Conselleria de Justícia I Administracions Públiques

Autoritat de Certificació de la Comunitat Valenciana

Certificados para Servidores de VPN

Fecha: 14 de noviembre de 2.007	**Versión:** 2.0
Estado: APROBADO	**Nº de páginas:** 1
OID: 1.3.6.1.4.1.8149.3.8.2.0	**Clasificación: PUBLICO**
Archivo: PKIGVA-CP-08V2.0-c2007.doc	
Preparado por: ACCV	

Control de Versiones

Versión	Autor	Fecha	Observaciones
1.0	José Antonio Amador	01/12/2003	Documento original, primera versión
1.1	Javier Vilalta	10/08/2007	Adaptación a DGM.
1.2	Javier Vilalta	21/09/2007	Adaptación a Ens
2.0	José Antonio Amador	14/11/2007	Adpatación nuevo perfil

Revisión de este documento:

Creado por: Fecha:	Supervisado por: Fecha:	Vº.Bº Cliente: Fecha

Tabla de Contenido

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 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.

1.1. 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 Autoritat de Certificació de la Comunitat Valenciana (ACCV) y las reglas de solicitud, adquisición gestión y uso de los certificados.

La Política de Certificación referida en este documento se utilizara para dotar de identidad a los servidores de *Redes Privadas Virtuales* (en adelante VPN) en el ámbito de la Generalitat Valenciana y de entidades y organismos con los quehaya establecido convenio de certificación.

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 con los que haya establecido convenio de certificación.

1.2. Identificación

Nombre de la política	Certificados para Servidores de VPN
Calificador de la política	El uso de este certificado está restringido a Servidores de VPN pertenecientes a la Generalitat Valenciana, a entidades y organismos vinculados a ella, o a alguna Administración Pública con la que haya establecido convenio de certificación
Versión de la política	2.0

Estado de la política	Vigente
Referencia de la política / OID (Object Identifier)	1.3.6.1.4.1.8149.3.8.2.0
Fecha de emisión	No aplicable
Fecha de expiración	No aplicable.
CPS relacionada	Declaración de Prácticas de Certificación (CPS) de la PKI de la Generalitat Valenciana. Versión 1.9 OID: 1.3.6.1.4.1.8149.2.1.0 Disponible en http://www.accv.es/cps
Localización	Esta Política de certificación se puede encontrar en: http://www.accv.es/legislacion_c.htm

1.3. Comunidad y Ámbito de aplicación

1.3.1.Autoridades de Certificación

La CA que puede emitir certificados acordes con esta política es la “ACCV-CA2” perteneciente a la Autoritat de Certificació de la Comunitat Valenciana.

1.3.2.Autoridades de Registro

La Autoridad de Registro que gestiona este tipo de certificados es el Ente Prestador de Servicios de Certificación Electrónica de la Comunitat Valenciana, en adelante, la Autoritat de Certificació de la Comunitat Valenciana, perteneciente a la Conselleria de Justícia i Administracions Públiques.

1.3.3.Entidades Finales

1.3.3.1. Subscriptores

El grupo de usuarios que pueden solicitar certificados definidos por esta política está limitado exclusivamente al compuesto por el conjunto Jefes de Servicio (o cargos superiores) de la Generalitat Valenciana y puestos organizativos equivalentes en organismos con lo que haya firmado algún convenio de certificación, siendo éstos los responsables últimos de su uso dentro de los distintos proyectos.

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 VPN en el ámbito de la verificación de la identidad del servidor al que se conectan.
- Las aplicaciones y servicios con capacidades de VPN, en el ámbito de verificación de la identidad de los servidores a los que se conectan.

1.3.4.Ámbito de aplicación

1.3.4.1. Usos Permitidos

Los certificados emitidos por la Autoritat de Certificació de la Comunitat Valenciana bajo esta Política de Certificación, pueden utilizarse para dotar de identidad a los Servidores de VPN .

