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

Autoritat de Certificació de la Comunitat Valenciana

Declaraciónde Prácticas de Certificación (CPS) de la ACCV

Fecha: 20 de octubre de 2004	**Versión:** 1.6
Estado: APROBADO	**Nº de páginas:** 63
OID: 1.3.6.1.4.1.8149.2.1.6	**Clasificación: PUBLICO**
Archivo: ACCV-CPS-V1.6.doc	
Preparado por: ACCV	

Tabla de Contenido

1. INTRODUCCIÓN

Dentro del proceso de Modernización de las Administraciones Públicas valencianas, el Segundo Plan de Modernización de la Comunidad Valenciana hace una apuesta firme por la implantación de la teleadministración en la Generalitat Valenciana, lo que hace necesario reglamentar el proceso de firma electrónica dentro del marco de nuestra Administración.

Se pretende adoptar así una normativa de desarrollo del Real Decreto Ley estatal, como medida para garantizar la seguridad jurídica y la implantación de la firma electrónica en el ámbito de las relaciones entre la Administración y ésta con el ciudadano, en la Comunidad Valenciana. Igualmente se impone la necesidad de desarrollar una Autoridad de Certificación propia en la Generalitat Valenciana, dotándola de la infraestructura necesaria para la emisión y gestión de claves y certificados para la utilización de la firma electrónica avanzada. Se crea así, mediante Decreto 87/2002, de 30 de mayo, del Gobierno Valenciano, la Autoridad de Certificación de la Comunidad Valenciana (ACCV). Mediante este Decreto, la Generalitat Valenciana se constituye en prestador de servicios de certificación de firma electrónica avanzada de acuerdo con lo previsto en la Ley de Firma Electrónica, para lo cual se ha dotado de una Infraestructura de Clave Pública (PKI), entendida como un conjunto de equipamiento y aplicaciones informáticas necesarias para la emisión y gestión de claves y certificados reconocidos.

El uso y la implantación de la firma electrónica en la Generalitat Valenciana se basará en lo siguientes principios y criterios de actuación:

a) Seguridad: en las relaciones telemáticas, y en concreto, en el funcionamiento de la Red Corporativa de Telecomunicaciones de la Administración de la Generalitat Valenciana.

b) Integridad de las comunicaciones telemáticas en las que se emplee la firma electrónica.

c) Autenticidad y conservación de los documentos generados.

d) Publicidad de las aplicaciones informáticas que empleen firma electrónica.

e) Objetividad, transparencia y no discriminación en la prestación de servicios de certificación de firma electrónica avanzada y firma electrónica reconocida.

1.1. Vista General

Este documento presenta la Declaración de Practicas de Certificación (CPS) que rigen el funcionamiento y operaciones de la Infraestructura de Clave Pública de la Generalitat Valenciana (desde ahora PKIGVA), que da soporte a la Autoridad de Certificación de la Generalitat Valenciana.

Esta CPS se aplica a todas las entidades relacionadas con la jerarquía de la PKI de la Generalitat Valenciana, incluyendo Autoridades de Certificación, Autoridades de Registros, subscriptores o firmantes y partes confiantes, entre otros.

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

1.2. Identificación

Nombre del documento	Declaración de Prácticas de Certificación (CPS) de la ACCV
Versión del documento	1.6
Estado del documento	APROBADO
Referencia de la CPS/ OID (Object Identifier)	1.3.6.1.4.1.8149.2.1.6
Fecha de emisión	10 de septiembre de 2004
Fecha de expiración	No aplicable.
Localización	Esta CPS se puede encontrar en www.pki.gva.es/cps

1.3. Comunidad y Ámbito de aplicación

1.3.1. Autoridades de Certificación

La Autoridad de Certificación de la Comunidad Valenciana (ACCV) queda adscrita a la Secretaría Autonómica de Telecomunicaciones y Sociedad de la Información, de la Conselleria de Infraestructuras y Transporte de la Generalitat Valenciana. La Autoridad de Certificación de la Comunidad Valenciana prestará los Servicios de Certificación, de acuerdo con lo previsto en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, y con lo establecido en el Decreto 87/2002, del Gobierno Valenciano. La Autoridad de Certificación definirá los procedimientos y prácticas operativas empleadas en la emisión de certificados digitales para garantizar que los servicios de certificación prestados cumplen los requisitos de seguridad, disponibilidad y funcionalidad requeridos. Dichos procedimientos y prácticas constituyen el documento de Declaración de Prácticas de Certificación (CPS).

Asimismo, la Autoridad de Certificación definirá el uso de cada tipo de certificado emitido, los usuarios posibles, los niveles de seguridad y confianza, las responsabilidades y obligaciones de los titulares de los certificados, los mecanismos de identificación de los titulares de los certificados y los controles de seguridad aplicados. Toda esta información se recoge en el documento de Política de Certificación para cada tipo de certificado.

Las Autoridades de Certificación que componen ACCV son:

- "Root CA GVA" como Autoridad de Certificación de primer nivel. Su función es la de establecer la raíz del modelo de confianza de la Infraestructura de Clave Pública o PKI. Esta CA no emite certificados para entidades finales. Esta Autoridad de Certificación de primer nivel se auto-firma, emitiendo un certificado cuyo firmante es "Root CAGVA" como, y que contiene la clave pública (o datos de verificación de firma) de "Root CAGVA" firmada con los datos de creación de firma (clave privada) de "Root CAGVA". La huella digital o fingerprint de la Autoridad de Certificación Raíz de la Generalitat Valenciana (Root CA), que establece la raíz del modelo de confianza de la Infraestructura de Clave Pública y, expresado en hexadecimal, es:

  A073 E5C5 BD43 610D 864C 2113 0A85 5857 CC9C EA46

  Con esta clave se verifica el certificado autofirmado de la Autoridad de Certificación raíz, que es válido desde el 6 de julio de 2001 al 1 de julio de 2021.

