 1.3.3. Entidades Finales

#### 1.3.3.1. Firmantes

El grupo de usuarios que pueden solicitar certificados definidos por esta política está compuesto por cualquier persona física en posesión de los elementos de identificación requeridos (DNI, NIE, etc.).

El soporte de claves y certificados es software (disquete, disco duro, CDROM u otros medios de almacenamiento).

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 clientes de correo electrónico S/MIME en el ámbito de la verificación de la identidad del emisor de mensajes de correo electrónico y del cifrado de los mismos.
- Las aplicaciones y servicios pertenecientes a la Generalitat Valenciana, a alguna de las entidades u organizaciones vinculados a la Generalitat o a Administraciones Públicas o Corporativas con las que se haya firmado convenio de certificación.
- Las aplicaciones y servicios que, sin pertenecer a la Generalitat Valenciana, entidades u organismos vinculados a ella, ni a Administraciones Públicas ni Corporativas con las que se haya establecido convenio de certificación, se emplean en relaciones entre ciudadanos, empresas u otras Administraciones Públicas con la Generalitat Valenciana, entidades u organismos vinculados a ella o Administraciones Públicas con las que se haya establecido convenio de certificación.

### 1.3.4. Ámbito de aplicación

#### 1.3.4.1. Usos Permitidos

Los certificados emitidos por la Autoridad de Certificación de la Comunidad Valenciana bajo esta Política de Certificación, pueden utilizarse para la firma electrónica y cifrado de cualquier información o documento. Asimismo, pueden utilizarse como mecanismo de identificación ante servicios y aplicaciones informáticas.

#### 1.3.4.2. Usos Restringidos

No estipulado

Clf.: <b>PUBLICO</b>	Ref.: PKIGVA-CP-07V2.0-c.doc	Versión: 2.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.7.2.0	Pág. 10 de 45

### 1.3.4.3. Usos Prohibidos

Esta prohibido el uso de los certificados emitidos por la Autoridad de Certificación de la Comunidad Valenciana bajo esta Política de certificación para cualquier uso no especificados por los puntos “1.3.4.1 Usos Permitidos” y “1.3.4.2 Usos Restringidos” del presente documento.

## 1.4. Datos de contacto

Esta Política de Certificación es propiedad y está administrada por la “Secretaria Autònica de Telecomunicacions i Societat de la Informació” por sus competencias como Autoridad de Certificación de la Comunidad Valenciana.

Nombre	<i>Secretaria Autònica de Telecomunicacions i Societat de la Informació</i>
Dirección de email	<i>satsi@gva.es</i>
Dirección	<i>C/ Colón, 66 – 46004 Valencia (Spain)</i>
Número de teléfono	<i>+34-96-196 1130</i>
Número de fax	<i>+34-96-196 1001</i>

### 1.4.1. Persona de Contacto

Para más información relacionada con la presente Política de Certificación por favor contacte con:

Nombre	<i>Secretaria Autònica de Telecomunicacions i Societat de la Informació Conselleria d'Infraestructures i Transport</i>
Dirección de email	<i>firma@gva.es</i>
Dirección	<i>C/ Colón, 66 – 46004 Valencia (Spain)</i>
Número de teléfono	<i>+34-902 482 481</i>
Número de fax	<i>+34-96 196 1001</i>

### 1.4.2. Determinación de la adecuación de la CPS a la Política

La Secretaria Autonómica de Telecomunicaciones y Sociedad de la Información es el Órgano que determina la adecuación de esta Política de Certificación a la Declaración de Prácticas de Certificación (CPS) de su PKI, tal y como se recoge en el Decreto 87/2002, de 30 de mayo, del Gobierno Valenciano.

## 2. Cláusulas Generales

### 2.1. Obligaciones

#### 2.1.1. Obligaciones de la CA

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

Adicionalmente, las CAs especificadas en el punto 1.3.1 “Autoridades de Certificación” están obligadas a:

- Adaptar sus operaciones para cumplir lo estipulado por esta Política de Certificación.
- Emitir certificados en conformidad con esta Política de Certificación.