1.3.4.2. Usos Restringidos

No se han establecido usos restringidos para este tipo de certificados

1.3.4.3. Usos Prohibidos

Esta prohibido el uso de los certificados emitidos por la Autoritat de Certificació de la Comunitat 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 de la Autoritat de Certificació de la Comunitat Valenciana por sus competencias como Ente Prestador de Servicios de Certificación Electrónica de la Comunitat Valenciana.

Nombre	*Autoritat de Certificació de la Comunitat Valenciana* *Conselleria de justícia i Administracions Públiques*
Dirección de email	accv@accv.es
Dirección	*Plaza Cánovas del Castillo, 1- 46005 Valencia (Spain)*
Número de teléfono	*+34·902 482484*
Número de fax	*+34·96·196 1080*

1.4.1.Persona de Contacto

Para más información relacionada con la presente Política de Certificación remitirse a los datos de contacto del punto anterior.

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

La Dirección General de Modernización 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 la Ley 14/2005, de 23 de diciembre, de la Generalitat, de Medidas Fiscales, de Gestión Financiera y Administrativa, y de Organización de la Generalitat. Capítulo XXVI. De la creación del Ente Prestador de Servicios de Certificación Electrónica de la Comunidad Valenciana, y el Decreto 122/2007, de 23 de julio, del Consell, por el que se regula el Reglamento Orgánico y Funcional de la Conselleria de Justicia y Administraciones Públicas.

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 ACCV.

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 ACCV.

2.1.3.Obligaciones de los Subscriptores

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

2.1.4.Obligaciones de las partes confiantes

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

2.1.5.Obligaciones del repositorio

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

2.2. Responsabilidad

2.2.1.Responsabilidad de la CA

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

2.2.2.Responsabilidad de la RA

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

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 ACCV.

2.3.2.Relaciones fiduciarias

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

2.3.3.Procesos administrativos

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

2.4. Interpretación y Ejecución

2.4.1.Leyes gubernamentales

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

2.4.2.Extinción, subsistencia, fusión, y notificación

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

2.4.3.Procedimientos de resolución de disputas

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

2.5. Tarifas

2.5.1.Tarifas de emisión de certificado o renovación

Los precios para la emisión inicial y la renovación de los certificados a los que se refiere la presente política de certificación se recogen en la Lista de Tarifas de la Autoritat de Certificació de la Comunitat Valenciana. Esta Lista se publica en la página web de la ACCV www.accv.es

2.5.2.Tarifas de acceso a los certificados

El acceso a los certificado emitidos bajo esta política, dada su naturaleza pública, 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 certificado 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

No se prevé ningún reintegro de las cantidades aportadas para la emisión de este tipo de certificados.

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 ACCV.

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.

2.6.2.Frecuencia de publicación

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

2.6.3.Controles de acceso

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

2.6.4.Repositorios

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la Autoritat de Certificació de la Comunitat Valenciana

En cualquier caso tanto los certificados emitidos bajo esta política como la CRL se encuentran en el directorio LDAP de la Autoritat de Certificació de la Comunitat Valenciana en "ldap://ldap.pkigva.es" bajo la base de búsqueda "ou=VPN, o=Generalitat Valenciana, c=es"

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 ACCV.

2.7.2.Identificación/cualificación del auditor

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

2.7.3.Relación entre el auditor y la entidad auditada

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

2.7.4.Tópicos cubiertos por el control de conformidad

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

2.7.5.Acciones a tomar como resultado de una deficiencia

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

2.7.6.Comunicación de resultados

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

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 ACCV.

2.8.2.Tipo de información no considerada confidencial

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

2.8.3.Divulgación de información de revocación /suspensión de certificados

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

2.8.4.Envío a la autoridad judicial y/o policial

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

2.8.5.Publicación como parte de un descubrimiento civil

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

2.8.6.Divulgación a petición del propietario

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

2.8.7.Otras circunstancias de publicación de información

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

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 Autoritat de Certificació de la Comunitat Valenciana.

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 ACCV.

3.1.2.Necesidad de los nombres de ser significativos

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

3.1.3.Reglas para interpretar varios 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 certificado se emitirá con el nombre completo (nombre del servidor más dominio) al que responda el servidor VPN. Este nombre debe ser único en la red. No se aceptarán nombres parciales.