- "CA GVA" Como Autoridad de Certificación subordinada de Root CA GVA. Su función es la emisión de certificados de entidad final para los subscriptores de ACCV. El certificado de "CA GVA" es válido desde el día 4 de septiembre de 2001 hasta el 2 de septiembre de 2011.

1.3.2. Autoridades de Registro

Las Autoridades de Registro son los órganos competentes de la gestión de solicitudes de certificación. Estas Autoridades de Registro pueden estar instaladas en departamentos propios de la Generalitat Valenciana, o en otras Entidades siempre que se haya formalizado un convenio de colaboración. Estas Autoridades de Registro, también llamados Puntos de Registro de Usuario o PRU en la documentación relativa a la Autoridad de Certificación de la Comunidad Valenciana, se constituyen para acercar la ACCV al Ciudadano y facilitar la presentación de solicitudes de certificado, confirmación de la identidad del solicitante y entrega del certificado. Las Autoridades de Registro en ningún caso emiten ni publican certificados. Estas Autoridades de Registro actúan en nombre y por cuenta de la ACCV, y deberán en todo caso:

- Comprobar la identidad y cualesquiera circunstancias personales de los solicitantes de certificados relevantes para el fin propio de éstos.
- Verificar que la información contenida en el certificado es exacta y que incluye toda la información prescrita para un certificado reconocido.
- Asegurarse de que el firmante está en posesión de los datos de creación de firma correspondientes a los de verificación que constan en el certificado.
- Informar a la persona que solicite el certificado de las condiciones precisas para la utilización del certificado y de sus limitaciones de uso.

1.3.3. Entidades Finales

1.3.3.1. Firmantes

Los firmantes son las personas destinatarias de los certificados digitales de la ACCV. El firmante es el titular del certificado, cuya identidad queda vinculada a la herramienta de firma electrónica en su poder. El firmante asume la responsabilidad de custodia de los datos de creación de firma, sin que pueda ceder su uso a cualquier otra persona bajo ningún concepto. En todo caso, el firmante asume la responsabilidad de daños y perjuicios ocasionados a sí mismo o a terceros si incurre en alguno de los siguientes supuestos:

- No haber proporcionado a la ACCV información veraz, completa y exacta de los datos que deban constar en el certificado, o que sean necesarios para su expedición o para la revocación o suspensión de su vigencia.
- La falta de comunicación de cualquier modificación de las circunstancias reflejadas en el certificado.
- Negligencia en la conservación de sus datos de creación de firma.
- No solicitar la suspensión o revocación del certificado en caso de duda en cuanto al mantenimiento de la confidencialidad de los datos de creación de firma.
- Utilizar los datos de creación de firma cuando el certificado haya sido revocado o suspendido por cualquier causa.
- No utilizar el certificado conforme a las condiciones establecidas por al ACCV y comunicadas al firmante en el contrato de certificación

El grupo de usuarios que pueden solicitar la emisión de certificados de ACCV se encuentra definido y limitado por cada Política de Certificación.

De forma genérica, y sin perjuicio de lo establecido por la Política de Certificación aplicable en cada caso, se establece que los posibles firmantes son el conjunto de ciudadanos de la Comunidad Valenciana.

1.3.3.2. Partes confiantes

Las partes confiantes son las personas que reciben el certificado. Son todas aquellas personas que, de forma voluntaria, confían en los certificados emitidos por la ACCV.

Las Políticas de Certificación aplicables en cada caso limitan el derecho a confiar en los certificados emitidos por ACCV.

De forma genérica, y sin perjuicio de lo establecido por la Política de Certificación aplicable en cada caso, se establecen como parte confiante en los certificados de ACCV a los empleados, sistemas y aplicaciones de la Generalitat Valenciana, así como cualquier otra entidad con la que se establezca el oportuno convenio para la prestación de servicios de certificación por parte de la Generalitat Valenciana.

1.3.4. Ámbito de aplicación

Las Políticas de Certificado correspondientes a cada tipo de certificado son quienes determinan el uso y limitaciones apropiado que debe darse a cada certificado. No es objetivo de esta CPS la determinación de dichos usos y limitaciones.

1.4. Datos de contacto

1.4.1. Especificación de la Organización Administradora

Esta CPS es propiedad de la Autoridad Certificadora de la Comunidad Valenciana, descrita en el decreto 87/2002, de 30 de mayo.

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

1.4.2. Persona de Contacto

Para más información relacionada con la presente CPS por favor contacte con:

Nombre de contacto	*Secretaria Autonòmica de Telecomunicacions i Societat de la Informació* *Conselleria d'Infraestructures i Transport*
Dirección de email	*firma@gva.es*
Dirección	*C/ Colón, 66 – 46004 Valencia (Spain)*
Número de teléfono	*+34·902 482 481*
Número de fax	*+34· 961 961 001*

1.4.3. Determinación de la adecuación de la CPS a las Políticas

La Secretaria Autonómica de Telecomunicaciones y Sociedad de la Información es el Órgano que determina la adecuación de esta CPS a las distintas Políticas de Certificado 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

La Autoridad de Certificación de la Comunidad Valenciana está obligada:

- Realizar sus operaciones en conformidad con esta CPS.
- Proteger sus claves privadas.
- Emitir certificados en conformidad con las Políticas de Certificación que les sean de aplicación.
- Tras la recepción de una solicitud válida de certificado, emitir certificados conformes con el estándar X.509 y con los requerimientos de la solicitud.
- Emitir certificados que sean conformes con la información conocida en el momento de su emisión, y libres de errores de entrada de datos.
- Garantizar la confidencialidad en el proceso de generación de datos de creación de firma y su entrega por un procedimiento seguro al firmante.
- Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte
- Utilizar sistemas fiables para almacenar certificados reconocidos que permitan comprobar su autenticidad e impedir que personas no autorizadas alteren los datos, restrinjan su accesibilidad en los supuestos o a las personas que el firmante haya indicado y permitan detectar cualquier cambio que afecte a estas condiciones de seguridad
- Publicar sin alteración los certificados emitidos en el directorio LDAP de ACCV (ldap.pki.gva.es).
- Garantizar que puede determinarse con precisión la fecha y la hora en las que se expidió un certificado o se extinguió o suspendió su vigencia
- Emplear personal con la cualificación, conocimientos y experiencia necesarios para la prestación de los servicios de certificación ofrecidos y los procedimientos de seguridad y de gestión adecuados en el ámbito de la firma electrónica.
- Revocar los certificados en los términos de la sección *4.4 Suspensión y Revocación de Certificados* y publicar los certificados revocados en la CRL del directorio LDAP de ACCV

(ldap.pki.gva.es), con la frecuencia estipulada en el punto 4.4. *Frecuencia de emisión de CRLs.*

- Publicar esta CPS y las CP aplicables en el sitio web www.pki.gva.es/cps, garantizando el acceso a las versiones actuales así como a las versiones anteriores.
- Notificar con prontitud, por correo electrónico, a los subscriptores de certificados en el caso que la CA proceda a la revocación o suspensión del mismo y el motivo que la hubiera producido.
- Colaborar con las auditorias dirigidas por ACCV para validar la renovación de sus propias claves.
- Operar de acuerdo con la legislación aplicable. En concreto con:
    - Decreto 87/2002, de 30 de mayo, del Gobierno Valenciano, por el que se regula la utilización de la firma electrónica avanzada en la Generalitat Valenciana.
    - Decreto 96/1998 de 6 de julio del Gobierno Valenciano, por el que se regulan la organización de la función informática, la utilización de sistemas de información y el Registro de Ficheros informatizados en el ámbito de la administración de la Generalitat Valenciana.
    - Orden de 3 de diciembre de 1999, de la Consellería de Justicia y Administraciones Públicas por la que se aprueba el Reglamento Técnico de Medidas de Seguridad para la Aprobación y Homologación de Aplicaciones y Medios de Tratamiento Automatizado de la Información
    - Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
    - La Orden de 21 de febrero de 2000 por la que se aprueba el reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de forma electrónica.
    - La 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
- Proteger, en caso de haberlas, las claves bajo su custodia.
- Garantizar la disponibilidad de las CRLs de acuerdo con las disposiciones de la sección 4.4.9 de la presente CPS.
- En caso de cesar en su actividad, deberá comunicarlo con una antelación mínima de dos meses al cese efectivo, a los titulares de los certificados emitidos por la ACCV, así como al Ministerio de Industria, Turismo y Comercio, comunicando el destino que va a dar a los certificados.

- Cumplir las especificaciones contenidas en la normativa sobre Protección de Datos de Carácter Personal
- Conservar registrada toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento durante quince años desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo

2.1.2. Obligaciones de la RA

Las personas que operan las RAs integradas en la jerarquía de ACCV –operadores de Punto de Registro de Usuario– están obligadas a:

- Realizar sus operaciones en conformidad con esta CPS.
- Realizar sus operaciones de acuerdo con la Política de Certificación que sea de aplicación para el tipo de certificado solicitado en cada ocasión.
- Comprobar exhaustivamente la identidad de las personas a las que se les concede el certificado digital por ellos tramitado, para lo que requerirán la presencia física del solicitante y la exhibición del DNI original y en vigor. En caso de usuarios extranjeros deberán mostrar la Tarjeta de Residencia / NIE.
- No almacenar ni copiar los datos de creación de firma de la persona a la que hayan prestado sus servicios.
- Informar, antes de la emisión de un certificado, a la persona que solicite sus servicios, de las obligaciones que asume, la forma que debe custodiar los datos de creación de firma, el procedimiento que debe seguir para comunicar la pérdida o utilización indebida de los datos o dispositivos de creación y de verificación de firma, de su precio, de las condiciones precisas para la utilización del certificado, de sus limitaciones de uso y de la forma en que garantiza su posible responsabilidad patrimonial, y de la página web donde puede consultar cualquier información de la ACCV, la CPS y las CP vigentes y anteriores, la legislación aplicable, las certificaciones obtenidas y los procedimientos aplicables para la resolución extrajudicial de los conflictos que pudieran surgir por el ejercicio de la actividad
- Validar y enviar de forma segura a la CA a la que está subordinada la RA una solicitud de certificación debidamente cumplimentada con la información aportada por el subscriptor y firmada digitalmente, y recibir los certificados emitidos de acuerdo con esa solicitud.