#### 2.1.2. Obligaciones de la RA

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

#### 2.1.3. Obligaciones de los Suscriptores

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

#### 2.1.4. Obligaciones de las partes confiantes

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

#### 2.1.5. Obligaciones del repositorio

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

### 2.2. Responsabilidad

#### 2.2.1. Responsabilidad de la CA

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

Clf.: <b>PUBLICO</b>	Ref.: PKIGVA-CP-07V2.0-c.doc	Versión: 2.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.7.2.0	Pág. 12 de 45

## 2.2.2. Responsabilidad de la RA

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

## 2.3. Responsabilidad Financiera

### 2.3.1. Indemnización a las partes confiantes

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

### 2.3.2. Relaciones fiduciarias

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

### 2.3.3. Procesos administrativos

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

## 2.4. Interpretación y Ejecución

### 2.4.1. Leyes gubernamentales

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

### 2.4.2. Extinción, subsistencia, fusión, y notificación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

### 2.4.3. Procedimientos de resolución de disputas

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

Clf.: <b>PUBLICO</b>	Ref.: PKIGVA-CP-07V2.0-c.doc	Versión: 2.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.7.2.0	Pág. 13 de 45

## 2.5. Tarifas

### 2.5.1. 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.

### 2.5.2. Tarifas de acceso a los certificados

El acceso a los certificados emitidos bajo esta política, dada su naturaleza publica, es libre y gratuito y por tanto no hay ninguna tarifa de aplicación sobre el mismo.

### 2.5.3. Tarifas de acceso a la información de estado o revocación

El acceso a la información de estado o revocación de los certificados es libre y gratuita y por tanto no se aplicará ninguna tarifa.

### 2.5.4. Tarifas de otros servicios como información de políticas

No se aplicará ninguna tarifa por el servicio de información sobre esta política ni por ningún otro servicio adicional del que se tenga conocimiento en el momento de la redacción del presente documento.

### 2.5.5. Política de reintegros

Al no existir ninguna tarifa de aplicación para esta Política de certificación no es necesaria ninguna política de reintegros.

## 2.6. Publicación y Repositorios

### 2.6.1. Publicación de información de la CA

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

La presente Política de Certificación es pública y se encuentra disponible, en formato PDF, en la ubicación especificada en el apartado localización del punto “1.2 Identificación” del presente documento.

Clf.: <b>PUBLICO</b>	Ref.: PKIGVA-CP-07V2.0-c.doc	Versión: 2.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.7.2.0	Pág. 14 de 45

### 2.6.2. Frecuencia de publicación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la G Comunidad Valenciana.

### 2.6.3. Controles de acceso

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

### 2.6.4. Repositorios

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

## 2.7. Control de conformidad

### 2.7.1. Frecuencia de los controles de conformidad para cada entidad

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

### 2.7.2. Identificación/cualificación del auditor

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Generalidad Valenciana.

### 2.7.3. Relación entre el auditor y la entidad auditada

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

### 2.7.4. Tópicos cubiertos por el control de conformidad

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

### 2.7.5. Acciones a tomar como resultado de una deficiencia

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

Clf.: <b>PUBLICO</b>	Ref.: PKIGVA-CP-07V2.0-c.doc	Versión: 2.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.7.2.0	Pág. 15 de 45

### 2.7.6. Comunicación de resultados

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

## 2.8. Política de Confidencialidad

### 2.8.1. Tipo de información a mantener confidencial

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

### 2.8.2. Tipo de información no considerada confidencial

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

### 2.8.3. Divulgación de información de revocación /suspensión de certificados

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

### 2.8.4. Envío a la autoridad judicial y/o policial

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

### 2.8.5. Publicación como parte de un descubrimiento civil

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

### 2.8.6. Divulgación a petición del propietario

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

### 2.8.7. Otras circunstancias de publicación de información

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

Clf.: <b>PUBLICO</b>	Ref.: PKIGVA-CP-07V2.0-c.doc	Versión: 2.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.7.2.0	Pág. 16 de 45



## 2.9. Derechos de propiedad Intelectual

Todos los derechos de propiedad intelectual de la presente Política de Certificación pertenecen y permanecerán en propiedad de la Generalitat Valenciana.

Clf.: <b>PUBLICO</b>	Ref.: PKIGVA-CP-07V2.0-c.doc	Versión: 2.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.7.2.0	Pág. 17 de 45

## 3. IDENTIFICACIÓN Y AUTENTIFICACIÓN

### 3.1. Registro inicial

#### 3.1.1. Tipos de nombres

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

#### 3.1.2. Necesidad de los nombres de ser significativos

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

#### 3.1.3. Reglas para interpretar varios formatos de nombres

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

#### 3.1.4. Unicidad de los nombres

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

#### 3.1.5. Procedimientos de resolución de disputas de nombres

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

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

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Generalidad Valenciana.