CN = NOMBRE DEL SISTEMA + DOMINIO AL QUE PERTENECE

3.1.5.Procedimientos de resolución de disputas de nombres

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

3.1.6.Reconocimiento, autentificación y función de las marcas registradas

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

3.1.7.Métodos de prueba de posesión de la clave privada

Dado que el solicitante es el que genera el par de claves y sólo entrega a la Autoridad de Certificación un fichero en formato PKCS#10 de solicitud de certificado, la prueba de posesión de la clave privada no es precisa: sólo si dispone de la clave privada le será de utilidad el fichero PKCS#10 firmado, que es el certificado digital.

3.1.8.Autentificación 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.

En el caso que el solicitante pertenezca al ámbito de la Generalitat Valenciana se validará su solicitud con la información de la Guía de Personas y Servicios relativa a esa persona.

En caso de no pertenecer a la Generalitat Valenciana, el solicitante deberá adjuntar la publicación del nombramiento (Boletín Oficial del Estado) o documento de toma de posesión del puesto ocupado o certificado del órgano encargado de gestión de personal de su organización, donde se indique claramente su puesto y responsabilidad.

3.1.9.Autentificación de la identidad de un individuo

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

3.2. Renovación rutinaria de la clave

La autenticación para la renovación del certificado se puede realizar utilizando las técnicas para la autenticación e identificación inicial, o sea utilizando solicitudes firmadas digitalmente, sistema con el que queda perfectamente identificado el solicitante de la renovación.

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.

3.4. Solicitud de revocación

La solicitud de revocación se puede realizar por medio de los mecanismos siguientes:

- Solicitud de revocación firmada digitalmente por la persona responsable del certificado utilizando la aplicación de gestión de certificados no personales de la Autoritat de Certificació de la Comunitat Valenciana https://npsc.accv.es:8450/npschttps://npsc.accv.es:8450/npsc
- Solicitud de revocación por la persona responsable del certificado, a través del teléfono de asistencia 902 482 481

La Autoritat de Certificació de la Comunitat 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 o cualquier otro hecho que recomendará emprender dicha acción.

4. REQUERIMIENTOS OPERACIONALES

4.1. Solicitud de certificados

El solicitante de un certificado acogido a la presente Política de Certificación deberá cumplimentar una solicitud de certificación a través de la aplicación de gestión de certificados no personales (NPSC) ubicado en https://npsc.accv.es:8450/npschttps://npsc.accv.es:8450/npsc, en el que podrá incrustar el fichero PKCS#10 generado por el solicitante.

Una vez cumplimentado el formulario de solicitud este se envía, firmado con un certificado digital reconocido admitido por la Autoritat de Certificació de la Comunitat Valenciana.

Es atribución de la Autoridad de Registro 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 un correo electrónico en la dirección que hizo constar en su solicitud, informándole de los motivos del rechazo de la misma.

4.2. Emisión de certificados

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 se determina la naturaleza y la forma de realizar dichas comprobaciones es esta Política de Certificación.

Tras la emisión del certificado, la Autoridad de Registro lo notificará al subscriptor del mismo mediante el envío de un correo electrónico firmado a la dirección que figure en la solicitud. El usuario debera entrar en la aplicación de gestión de certificados no personales (NPSC) ubicada en https://npsc.accv.es:8450/npsc para recoger el certificado, firmando previamente el Contrato de Certificación en dicha aplicación con su certificado personal reconocido.

El Contrato de Certificación es un documento que debe ser firmado electrónicamente por el solicitante, y cuyo fin es vincularlo con la acción de la solicitud, con el conocimiento de las normas de uso y con la veracidad de los datos presentados.