- Almacenar de forma segura y hasta el momento de su remisión a la Autoridad de Certificación de la Comunidad Valenciana, tanto la documentación aportada por el subscriptor como la generada por la propia RA, durante el proceso de registro o revocación
- Formalizar el Contrato de Certificación con el subscriptor según lo establecido por la Política de Certificación aplicable.
- Solicitar la revocación de un certificado cuando tenga conocimiento o sospecha del compromiso de una clave privada.
- Autentificar las solicitudes de usuarios finales para la renovación o revocación de sus certificados, generar solicitudes de renovación o revocación firmadas digitalmente y enviarlas a su CA superior.
- En el caso de la aprobación de una solicitud de certificación notificar al subscriptor la emisión de su certificados y la forma de obtenerlo.
- En el caso del rechazo de una solicitud de certificación notificar al solicitante dicho rechazo y el motivo del mismo.
- Cuando se trata de certificados personales, utilizar las herramientas de solicitud y tramitación de certificados en presencia de la persona para la que se realizará la solicitud, tras haber realizado una identificación fiable.
- Mantener bajo su estricto control las herramientas de tramitación de certificados digitales y notificar a la Autoridad de Certificación de la Comunidad Valenciana cualquier malfuncionamiento u otra eventualidad que pudiera salirse del comportamiento normal esperado.
- Remitir copia firmada del contrato de certificación y de las solicitudes de revocación a la Autoridad de Certificación de la Comunidad Valenciana.
- Recibir y tramitar las solicitudes de revocación presenciales que reciba de manera inmediata, después de haber llevado a cabo una identificación fiable basada en el DNI del demandante, o en el NIE en el caso de extranjeros.
- Colaborar en cuantos aspectos de la operación, auditoría o control del Punto de Registro de Usuario se le soliciten por parte de la Autoridad de Certificación de la Generalitat Valenciana.
- A la más general y amplia obligación de confidencialidad, durante y con posterioridad a la prestación del servicio como Autoridad de Registro, respecto de la información recibida por la ACCV y respecto de la información y documentación en que se haya concretado el servicio. En el mismo sentido, no transmitir a terceros dicha información, bajo ningún concepto, sin autorización expresa, escrita y con carácter previo de la ACCV, en cuyo caso trasladará a dichos terceros idéntica obligación de confidencialidad.

2.1.3. Obligaciones de los firmantes

Es obligación de los subscriptores de los certificados emitidos bajo la presente política:

- Limitar y adecuar el uso del certificado a propósitos lícitos y acordes con los usos permitidos por la Política de Certificación pertinente y la presente CPS.
- Poner el cuidado y medios necesarios para garantizar la custodia de su clave privada.
- Solicitar inmediatamente la revocación de un certificado en caso de tener conocimiento o sospecha del compromiso de la clave privada correspondiente a la clave pública contenida en el certificado. Los modos en el que puede realizarse esta solicitud se encuentran especificados en este documento en el apartado 4.4.3 *Procedimientos de solicitud de revocación*.
- No utilizar un certificado digital que hubiera perdido su eficacia, por haber sido suspendido, revocado o por haber expirado el periodo de validez del certificado.
- Suministrar a las Autoridades de Registro información que consideren exacta y completa con relación a los datos que estas les soliciten para realizar el proceso de registro. Así como informar a los responsables de la PKI de la Generalitat Valenciana de cualquier modificación de esta información.
- Abonar las tasas que se devenguen por los servicios de certificación que soliciten de registro que corresponda en relación con los servicios que se soliciten.

2.1.4. Obligaciones de las partes confiantes

Es obligación de las partes que confíen en los certificados emitidos por ACCV:

- Limitar la fiabilidad de los certificados a los usos permitidos de los mismos, en conformidad con lo expresado en las extensiones de los certificado y la Política de Certificación pertinente.
- Verificar la validez de los certificados en el momento de realizar o verificar cualquier operación basada en los mismos.
- Asumir su responsabilidad en la correcta verificación de las firmas digitales
- Asumir su responsabilidad en la comprobación de la validez, revocación o suspensión de los certificados en que confía.
- Tener pleno conocimiento de las garantías y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía, y aceptar sujetarse a las mismas.

2.1.5. Obligaciones del repositorio

- Mantener accesible para las entidades finales el conjunto de certificados emitidos por ACCV
- Mantener accesible para las entidades finales la información de los certificados que han sido revocados, en formato CRL.

2.2. Responsabilidad

2.2.1. Garantías y limitaciones de garantías

ACCV responderá por los daños y perjuicios que causen a cualquier persona, en el ejercicio de su actividad, cuando incumplan las obligaciones que le impone el Decreto 87/2002, de 30 de mayo, del Gobierno Valenciano, sobre Firma Electrónica Avanzada, y la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, o actúe con negligencia.

ACCV responderá de los perjuicios que se causen al firmante o a terceros de buena fe por la falta o el retraso en la inclusión en el servicio de consulta sobre la vigencia de los certificados de la extinción o suspensión de la vigencia del certificado emitido por ACCV, una vez tenga conocimiento de ello.

ACCV asume toda la responsabilidad frente a terceros por la actuación de las personas que realicen las funciones necesarias para la prestación del servicio de certificación.

ACCV es la Autoridad de Certificación de la Generalitat Valenciana. La responsabilidad de la Administración se asienta sobre bases objetivas y cubre toda lesión que los particulares sufran siempre que sea consecuencia del funcionamiento normal o anormal de los servicios públicos.

ACCV sólo responderá de los daños y perjuicios causados por el uso indebido del certificado reconocido, cuando no haya consignado en él, de forma claramente reconocible por terceros, el limite en cuanto a su posible uso o al importe del valor de las transacciones válidas que pueden realizarse empleándolo, No responderá cuando el firmante supere los límites que figuran en el certificado en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan relaizrse con él o no utilizarlo conforme a las condiciones establecidas y comunicadas al firmante por la ACCV Tampoco responderá la ACCV si el destinatario de los documentos firmados electrónicamente no comprueba y tiene en cuenta las restricciones que figuran en el certificado en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él.

2.2.2. Deslinde de responsabilidades

Las CAs y RAs de ACCV no asumen ninguna responsabilidad en caso de perdida o perjuicio:

- De los servicios que prestan, en caso de guerra, desastres naturales o cualquier otro caso de fuerza mayor.
- Ocasionados durante el periodo comprendido entre la revocación de un certificado y la momento de publicación de la siguiente CRL
- Ocasionados por el uso de certificados que exceda los límites establecidos por los mismos, la Política de Certificación pertinente y esta CPS.