#### 3.1.7. Métodos de prueba de posesión de la clave privada

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

#### 3.1.8. 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

Clf.: <b>PUBLICO</b>	Ref.: PKIGVA-CP-07V2.0-c.doc	Versión: 2.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.7.2.0	Pág. 18 de 45

personas jurídicas, entidades u organizaciones. Por tanto, no se considera necesaria la identificación de ninguna organización.

### 3.1.9. Autenticación de la identidad de un individuo

La autenticación de la identidad del solicitante de un certificado se realizará mediante su personación ante el Operador del Punto de Registro, acreditándose mediante la presentación del Documento Nacional de Identidad (DNI) pasaporte español o el Número de Identificación de Extranjeros (NIE) del solicitante.

Es necesario hacer notar que en este tipo de certificados se incluye la dirección de correo electrónico del suscriptor como elemento necesario para soportar el protocolo S/MIME, pero que la Autoridad de certificación de la Comunidad Valenciana no garantiza que esta dirección de correo esté vinculada con el suscriptor 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 Autoridad de Certificación de la Comunidad Valenciana 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 y/o que consta como vinculada al titular en las bases de datos de personal de la Comunidad Valenciana.

## 3.2. Renovación rutinaria de la clave

La autenticación para la renovación del certificado se realizará de forma presencial del mismo modo que el la identificación inicial descrita en el punto 3.1.9.

Está prevista la creación de un mecanismo de renovación telemática disponible desde el web de la Autoridad de Certificación utilizando solicitudes firmadas digitalmente mediante el certificado original que se pretende renovar y que elimine la necesidad de personarse para la renovación de los certificados, siempre que este no haya vencido ni se haya procedido a su revocación, y que le conste a la Autoridad de Certificación de la Comunidad Valenciana que el período de tiempo transcurrido desde la identificación por comparecencia personal del firmante es menor de cinco años.

## 3.3. 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 descrita en el punto 3.1.9.

Clf.: <b>PUBLICO</b>	Ref.: PKIGVA-CP-07V2.0-c.doc	Versión: 2.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.7.2.0	Pág. 19 de 45

### 3.4. Solicitud de revocación

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

- Presencial. Es el mismo que para el registro inicial descrito en el punto 3.1.9.
- Telemática. Mediante la firma electrónica del formulario de revocación ubicado en la URL [http://www.pki.gva.es/revoca\\_c.htm](http://www.pki.gva.es/revoca_c.htm).
- Telefónica. Mediante la respuesta a las preguntas realizadas desde el servicio de soporte telefónico disponible en el número 902482481

La Autoridad de Certificación de la Comunidad Valenciana 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.

Clf.: <b>PUBLICO</b>	Ref.: PKIGVA-CP-07V2.0-c.doc	Versión: 2.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.7.2.0	Pág. 20 de 45

## 4. REQUERIMIENTOS OPERACIONALES

### 4.1. Solicitud de certificados

El ciudadano que desee que le sea emitido un certificado de acuerdo con esta política de certificación deberá presentarse para solicitarlo en un Punto de Registro Autorizado de la Autoridad de certificación de la Comunidad Valenciana con su Documento Nacional de Identidad (DNI) o Número de Identificación de Extranjero (NIE) en vigor.

El listado de Puntos de registro autorizados se encuentra en la URL [http://www.pki.gva.es/puntreg\\_c.htm](http://www.pki.gva.es/puntreg_c.htm).

Es atribución de la Autoridad de Registro de la Autoridad de Certificación de la Comunidad Valenciana 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 del Operador de la Autoridad de Registro, el solicitante recibirá información de los motivos del rechazo de la misma.

### 4.2. Emisión de certificados

La emisión del certificado es un proceso que se realiza de forma inmediatamente posterior a la solicitud del mismo y en presencia del solicitante.

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

### 4.3. Aceptación de certificados

El suscriptor demuestra su aceptación del certificado con la firma del Contrato de Certificación y la recogida del mismo.

El Contrato de Certificación es un documento que debe ser firmado manualmente por el solicitante y 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.