4.3. Aceptación de certificados

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

4.4. Suspensión y revocación de certificados

4.4.1.Circunstancias para la revocación

Los certificados emitidos por la Autoritat de Certificació de la Comunitat Valenciana se revocarán o extinguirán su vigencia en los siguientes casos:

- Expiración del período de validez que figura en el certificado.
- Revocación formulada por el firmante, la persona representada por éste o un tercero autorizado.
- Violación o puesta en peligro del secreto de los datos de creación de firma del firmante o de la Autoritat de Certificació de la Comunitat Valenciana o utilización indebida de estos datos por un tercero
- Resolución judicial o administrativa que lo ordene
- Fallecimiento o incapacidad sobrevenida, total o parcial, del firmante
- Cese de la actividad de la Autoritat de Certificació de la Comunitat 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 en el servicio de consulta sobre la vigencia de los certificados de la Autoritat de Certificació de la Comunitat Valenciana.

4.4.2.Quién puede solicitar la revocación

La revocación de un certificado se puede iniciar tanto por el subscriptor del mismo como por parte de la Autoritat de Certificació de la Comunitat Valenciana.

Los subscriptores de certificados pueden solicitar su revocación por cualquier razón o sin ninguna razón y deben solicitar la revocación bajo las condiciones especificadas en el siguiente apartado.

4.4.3.Procedimiento de solicitud de revocación

Se determina que:

- Se aceptarán solicitudes de revocación remotas si están firmadas digitalmente con un certificado de la Autoritat de Certificació de la Comunitat Valenciana y presenciales si se cumplen los requisitos de identificación del usuario establecidos para el registro inicial.
- En el caso de producirse una solicitud de revocación sin posible verificación de la identidad del solicitante (telefónica, correo electrónico sin firma digital,…), se procederá a la suspensión 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 del certificado. Es importante reseñar que el certificado no será utilizable desde el momento del procesamiento de la solicitud.

- Tras la revocación del certificado el subscriptor del mismo deberá destruir la clave privada que se corresponda con la pública contenida en el certificado.

Una solicitud de revocación tanto si se realiza en papel o de forma electrónica (ej.: correo electrónico) debe contener la información siguiente:

Solicitud de revocación de certificado Fecha : _____

Sección 1 – Detalles del certificado (si se conocen)

ID certificado: .....

Número de serie del certificado:.....

Tipo de certificado: .....

Sección 2 – Datos del suscriptor del certificado

Nombre: .....

NIF: .....

Sección 3 – Motivo de la revocación *

.....

.....

.....

.....

.....

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

Sección 4 – Autorización

Autorizado por:
- ❑ Subscriptor del certificado
- ❑ Tercera parte autorizada (especificar)

……

Firma: .....

4.4.4.Periodo de gracia de la solicitud de revocación

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

4.4.5.Circunstancias para la suspensión

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

4.4.6.Quien puede solicitar la suspensión

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

4.4.7.Procedimiento para la solicitud de suspensión

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

4.4.8.Límites del periodo de suspensión

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

4.4.9.Frecuencia de emisión de CRLs (si aplicable)

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

4.4.10.Requisitos de comprobación de CRLs

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

Las CRLs con la información de revocación de los certificados emitidos al amparo de esta Política de Certificación se pueden encontrar en el directorio LDAP de la Autoritat de Certificació de la Comunitat Valenciana en la siguiente dirección *ldap:///ldap.pki.gva.es* bajo la base de búsqueda *"o=Generalitat Valenciana, c=es"*

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

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

El estado de los certificados emitidos en bajo el amparo de esta política de certificación se puede comprobar haciendo uso del servidor OCSP que se localiza en la siguiente dirección de Internet: *ocsp.pki.gva.es:80*

4.4.12.Requisitos de comprobación on-line de revocación

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

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 Autoritat de Certificació de la Comunitat Valenciana (http://www.accv.es).

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 ACCV.

4.4.15.Requisitos especiales de renovación de claves comprometidas

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

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 ACCV.

4.5.2.Frecuencia de procesado de logs

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

4.5.3.Periodo de retención para los logs de auditoría

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

4.5.4.Protección de los logs de auditoría

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

4.5.5.Procedimientos de backup de los logs de auditoría

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

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 ACCV.