- Ocasionado por el uso indebido o fraudulento de los certificados o CRLs emitidos por ACCV.
-
- Ocasionados al firmante o terceros de buena fe si el destinatario de los documentos firmados electrónicamente no comprueba ni tiene en cuenta las restricciones que figuren en el certificado en cuanto a sus posibles usos, o cuando no tenga en cuenta la suspensión o pérdida de vigencia del certificado publicada en la CRL, o cuando no verifique la firma electrónica

2.2.3. Limitaciones de pérdidas

A excepción de lo establecido por las disposiciones de la presente CPS, ACCV no asume ningún otro compromiso ni brinda ninguna otra garantía, así como tampoco asumen ninguna otra responsabilidad ante subscriptores o partes confiantes.

2.2.4. Otras exclusiones

No estipulado

2.3. Responsabilidad Financiera

2.3.1. Indemnización a las partes confiantes

El sistema de responsabilidad es el que se aplica a todas las Administraciones Públicas y se encuentra recogido en la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. ACCV. Se regirá por la normativa que, en materia de responsabilidad patrimonial, se aplique a las Administraciones Públicas.

2.3.2. Relaciones fiduciarias

ACCV no se desempeña como agente fiduciario ni representante en forma alguna de subscriptores ni de terceras partes confiantes en los certificados que emite.

2.3.3. Procesos administrativos

ACCV garantiza la realización de auditorías de los procesos y procedimientos establecidos de manera regular. Estas auditorías se llevarán a cabo tanto de manera interna como externa.

2.4. Interpretación y Ejecución

2.4.1. Legislación aplicable

El funcionamiento y operaciones de ACCV, así como la presente CPS están regidos por la Legislación Española y por la Legislación que el Gobierno Valenciano desarrolle a este respecto.

Explícitamente se asumen como de aplicación obligatoria las siguientes normas:

- Decreto 87/2002, de 30 de mayo, del Gobierno Valenciano por el que se regula la utilización de la firma electrónica avanzada en la Generalitat Valenciana.
- Decreto 96/1998 de 6 de julio del Gobierno Valenciano, por el que se regulan la organización de la función informática, la utilización de sistemas de información y el Registro de Ficheros informatizados en el ámbito de la administración de la Generalitat Valenciana.
- Orden de 3 de diciembre de 1999, de la Consellería de Justicia y Administraciones Públicas por la que se aprueba el Reglamento Técnico de Medidas de Seguridad para la Aprobación y Homologación de Aplicaciones y Medios de Tratamiento Automatizado de la Información
- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- La Orden de 21 de febrero de 2000 por la que se aprueba el reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de forma electrónica.
- La directiva 11999/93/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.

2.4.2. Independencia, subsistencia, fusión, y notificación

2.4.2.1. Independencia

En el caso que una o mas cláusulas de esta CPS sea o llegase a ser inválida, ilegal, o inexigible legalmente, tal inaplicabilidad no afectará a ninguna otra cláusula, sino que se actuará entonces como si las cláusula o cláusulas inaplicables nunca hubieran sido contenidas por esta CPS, y en tal grado como sea posible se interpretará la CPS para mantener la voluntad original de la misma.

2.4.2.2. Subsistencia

No estipulado.

2.4.2.3. Fusión

No estipulado.

2.4.2.4. Notificación

Toda notificación, demanda, solicitud o cualquier otra comunicación requerida bajo las practicas descritas en esta CPS se realizará mediante documento o mensaje electrónico firmado digitalmente de conformidad con esta última o por escrito mediante correo certificado dirigido a cualquiera de las direcciones contenidas en el punto *1.4 Datos de contacto*. Las comunicaciones electrónicas se harán efectivas una vez que las reciba el destinatario al que van dirigidas.

2.4.3. Procedimientos de resolución de disputas

En caso de existir disputas relacionadas con los servicios o disposiciones contempladas por esta Declaración de Prácticas de Certificación, las partes se someterán a la jurisdicción contencioso-administrativa, conforme a lo dispuesto en la Ley 29/1998, de 13 de julio, Reguladora de la Jurisdicción Contencioso-Administrativa.

2.5. Tarifas

2.5.1. Tarifas de emisión de certificado o renovación

Las tarifas de emisión y revocación de cada certificado se especifican en la Política de Certificación que le sea de aplicación.

2.5.2. Tarifas de acceso a los certificados

El acceso a los certificados emitidos, 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 CPS ni las políticas de certificación administradas por ACCV ni por ningún otro servicio adicional del que se tenga conocimiento en el momento de la redacción del presente documento.

Esta disposición podrá ser modificada por la Política de Certificación aplicable en cada caso.

2.5.5. Política de reintegros

En el caso que alguna Política de Certificación especifique alguna tarifa aplicable a la prestación de servicios de certificación o revocación por parte de ACCV para el tipo de certificados que defina, será obligación de esa política la especificación de la política de reintegros correspondiente.

2.6. Publicación y Repositorios

2.6.1. Publicación de información de la CA

Es obligación de las CAs pertenecientes a la jerarquía de confianza de ACCV publicar información relativa a sus prácticas, sus certificados y el estado actual de dichos certificados.

La presente CPS es pública y se encuentra disponible en el sitio web de ACCV http://www.pki.gva.es/cps, en formato PDF.

Las Políticas de Certificación de ACCV son públicas y se encuentran disponibles en el sitio de web de ACCV http://www.pki.gva.es/cps, en formato PDF.

El certificado de la CA de ACCV es público y se encuentra disponible en el repositorio de ACCV, en formato X.509 v3. Tambien se encuentra en la http://www.pki.gva.es.