Clf.: <b>PUBLICO</b>	Ref.: PKIGVA-CP-07V2.0-c.doc	Versión: 2.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.7.2.0	Pág. 21 de 45

## 4.4. Suspensión y revocación de certificados

### 4.4.1. Circunstancias para la revocación

Los certificados emitidos por la Autoridad de Certificación de la Comunidad Valenciana bajo esta Política de Certificación se revocarán o extinguirán su vigencia en los siguientes casos:

1. Expiración del período de validez que figura en el certificado.
2. Revocación formulada por el firmante, la persona representada por éste o un tercero autorizado.
3. Violación o puesta en peligro del secreto de los datos de creación de firma del firmante o de la Autoridad de Certificación de la Comunidad Valenciana o utilización indebida de estos datos por un tercero
4. Resolución judicial o administrativa que lo ordene
5. Fallecimiento o incapacidad sobrevenida, total o parcial, del firmante
6. Cese de la actividad de la Autoridad de Certificación de la Comunidad Valenciana, salvo que, previo consentimiento expreso del firmante, la gestión de estos certificados sean transferidos a otro prestador de servicios de certificación

La extinción de la vigencia de los certificados surtirá efectos frente a terceros, en el supuesto primero, desde que se produzca la expiración del período de validez, y en los demás casos, desde que la indicación de esta circunstancia se incluya e el servicio de consulta sobre la vigencia de los certificados de la Autoridad de Certificación de la Comunidad Valenciana.

### 4.4.2. Quién puede solicitar la revocación

La revocación de un certificado se puede iniciar tanto por el suscriptor del mismo como por parte de la propia Autoridad de Certificación de la Comunidad Valenciana.

Los suscriptores de certificados pueden solicitar su revocación por cualquier causa y deben solicitarla bajo las condiciones especificadas en el siguiente apartado.

### 4.4.3. Procedimiento de solicitud de revocación

La Autoridad de Certificación de la Comunidad Valenciana acepta solicitudes de revocación por los siguientes procedimientos

#### 4.4.3.1. Presencial

Mediante la presentación en un Punto de Registro de los especificados en el punto 1.3.2 de este documento del suscriptor del certificado y su identificación según el mecanismo establecido en el

Clf.: <b>PUBLICO</b>	Ref.: PKIGVA-CP-07V2.0-c.doc	Versión: 2.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.7.2.0	Pág. 22 de 45

punto 3.1.9 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

#### **4.4.3.2. Telemático**

Mediante la firma electrónica del formulario de revocación que se encuentra en la URL [http://www.pki.gva.es/revoca\\_c.htm](http://www.pki.gva.es/revoca_c.htm).

#### **4.4.3.3. Telefónico**

Mediante llamada telefónica al número de soporte telefónico de la Autoridad de Certificación de la Comunidad Valenciana 902482481.

En este caso, al no ser posible verificación de la identidad del solicitante, se procederá a la suspensión inmediata de la validez del certificado durante un plazo máximo de 15 días naturales, durante los que se procederá a verificar la veracidad de la solicitud. En el caso de no poder verificar la falsedad de la solicitud en dicho plazo, se procederá a la revocación definitiva del certificado. Es importante reseñar que el certificado no será válido desde el momento del procesamiento de la solicitud durante la llamada al centro de soporte. El mecanismo de verificación que se empleará será el envío a la dirección de correo electrónico vinculada al certificado a revocar de un mensaje advirtiendo del proceso de revocación en curso. Si el legítimo suscriptor del certificado deseara anular dicho proceso deberá enviar una respuesta firmada al mensaje de correo expresando este deseo.

#### **4.4.4. Periodo de gracia de la solicitud de revocación**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

#### **4.4.5. Circunstancias para la suspensión**

Son causas para la suspensión de un certificado emitido bajo esta Política:

1. Solicitud del firmante o un tercero autorizado.
2. Resolución judicial o administrativa que lo ordene
3. Existencia de dudas sobre el secreto de los datos de creación de firma del firmante.
4. Los certificados también se suspenden como parte del proceso de revocación para el caso de solicitudes sin origen verificado (por ejemplo, revocación del certificado a través de una llamada telefónica al call-center)

Clf.: <b>PUBLICO</b>	Ref.: PKIGVA-CP-07V2.0-c.doc	Versión: 2.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.7.2.0	Pág. 23 de 45

#### 4.4.6. Quien puede solicitar la suspensión

La suspensión de un certificado se puede iniciar tanto por el suscriptor del mismo como por parte de la propia Autoridad de Certificación de la Comunidad Valenciana.

#### 4.4.7. Procedimiento para la solicitud de suspensión

La suspensión de un certificado iniciada por el suscriptor deberá realizarse por vía telefónica, mediante llamada telefónica al número de soporte telefónico de la Autoridad de Certificación de la Comunidad Valenciana 902482481.