4.5.7.Notificación al sujeto causa del evento

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

4.5.8.Análisis de vulnerabilidades

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

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 ACCV.

4.6.2.Periodo de retención para el archivo

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

4.6.3.Protección del archivo

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

4.6.4.Procedimientos de backup del archivo

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

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 ACCV.

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 ACCV.

4.6.7.Procedimientos para obtener y verificar información archivada

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

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 ACCV.

4.8.2.La clave publica de una entidad se revoca

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

4.8.3.La clave de una entidad se compromete

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

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 ACCV.

4.9. Cese de una CA

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

4.10. Caducidad de las claves de certificado de CA.

La ACCV evitará generar certificados de subscriptor que caduquen con posterioridad a los certificados de CA. Para ello no se emitirán certificados de subscriptor cuyo periodo de validez exceda el del certificado de CA en cuestión.

La ACCV, en los casos que sea necesario, creara con anterioridad la CA que asumira la emisión de certificados asociados a esta política.

5. CONTROLES DE SEGURIDAD FÍSICA, PROCEDURAL Y DE PERSONAL

5.1. Controles de Seguridad Física

5.1.1.Ubicación y construcción

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

5.1.2.Acceso físico

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

5.1.3.Alimentación eléctrica y aire acondicionado

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

5.1.4.Exposición al agua

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

5.1.5.Protección y prevención de incendios

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

5.1.6.Sistema de almacenamiento

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

5.1.7.Eliminación de residuos

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

5.1.8.Backup remoto

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

5.2. Controles procedimentales

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 autentificación para cada papel

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

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 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 la 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.

6. CONTROLES DE SEGURIDAD TÉCNICA

6.1. Generación e Instalación del Par de Claves

6.1.1.Generación del par de claves

El par de claves para los certificados emitidos bajo el ámbito de la presente Política de Certificación se generan por el subscriptor del certificado.

6.1.2.Entrega de la clave privada a la entidad

La clave privada se genera por parte del subscriptor y, por tanto, no procede hacerle entrega de la misma.

6.1.3.Entrega de la clave publica al emisor del certificado

La clave pública generada por el subscriptor se le entrega a la Autoritat de Certificació de la Comunitat Valenciana para la emisión del certificado contenida en el fichero PKCS #10 generado por el solicitante y firmado con su clave personal que es enviado mediante la aplicación de gestión de certificados no personales (NPSC) ubicada en https://npsc.accv.es:8450/npsc.

La clave pública firmada por la Autoritat de Certificació de la Comunitat Valenciana se entrega al subscriptor contenida en el certificado digital que se le proporciona.

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 subscriptor se pueden descargar del sitio web http://www.accv.es .

Adicionalmente las claves públicas de todas las CA's pertenecientes a la jerarquía de confianza de la Autoritat de Certificació de la Comunitat Valenciana se pueden descargar del sitio web http://www.accv.es .

6.1.5.Tamaño de las claves

Las claves de la Root CA y ACCV-CA2 son claves RSA de 2048 bits de longitud

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

No aplicable.

6.1.7.Comprobación de la calidad de los parámetros

No aplicable.

6.1.8.Hardware/software de generación de claves

La generación de la clave la realiza el subscriptor del certificado por sus propios medios y por tanto a él corresponde la selección del soporte de la misma.

6.1.9.Fines del uso de la clave

La clave definida por la presente política se utilizará para la verificación del código de aplicaciones, o de partes de ellas en el ámbito de la Generalitat Valenciana. Para los certificados X.509 v3, este propósito se mapeará en las extensiones "*Key Usage*" y *"Extended Key Usage*" del siguiente modo:

Key Usage:

- Digital Signature
- Data Encipherment
- Key Encipherment
- Key Agreement

Extended Key Usage

- Server Authentication
- Client Authentication
- IPSEC Tunel
- IPSEC End System
- IPSEC User

La definición detallada del perfil de certificado y los usos de las claves se encuentra en el apartado 7 "*Perfiles de certificado y CRL*" de este documento.