Los certificados emitidos por ACCV son públicos y se encuentran disponibles en el repositorio de ACCV, en formato X.509 v3

La lista de certificados revocados por ACCV es pública y se encuentra disponible, en formato CRL v2, en el repositorio de ACCV

2.6.2. Frecuencia de publicación

La CPS y las Políticas de Certificación se publicarán en el momento de su creación y se republicarán en el momento que se apruebe cualquier modificación sobre las mismas.

Los certificados emitidos por la CA se publicarán de forma inmediatamente posterior a su emisión.

La CA añadirá los certificados revocados a la CRL pertinente dentro del periodo de tiempo estipulado en el punto 4.4.9 *Frecuencia de emisión de CRLs*.

2.6.3. Controles de acceso

El acceso a lectura de la información del repositorio de ACCV y de su sitio web es libre.

Sólo ACCV está autorizada a modificar, sustituir o eliminar información de su repositorio y sitio web. Los medios de control adecuados se utilizan para restringir la capacidad de escritura o modificación de estos elementos.

2.6.4. Repositorios

El repositorio de ACCV esta compuesto por un servicio de directorio LDAP, en alta disponibilidad, accesible en: ldap://ldap.pki.gva.es:389.

El repositorio de ACCV no contiene ninguna información de naturaleza confidencial.

ACCV no utiliza ningún otro repositorio operado por ninguna organización distinta a ACCV a excepción del directorio LDAP corporativo de la Generalitat Valenciana (ldap.gva.es).

2.7. Control de conformidad

2.7.1. Frecuencia de los controles de conformidad para cada entidad

Se llevará a cabo una auditoría sobre ACCV, al menos una vez al año, para garantizar la adecuación de su funcionamiento y operativa con las disposiciones incluidas en esta CPS.

2.7.2. Identificación/cualificación del auditor

El auditor será seleccionado en el momento de la realización de cada auditoría.

Cualquier empresa o persona contratada para realizar una auditoría de seguridad sobre ACCV deberá cumplir con los siguientes requisitos:

- Adecuada capacitación y experiencia en PKI, seguridad, procesos de auditoría y tecnologías criptográficas.
- Independencia a nivel organizativo de la autoridad de ACCV.

2.7.3. Relación entre el auditor y la entidad auditada

Al margen de la función de auditoría, el auditor y la parte auditada (ACCV) no deberán tener ninguna relación, actual o planificada, financiara, legal, o de cualquier otra clase que pueda derivar en un conflicto de intereses.

En cumplimiento de lo establecido en la normativa vigente en nuestro ordenamiento sobre protección de datos de carácter personal, y habida cuenta de que para el cumplimiento, por parte del auditor, de los servicios regulados en el contrato será preciso acceder a los datos de carácter personal de los ficheros titularidad de la ACCV, el auditor tendrá la consideración de Encargado de Tratamiento, en virtud de lo previsto en el articulo 12 de la Ley Orgánica 15/1999, de 13 de Diciembre.

2.7.4. Tópicos cubiertos por el control de conformidad

La auditoría determinará la conformidad de los servicios de ACCV con esta CPS y las CP's aplicables. También determinará los riesgos del no cumplimiento de la adecuación con la operativa definida por esos documentos.

Los aspectos cubiertos por una auditoría incluirá, pero no estará limitada a:

1. Política de seguridad
2. Seguridad física
3. Evaluación tecnológica
4. Administración de los servicios de la CA
5. Selección de personal
6. CPS y CP's competentes
7. Contratos
8. Política de privacidad

2.7.5. Acciones a tomar como resultado de una deficiencia

La identificación de deficiencias en la auditoría dará lugar a la adopción de medidas correctivas. La Secretaria Autonómica de Telecomunicaciones y Sociedad de la Información, en colaboración con el auditor será la responsable de la determinación de las mismas.

En el caso de una deficiencia grave, la Secretaria Autonómica de Telecomunicaciones y Sociedad de la Información podrá determinar la suspensión temporal de las operaciones de la ACCV hasta que las deficiencias se corrijan, la revocación del certificado de la entidad, cambios en el personal, etc.

2.7.6. Comunicación de resultados

El auditor comunicará los resultados de la auditoría a la Secretaria Autonómica de Telecomunicaciones y Sociedad de la Información, en tanto que responsable máximo de la ACCV, al Responsable de Seguridad de ACCV, así como a los responsables de las distintas áreas en las que se detecten no conformidades.

2.8. Política de Confidencialidad

2.8.1. Tipo de información a mantener confidencial

Se declaran expresamente como información confidencial y no será divulgada a terceros excepto en los casos en que la ley exija lo contrario:

- Las claves privadas de las entidades que componen ACCV.
- Las claves privadas de firmantes de las que ACCV mantenga en custodia.
- Toda la información relativa a las operaciones que lleve a cabo ACCV.
- Toda la información relativa a los parámetros de seguridad, control y procedimientos de auditoría.
- Toda la información de carácter personal proporcionada a ACCV durante el proceso de registro de los subscriptores de certificados con la salvedad de lo especificado por la Política de Certificación aplicable y el contrato de certificación.
- Toda la información clasificada como "CONFIDENCIAL" o "ESTRICTAMENTE CONFIDENCIAL"

Toda información de carácter personal proporcionada a ACCV por los subscriptores de sus certificados será tratada de acuerdo con los términos de la "*Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal*". En este sentido se ha creado un fichero de Usuarios de Firma Electrónica, cuyo responsable es la Secretaria Autonómica de Telecomunicaciones y Sociedad de la Información, mediante Orden de 8 de marzo de 2002, (publicada en el DOGV nº 4.221de 4 de abril de 2002) y la corrección de errores de dicha Orden (publicada en el DOGV nº 4.304, de 31 de julio de 2002), así como su modificación por Orden de 26 de mayo de 2004, de la Conselleria de Infraestructuras y Transporte, por la que se crean, modifican y cancelan ficheros de datos de carácter personal (DOGV 4.772, de 10 de junio de 2004).