#### 4.4.8. Limites del periodo de suspensión

El período de suspensión de la vigencia de los certificados será normalmente de 15 días, salvo que la resolución judicial o administrativa que lo dictamine imponga un plazo superior o inferior, para lo cual, se estará al mismo.

#### 4.4.9. Frecuencia de emisión de CRLs

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

#### 4.4.10. Requisitos de comprobación de CRLs

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

#### 4.4.11. Disponibilidad de comprobación on-line de revocación/estado

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

#### 4.4.12. Requisitos de comprobación on-line de revocación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

Clf.: <b>PUBLICO</b>	Ref.: PKIGVA-CP-07V2.0-c.doc	Versión: 2.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.7.2.0	Pág. 24 de 45



#### 4.4.13. Otras formas de divulgación 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 URL [http://www.pki.gva.es/estado\\_c.htm](http://www.pki.gva.es/estado_c.htm)

#### 4.4.14. Requisitos de comprobación para otras formas de divulgación de revocación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

#### 4.4.15. Requisitos especiales de renovación de claves comprometidas

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

### 4.5. Procedimientos de Control de Seguridad

#### 4.5.1. Tipos de eventos registrados

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

#### 4.5.2. Frecuencia de procesado de logs

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

#### 4.5.3. Periodo de retención para los logs de auditoría

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

#### 4.5.4. Protección de los logs de auditoría

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

Clf.: <b>PUBLICO</b>	Ref.: PKIGVA-CP-07V2.0-c.doc	Versión: 2.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.7.2.0	Pág. 25 de 45

#### 4.5.5. Procedimientos de backup de los logs de auditoría

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

#### 4.5.6. Sistema de recogida de información de auditoría (interno vs externo)

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

#### 4.5.7. Notificación al sujeto causa del evento

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

#### 4.5.8. Análisis de vulnerabilidades

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

### 4.6. Archivo de registros

#### 4.6.1. Tipo de eventos registrados

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

#### 4.6.2. Periodo de retención para el archivo

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

#### 4.6.3. Protección del archivo

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

#### 4.6.4. Procedimientos de backup del archivo

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

Clf.: <b>PUBLICO</b>	Ref.: PKIGVA-CP-07V2.0-c.doc	Versión: 2.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.7.2.0	Pág. 26 de 45

#### 4.6.5. Requerimientos para el sellado de tiempo de los registros

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

#### 4.6.6. Sistema de recogida de información de auditoría (interno vs externo)

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

#### 4.6.7. Procedimientos para obtener y verificar información archivada

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

### 4.7. Cambio de Clave

No estipulado.

### 4.8. Recuperación en caso de compromiso de una clave o un desastre

#### 4.8.1. Alteración de los recursos hardware, software y/o datos

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

#### 4.8.2. La clave publica de una entidad se revoca

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

#### 4.8.3. La clave de una entidad se compromete

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

#### 4.8.4. 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 Autoridad de Certificación de la Comunidad Valenciana.

Clf.: <b>PUBLICO</b>	Ref.: PKIGVA-CP-07V2.0-c.doc	Versión: 2.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.7.2.0	Pág. 27 de 45

## 4.9. Cese de una CA

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

Clf.: <b>PUBLICO</b>	Ref.: PKIGVA-CP-07V2.0-c.doc	Versión: 2.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.7.2.0	Pág. 28 de 45

## **5. CONTROLES DE SEGURIDAD FÍSICA, PROCEDURAL Y DE PERSONAL**

### **5.1. Controles de Seguridad Física**

#### **5.1.1. Ubicación y construcción**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

#### **5.1.2. Acceso físico**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

#### **5.1.3. Alimentación eléctrica y aire acondicionado**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

#### **5.1.4. Exposición al agua**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

#### **5.1.5. Protección y prevención de incendios**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

#### **5.1.6. Sistema de almacenamiento**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

#### **5.1.7. Eliminación de residuos**

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

Clf.: <b>PUBLICO</b>	Ref.: PKIGVA-CP-07V2.0-c.doc	Versión: 2.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.7.2.0	Pág. 29 de 45

### 5.1.8. Backup remoto

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

## 5.2. Controles procedimentales

### 5.2.1. Papeles de confianza

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

### 5.2.2. Numero de personas requeridas por tarea

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

### 5.2.3. Identificación y autenticación para cada papel

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

## 5.3. Controles de seguridad de personal

### 5.3.1. Requerimientos de antecedentes, calificación, experiencia, y acreditación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