6.2. Protección de la Clave Privada

6.2.1.Estándares para los módulos criptográficos

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

6.2.2.Control multipersona (n de entre m) de la clave privada

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

6.2.3.Custodia de la clave privada

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

6.2.4.Copia de seguridad de la clave privada

La clave privada es generada por el suscriptor y nunca está en posesión de la Autoritat de Certificació de la Comunitat Valenciana. Por lo tanto este apartado no procede.

6.2.5.Archivo de la clave privada

La clave privada es generada por el suscriptor y nunca está en posesión de la Autoritat de Certificació de la Comunitat Valenciana. Por lo tanto este apartado no procede.

6.2.6.Introducción de la clave privada en el módulo criptográfico

La clave privada es generada por el suscriptor y nunca está en posesión de la Autoritat de Certificació de la Comunitat Valenciana. Por lo tanto este apartado no procede.

6.2.7.Método de activación de la clave privada

La clave privada es generada por el suscriptor y nunca está en posesión de la Autoritat de Certificació de la Comunitat Valenciana. Por lo tanto este apartado no procede.

6.2.8.Método de desactivación de la clave privada

La clave privada es generada por el suscriptor y nunca está en posesión de la Autoritat de Certificació de la Comunitat Valenciana. Por lo tanto este apartado no procede.

6.2.9.Método de destrucción de la clave privada

La clave privada es generada por el suscriptor y nunca está en posesión de la Autoritat de Certificació de la Comunitat Valenciana. Por lo tanto este apartado no procede.

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.

El certificado de “ACCV-CA2” es válido desde el día 4 de mayo de 2006 hasta el 1 de mayo de 2016.

6.4. Datos de activación

6.4.1.Generación y activación de los datos de activación

El par de claves para este tipo de certificado es generado por el suscriptor y nunca está en posesión de la Autoritat de Certificació de la Comunitat Valenciana. Por lo tanto este apartado no procede.

6.4.2.Protección de los datos de activación

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

6.4.3.Otros aspectos de los datos de activación

No estipulado.

6.5. Controles de Seguridad Informática

6.5.1.Requerimientos técnicos de seguridad informática específicos

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

6.5.2.Valoración de la seguridad informática

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

6.6. Controles de Seguridad del Ciclo de Vida

6.6.1.Controles de desarrollo del sistema

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

6.6.2.Controles de gestión de la seguridad

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

6.6.3.Evaluación de la seguridad del ciclo de vida

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

6.7. Controles de Seguridad de la Red

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

6.8. Controles de Ingeniería de los Módulos Criptográficos

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

7. PERFILES DE CERTIFICADO Y CRL

7.1. Perfil de Certificado

7.1.1.Número de versión

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

7.1.2.Extensiones del certificado

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

- Key Usage {joint-iso-itu-t(2) ds(5) certificateExtension(29) keyUsage(15)}

  Marcada como crítica y con la siguiente combinación de valores:

  - Digital Signature
  - Data Enciphement
  - Key Enciphement
  - Key Agreement

- Extended Key Usage {joint-iso-itu-t(2) ds(5) certificateExtension(29) extKeyUsage(37)}

  Marcada como crítica y con la siguiente combinación de valores:

  - Server Authentication
  - Client Authentication
  - IPSEC Tunel
  - IPSEC End System
  - IPSEC User

- Certificate Policies. {joint-iso-itu-t(2) ds(5) certificateExtension(29) certificatePolicies(32)}

  Marcada como crítica y con la siguiente combinación de valores:

  - Policy OID: 1.3.6.1.4.1.8149.3.8.2.0
  - Policy CPS Location: http://www.accv.es/legislacion_c.htm

- Policy Notice: El uso de este certificado está restringido a Servidores VPN pertenecientes a la Generalitat Valenciana y con los que haya establecido convenio de certificación.

- Subject Alternative Name {joint-iso-itu-t(2) ds(5) certificateExtension(29) subjectAltName(17)}

  Marcada como no crítica y con el valor:

  - Nombre RFC822: Dirección de correo electrónico del subscriptor.
  - Directory name: uid=*NIF*, cn=Nombre|Primer apellido|Segundo apellido

- CRL Distribution Point {joint-iso-itu-t(2) ds(5) certificateExtension(29) cRLDistributionPoints(31)}

  Marcada como no crítica.