La ACCV dispone de un Documento de Seguridad, que responde a la obligación establecida en el artículo 8 del Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal.

La ACCV dispone de una Política de Privacidad, publicada en la web de ACCV, de acuerdo con la legislación de datos de carácter personal vigente.

2.8.2. Tipo de información no considerada confidencial

ACCV considera información pública:

- La información contenida en la presente CPS.
- La información contenida en las Políticas de Certificación que le son de aplicación.
- Los certificados emitidos, con las informaciones en ellos contenidas
- Lista de certificados revocados (CRL)
- Toda la información que no sea considerada confidencial

La CPS de ACCV y las CP's que le son de aplicación no incluirán información considerada confidencial por el punto 2.8.1 del presente documento.

Se permite el acceso a la información no considerada confidencial para su lectura. La ACCV establecerá los controles de seguridad necesarios para proteger la autenticidad e integridad de la información e impedir que personas no autorizadas puedan añadir, modificar o suprimir la misma.

2.8.3. Divulgación de información de revocación /suspensión de certificados

La información de la revocación o suspensión de certificados se proporciona vía CRL en el directorio LDAP que actúa como repositorio de ACCV

Esta información también se encuentra disponible en el servidor de validación OCSP de ACCV en ocsp.pki.gva.es:80

2.8.4. Envío a la autoridad judicial y/o policial

Como principio general ningún documento o registro perteneciente a ACCV se envía a las autoridades judiciales o policiales excepto cuando:

- El agente de la ley se identifique adecuadamente.
- Se proporcione una orden judicial debidamente redactada.

2.8.5. Publicación como parte de un descubrimiento civil

No estipulado

2.8.6. Divulgación a petición del propietario

El sujeto de un proceso de registro o usuario tiene acceso a la información del mismo, y NO está facultado a autorizar el acceso a esa información a otra persona. Se garantiza la posibilidad de ejercer el derecho de acceso, tal y como se entiende en la legislación relativa a protección de datos de carácter personal.

2.8.7. Otras circunstancias de publicación de información

No está permitida la divulgación de información bajo ninguna circunstancia diferente de las reseñadas en los puntos anteriores de este documento.

2.9. Derechos de propiedad Intelectual

Todos los derechos de propiedad intelectual incluyendo los referidos a certificados y CRL's emitidos por ACCV, OIDs, la presente CPS, las Políticas de Certificación que le son de aplicación, así como cualquier otro documento, electrónico o de cualquier otro tipo, propiedad de ACCV, pertenecen y permanecerán en propiedad de ACCV.

Las claves privadas y las claves públicas son propiedad del usuario, independientemente del medio físico que se emplee para su almacenamiento.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. Registro inicial

3.1.1. Tipos de nombres

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

El *distinguished name* se incluye en el campo Common Name (CN) y se trata del nombre que aparece identificado en el DNI, Pasaporte o Documento que identifique al firmante del certificado.

3.1.2. Necesidad de los nombres de ser significativos

En todos los casos los nombres distintivos deben tener sentido. Si la Política de Certificación aplicable al tipo de certificado no indica lo contrario, se utilizan el nombre y NIF del solicitante.

ACCV no permite el uso de seudónimos en los certificados que emite.

3.1.3. Reglas para interpretar varios formatos de nombres

Reglas utilizadas por ACCV para interpretar los nombres distintivos de los certificados que emite es ISO/IEC 9595 (X.500) Distinguished Name (DN)

3.1.4. Unicidad de los nombres

Los nombres distintivos (distinguished names) deben ser no ambiguos y únicos.

Para ello se incluirá como parte del nombre común (common name) del nombre distintivo (distinguished name) el nombre del subscriptor seguido de su NIF, con el formato "*nombre* - NIF *número de NIF*".

Las Políticas de Certificación pueden disponer la sustitución de este mecanismo de unicidad

3.1.5. Procedimientos de resolución de disputas de nombres

Cualquier disputa concerniente a la propiedad de nombres se resolverá según lo estipulado en el punto 2.4.3 de este documento.

3.1.6. Reconocimiento, autenticación y función de las marcas registradas

No estipulado

3.1.7. Métodos de prueba de posesión de la clave privada

En el caso que el par de claves sea generado por la entidad final (subscriptor) este deberá probar la posesión de la clave privada correspondiente a la clave pública que solicita que se certifique mediante el envío de la solicitud de certificación en formato PKCS #10

Esta norma podrá verse revocada por lo establecido en cada caso en la Política de Certificación aplicable para cada solicitud

3.1.8. Autenticación de la identidad de una organización

En el caso que una Política de Certificación considere necesaria la autenticación de la identidad de una organización, dicha política será la responsable del establecimiento de los métodos necesarios para la verificación de la mencionada identidad.

Explícitamente se prohibe en esta CPS el uso de métodos de identificación remota de organizaciones.

3.1.9. Autenticación de la identidad de un individuo

El proceso de identificación individual se define por la Política de Certificación aplicable a cada tipo de certificado.

No se considerará que el proceso deba ser menos estricto que otros mecanismos de autenticación utilizados por la Generalitat Valenciana.

Como norma general no se emplearán métodos de identificación remota distintos a la firma digital realizada con certificados emitidos por la propia ACCV o por algún otro Prestador de Servicios de Certificación reconocido con el que se haya establecido convenio de reconocimiento mutuo o convalidación de certificados, en los términos que establece el artículo 13 del decreto 87/2002, de 30 de mayo, del Gobierno Valenciano., siempre que éste 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..