### 5.3.2. Procedimientos de comprobación de antecedentes

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

### 5.3.3. Requerimientos de formación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

Clf.: <b>PUBLICO</b>	Ref.: PKIGVA-CP-07V2.0-c.doc	Versión: 2.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.7.2.0	Pág. 30 de 45

#### 5.3.4. Requerimientos y frecuencia de la actualización de la formación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

#### 5.3.5. Frecuencia y secuencia de rotación de tareas

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

#### 5.3.6. Sanciones por acciones no autorizadas

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

#### 5.3.7. Requerimientos de contratación de personal

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

#### 5.3.8. Documentación proporcionada al personal

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

Clf.: <b>PUBLICO</b>	Ref.: PKIGVA-CP-07V2.0-c.doc	Versión: 2.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.7.2.0	Pág. 31 de 45

## 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 por parte de la Autoridad de Certificación de la Comunidad Valenciana, que no almacenará las vinculadas al certificado de firma.

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

Las claves privadas para los certificados emitidos bajo el ámbito de la presente Política de Certificación se encuentran en los ficheros con formato PKCS#12. Estos ficheros contienen las claves y los certificados de usuario en sendos ficheros cifrados.

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

La clave pública a ser certificada es generada por la Autoridad de Certificación, tras la recepción de una solicitud firmada del operador de la Autoridad de Registro.

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

La clave pública de la Autoridad de Certificación que emite el certificado del suscriptor se puede descargar de la URL [http://www.pki.gva.es/ca\\_c.htm](http://www.pki.gva.es/ca_c.htm)

Adicionalmente las claves públicas de todas las CA's pertenecientes a la jerarquía de confianza de PKIGVA se pueden descargar de la misma URL

#### 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.

Clf.: <b>PUBLICO</b>	Ref.: PKIGVA-CP-07V2.0-c.doc	Versión: 2.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.7.2.0	Pág. 32 de 45



### 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	Signature algorithm	Signature algorithm	Key generation algorithm	Padding method	Cryptographic hash	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	Signature algorithm	Signature algorithm	Key generation algorithm	Padding method	Cryptographic hash	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 Generalitat Valenciana.

### 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 *1.3.4 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 CRL*”.

## 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

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana

### 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

Se hace custodia de las claves vinculadas a los certificados de cifrado. No se custodian claves privadas de firma de los suscriptores de los certificados definidos por la presente política..

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

Para la custodia de las claves vinculadas a los certificados de cifrado la Autoridad de Certificación realiza una copia de seguridad de dichas claves.

### 6.2.5. Archivo de la clave privada

Para la custodia de las claves vinculadas a los certificados de cifrado la Autoridad de Certificación almacena la copia de seguridad de dichas claves referida en el punto anterior.

### 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 Autoridad de Certificación de la Comunidad Valenciana

### 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 PKCS#12.

Clf.: <b>PUBLICO</b>	Ref.: PKIGVA-CP-07V2.0-c.doc	Versión: 2.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.7.2.0	Pág. 34 de 45

#### 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 Autoridad de Certificación de la Comunidad Valenciana.

#### 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

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.

Clf.: <b>PUBLICO</b>	Ref.: PKIGVA-CP-07V2.0-c.doc	Versión: 2.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.7.2.0	Pág. 35 de 45

## 6.5. Controles de Seguridad Informática

### 6.5.1. Requerimientos técnicos de seguridad informática específicos

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

### 6.5.2. Valoración de la seguridad informática

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

## 6.6. Controles de Seguridad del Ciclo de Vida

### 6.6.1. Controles de desarrollo del sistema

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

### 6.6.2. Controles de gestión de la seguridad

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

### 6.6.3. Evaluación de la seguridad del ciclo de vida

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

## 6.7. Controles de Seguridad de la Red

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

## 6.8. Controles de Ingeniería de los Módulos Criptográficos

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

Clf.: <b>PUBLICO</b>	Ref.: PKIGVA-CP-07V2.0-c.doc	Versión: 2.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.7.2.0	Pág. 36 de 45

## 7. PERFILES DE CERTIFICADO Y CRL

### 7.1. Perfil de Certificado

Esta política de certificación especifica el uso de dos certificados distintos para firma digital y cifrado de datos. El perfil de ambos certificados es idéntico excepto en el apartado 7.1.2 Extensiones del certificado. En dicho punto se especifica cuando existen diferencias entre ambos certificados.