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 subscriptor del certificado en los campos issuer name y subject name respectivamente.

- Subject name: cn=*Nombre Completo del Servidor*, ou=VPN, 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”.

- Issuer name: cn=ACCV-CA2, 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 la Autoritat de Certificació de la Comunitat Valenciana para identificar la presente política es el siguiente: 1.3.6.1.4.1.8149.3.8.2.0

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 critica “Certificate Policy”

La extensión “*Certificate Policy*” identifica la política que define las Prácticas que la Autoritat de Certificació de la Comunitat Valenciana 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.

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 Autoritat de Certificació de la Comunitat 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 subscriptores de los certificados afectados.

En el caso de modificaciones significativas en la Declaración de Prácticas de Certificación de la Autoritat de Certificació de la Comunitat Valenciana la notificación se hará extensiva a los subscriptores de todos los certificados emitidos.

Adicionalmente las modificaciones se harán públicas en el sitio web de la Autoritat de Certificació de la Comunitat Valenciana en http://www.accv.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 Autoritat de Certificació de la Comunitat Valenciana.

Anexo I

CONTRATO DE CERTIFICACIÓN – CÓDIGO 1.3.6.1.4.1.8149.3.8.2.0

Sección 1 – Datos del solicitante

Apellidos: .....

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

Organismo / Servicio: .....

Organización (si es diferente a Generalitat Valenciana): .....

Dirección correo electrónico: .....

Dirección postal: ..... Tel.: .....

Sección 2 – Datos del Sistema informático a certificar

Nombre cualificado: .....

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

Dirección IP: .....

Sección 4 – Fecha y Firma

Solicito el Certificado asociado a la Política de Certificación con código 1.3.6.1.4.1.8149.3.8.2.0, para Servidores de VPN, emitido por la Autoritat de Certificació de la Comunitat Valenciana. Declaro conocer y aceptar las normas de utilización de este tipo de certificados que se encuentran expuestos en **http://www.accv.es**. Declaro, asimismo, que los datos expuestos son verdaderos.

En ..... a ..... de ..... de 2.00...

Firma del solicitante

Fdo.:

CONTRATO DE CERTIFICACIÓN – CÓDIGO 1.3.6.1.4.1.8149.3.8.2.0
Condiciones de utilización de los certificados

1. Los certificados asociados a la la Política de Certificación para Servidores de VPN, emitidos por la Autoritat de Certificació de la Comunitat Valenciana son del tipo X.509v3 y se rigen por la Declaración de Prácticas de Certificación de la Autoritat de Certificació de la Comunitat 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.accv..es**.

6. La Generalitat Valenciana, en tanto que Prestador de Servicios de Certificación, no se responsabiliza del funcionamiento de los servidores informáticos que hacen uso de los certificados emitidos.

7. La Autoritat de Certificació de la Comunitat 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 identificación de los solicitantes se hará en base a su certificado digital personal expedido por la Autoritat de Certificació de la Comunitat Valenciana o por algún otro Prestador de Servicios de Certificación reconocido con los que se haya conveniado para establecer el reconocimiento de sus certificados.

11. En cumplimiento de la ley 15/1.999, de 13 de diciembre, de Protección de Datos de Carácter Personal, se informa al solicitante de la existencia de un fichero automatizado de datos de carácter personal creado bajo la responsabilidad de la Autoritat de Certificació de la Comunitat Valenciana y la Conselleria de Justícia y Administraciones Públicas. La finalidad de dicho fichero es la servir a los usos relacionados con los servicios de certificación prestados por la Autoritat de Certificació de la Comunitat 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 Dirección general de Modernización 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 Autoritat de Certificació de la Comunitat Valenciana, a través de cualquiera de los Registros de Entrada de la Generalitat Valenciana e indicando claramente esta voluntad