#### 7.1.1. Número de versión

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

#### 7.1.2. Extensiones del certificado

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

<b>Campo</b>	<b>Valor</b>
<b>Subject</b>	
SerialNumber	NIF del suscriptor. 9 caracteres completados a ceros por la izquierda.
GivenName	Nombre del suscriptor , tal como aparece en el DNI
SurName	Apellidos del suscriptor, tal como aparece en el DNI
CommonName	Cadena compuesta de la forma: NOMBRE APELLIDO1 APELLIDO2 – NIF:NIFDELSUSSCRIPTOR
OrganizationalUnit	Ciudadanos
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	CAGVA
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

Clf.: <b>PUBLICO</b>	Ref.: PKIGVA-CP-07V2.0-c.doc	Versión: 2.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.7.2.0	Pág. 37 de 45

<b>Extended Key Usage</b>	
	Client Authentication
	Email Protection
<b>CRL Distribution Point</b>	HTTP URI: <a href="http://www.pki.gva.es/gestcert/cagva.crl">http://www.pki.gva.es/gestcert/cagva.crl</a>
<b>SubjectAlternativeName</b>	
RFC822Name	Correo electrónico del suscriptor
DirectoryName	
	CN=Nombre Apellido1 Apellido2
	UID=NIF
<b>Certificate Policy Extensions</b>	
Policy OID	1.3.6.1.4.1.8149.3.7.2.0
Policy CPS Location	<a href="http://www.pki.gva.es/legislacion_c.htm">http://www.pki.gva.es/legislacion_c.htm</a>
Policy Notice	Certificado reconocido para Ciudadano expedido por la Autoridad de Certificación de la Generalitat Valenciana (Pl. Manises 1. CIF S4611001A). CPS y CP en <a href="http://www.pki.gva.es">http://www.pki.gva.es</a>
<b>Authority Information Access</b>	<a href="http://ocsp.pki.gva.es">http://ocsp.pki.gva.es</a>
<b>Fingerprint issuer</b>	714C 0354 F272 6B5C 8D1E 71D4 5882 0DD7 1F57 B7DD
<b>Algoritmo de hash</b>	SHA-1
<b>KeyUsage (críticos)</b>	
Certificado de Firma	Digital Signature
Certificado de Cifrado	Key Encipherment Data 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 bajo la presente política contienen el distinguished name X.500 del emisor y el suscriptor del certificado en los campos issuer name y subject name respectivamente.

Clf.: <b>PUBLICO</b>	Ref.: PKIGVA-CP-07V2.0-c.doc	Versión: 2.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.7.2.0	Pág. 38 de 45

- Subject name: cn=*NOMBRE APELLIDO1 APELLIDO2* – NIF:*nif*, ou=Ciudadanos, o=Generalitat Valenciana, c=ES

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.

- Issuer name: cn=CAGVA, ou=PKIGVA, o=Generalitat Valenciana, c=ES

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

1.3.6.1.4.1.8149.3.7.2.0

#### 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 la Autoridad de Certificación asocia explícitamente con el certificado. Adicionalmente la extensión contiene un cualificador de la política y una dirección URL de localización de la misma.

### 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 (v2).

#### 7.2.2. CRL y extensiones

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

Clf.: <b>PUBLICO</b>	Ref.: PKIGVA-CP-07V2.0-c.doc	Versión: 2.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.7.2.0	Pág. 39 de 45

## 8. ESPECIFICACIÓN DE LA ADMINISTRACIÓN

### 8.1. Procedimientos de Especificación de Cambios

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Comunidad Valenciana.

### 8.2. Procedimientos de Publicación y Notificación

Cuando se realicen modificaciones significativas en la presente Política de Certificación éstas se notificarán mediante correo electrónico, a los suscriptores de los certificados afectados.

En el caso de modificaciones significativas en la Declaración de Prácticas de Certificación de la Autoridad de Certificación de la Comunidad Valenciana la notificación se hará extensiva a los suscriptores de todos los certificados emitidos.

Adicionalmente las modificaciones se harán públicas en el sitio web de la Autoridad de Certificación en <http://www.pki.gva.es>

Esta notificación se realizará con anterioridad a la entrada en vigor de la modificación que la haya producido.

### 8.3. Procedimientos de Aprobación de la CPS

La Autoridad de Certificación es la entidad encargada de la aprobación en el momento de su creación de la presente Política de Certificación (CP), así como de la Declaración de Prácticas de Certificación (CPS).

La Autoridad de Certificación también se encarga de aprobar y autorizar las modificaciones de dichos documentos.

Las funciones y competencias de la Autoridad de Certificación corresponden a la Secretaría Autónoma de Telecomunicaciones y Sociedad de la Información.

Clf.: <b>PUBLICO</b>	Ref.: PKIGVA-CP-07V2.0-c.doc	Versión: 2.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.7.2.0	Pág. 40 de 45





**CONTRATO DE CERTIFICACIÓN - CÓDIGO 1.3.6.1.4.1.8149.3.7.2.0****Condiciones de utilización de los certificados**

1. Los certificados asociados a la Política de Certificación para Certificados Reconocidos en soporte software para Ciudadanos, emitidos por la Generalitat Valenciana son del tipo X.509v3 y se rigen por la Declaración de Prácticas de Certificación de la Generalitat Valenciana, en tanto que Prestador de Servicios de Certificación, así como por la Política de Certificación referida. Ambos documentos se deben interpretar según la legislación de la Comunidad Europea, el Ordenamiento Jurídico Español y la legislación propia de la Generalitat Valenciana.
2. Los solicitantes deberán ser personas físicas, en posesión de un NIF, un NIE u otro documento de identificación válido en Derecho.
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. El titular del certificado es responsable de la custodia de su clave privada y de comunicar a la mayor brevedad posible cualquier pérdida o sustracción de esta clave.
5. El titular 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.pki.gva.es>.
6. La Generalitat Valenciana, en tanto que Prestador de Servicios de Certificación, no se responsabiliza del contenido de los documentos firmados haciendo uso de los certificados por ella emitidos.
7. La Generalitat Valenciana, en tanto que Prestador de Servicios de Certificación, 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 Generalitat Valenciana y en la Política de Certificación asociada a este tipo de certificados.
8. El periodo de validez de estos certificados es de tres (3) 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 y por fallecimiento del titular 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 los solicitantes será el Documento Nacional de Identidad, NIE o Pasaporte válido y vigente.
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 Secretaría Autónoma de Telecomunicaciones y Sociedad de la Información de la Conselleria de Infraestructuras y Transporte. La finalidad de dicho fichero es la servir a los usos relacionados con los servicios de certificación prestados por la Generalitat Valenciana. 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 Secretaría Autónoma de Telecomunicaciones y Sociedad de la Información 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 Secretaría Autónoma de Telecomunicaciones y Sociedad de la Información, a través de cualquiera de los Registros de Entrada de la Generalitat Valenciana 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 Autoridad de Certificación.

Ejemplar para el solicitante - Reverso

Clf.: <b>PUBLICO</b>	Ref.: PKIGVA-CP-07V2.0-c.doc	Versión: 2.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.7.2.0	Pág. 42 de 45

**CONTRATO DE CERTIFICACIÓN - CÓDIGO 1.3.6.1.4.1.8149.3.7.2.0****Secció 1 – Dades del subscriptor / Sección 1 – Datos del suscriptor**Cognoms/*Apellidos*:Nom/*Nombre*:

DNI/NIF:

Tel.:

Adreça de correu electrònic/*Dirección correo electrónico*:Adreça postal/*Dirección postal*:**Secció 2 – Dades del operador del Punt de Registre / Sección 2 – Datos del operador del Punto de Registro**Nom i cognoms/*Nombre y Apellidos*:**Secció 3 - Data i Firma / Sección 3 – Fecha y Firma**

Subscriu el present contracte de certificació associat a la Política de Certificació de Certificats Reconeguts en suport software per a ciutadans amb codi 1.3.6.1.4.1.8149.3.7, emés per la Generalitat Valenciana. Declare que conec i accepte les normes d'utilització d'este tipus de certificats que es troben exposades en <http://www.pki.gva.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 Reconocidos en soporte software para Ciudadanos con código 1.3.6.1.4.1.8149.3.7, emitido por la Generalitat Valenciana. Declaro conocer y aceptar las normas de utilización de este tipo de certificados que se encuentran expuestas en <http://www.pki.gva.es>. Declaro, asimismo, que los datos puestos de manifiesto son ciertos.*

Firma del subscriptor  
*Firma del suscriptor*Firma i segell del Punt de Registre  
*Firma y sello del Punto de Registro*Firmat/*Firmado*:Firmat/*Firmado*:

Nº de petició

Exemplar per a la Generalitat Valenciana / *Ejemplar para la Generalitat Valenciana*

Clf.: <b>PUBLICO</b>	Ref.: PKIGVA-CP-07V2.0-c.doc	Versión: 2.0
Est.: APROBADO	OID: 1.3.6.1.4.1.8149.3.7.2.0	Pág. 43 de 45