3.2. 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 utilizando solicitudes firmadas digitalmente mediante el certificado original que se pretende renovar, siempre que este no haya vencido ni se haya procedido a su revocación. Existen, por tanto, dos mecanismos alternativos para la renovación:

- Formularios web firmados en el Área Personal de Servicios de Certificación, disponible en www.pki.gva.es

- Presentación en cualquier Punto de Registro de Usuario, con los documentos de identificación suficientes (ver apartado 3.1.9 de esta CPS).

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, o bien se empleará algún método electrónico que garantice de manera fiable e inequívoca la identidad del solicitante y la autenticidad de la solicitud.

3.4. Solicitud de revocación

El proceso de solicitud de revocación se define por la Política de Certificación aplicable a cada tipo de certificado.

La política de identificación para las solicitudes de revocación podrá ser la misma que para el registro inicial. La política de autenticación aceptará solicitudes de revocación firmadas digitalmente por el subscriptor del certificado.

Las distintas Políticas de Certificación pueden definir otras políticas de identificación menos severas.

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

Las distintas Políticas de Certificación pueden definir la creación de una contraseña de revocación en el momento del registro del certificado.

4. REQUERIMIENTOS OPERACIONALES

Todo lo especificado en este apartado queda supeditado a lo estipulado por las distintas Políticas de Certificación para la emisión de certificados acogidos a las mismas.

4.1. Solicitud de certificados

En cada Política de Certificación se especifica la información que se debe suministrar en la solicitud de certificados del tipo por ellas definido y los pasos que deben seguirse para llevar a cabo este proceso.

Es atribución de la RA de ACCV 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.

Las solicitudes de certificación una vez completadas serán enviadas a la Autoridad de Certificación por la Autoridad de Registro de ACCV.

4.2. Emisión de certificados

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

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

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

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

Todo lo especificado en este apartado queda supeditado a lo estipulado por las distintas Políticas de Certificación para la emisión de certificados acogidos a las mismas.

4.3. Aceptación de certificados

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

4.4. Suspensión y revocación de certificados

4.4.1. Circunstancias para la revocación

Un certificado se revoca cuando:

- El subscriptor del certificado o sus claves o las claves de sus certificados se han comprometido por:
  - El robo, perdida, revelación, modificación, u otro compromiso o sospecha de compromiso de la clave privada del usuario.
  - El mal uso deliberado de claves y certificados, o la falta de observación de los requerimientos operacionales del acuerdo de subscripción, la CP asociada o de la presente CPS.
- Se produce la emisión defectuosa de un certificado debido a:
  - Que no se ha satisfecho un prerrequisito material para la emisión del certificado.
  - Que un factor fundamental en el certificado se sepa o crea razonablemente que puede ser falso.
  - Un error de entrada de datos u otro error de proceso.
- El par de claves generado por un usuario final se revela como “débil”.
- La información contenida en un certificado o utilizada para realizar su solicitud se convierte en inexacta, por ejemplo cuando el dueño de un certificado cambia su nombre.
- Una solicitud de revocación válida se recibe de un usuario final.
- Una solicitud de revocación válida se recibe de una tercera parte autorizada, por ejemplo una orden judicial.
- El certificado de una RA o CA superior en la jerarquía de confianza del certificado es revocado.

4.4.2. Entidad que puede solicitar la revocación

La revocación de un certificado se puede iniciar tanto por el subscriptor del mismo como por parte de ACCV.

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

El procedimiento para la solicitud de la revocación de cada tipo de certificado se definirá en la Política de Certificación correspondiente.

De forma general y sin perjuicio de lo definido en las Políticas de Certificación se determina que:

- Se aceptarán solicitudes de revocación remotas si están firmadas digitalmente con un certificado de ACCV o de algún otro Prestador de Servicios de Certificación reconocido y admitido por la ACCV, en los términos que establece el artículo 13 del decreto 87/2002, de 30 de mayo, del Gobierno Valenciano, 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 30 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 el mismo.

Existe un formulario de solicitud de revocación de certificados en la web de ACCV, en la URL http://www.pki.gva.es.

Una solicitud de revocación tanto si se realiza en papel o de forma electrónica (ej..: mail) debe contener la información que se describe en el formulario de solicitud de revocación, recogido en cada una de las Políticas de Certificación.

4.4.4. Periodo de gracia de la solicitud de revocación

La revocación se realizará de forma inmediata al procesamiento de cada solicitud verificada como válida. Por tanto no existe ningún periodo de gracia asociado a este proceso.

4.4.5. Circunstancias para la suspensión

La suspensión implica invalidez del certificado durante el tiempo que permanece suspendido.

La suspensión únicamente se puede declarar de oficio por la propia ACCV, cuando se ha producido una solicitud de revocación de un certificado sin posible verificación inmediata de la identidad del

solicitante (telefónica, por correo electrónico sin firma digital...), o cuando ACCV sospecha que se haya podido comprometer la clave privada asociada al certificado de un usuario, o si ACCV tiene dudas sobre la veracidad de los datos asociados al certificado. El plazo máximo que puede quedar suspendido un certificado por alguna de estas causas será de 30 días.

También se suspenderá un certificado si así lo dispone una autoridad judicial o administrativa, por el tiempo que la misma establezca.

ACCV no soporta la suspensión de certificados como operación independiente sobre sus certificados.

4.4.6. Entidad que 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. Límites 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

ACCV publicará una nueva CRL en su repositorio en intervalos de máximo 3 horas, aunque no se hayan producido modificaciones en la misma (cambios de estado de certificados) durante el citado periodo.

4.4.10. Requisitos de comprobación de CRLs

La verificación de la CRL es obligatoria para cada uso de los certificados de entidades finales.

Las partes confiantes deberán comprobar la validez de la CRL previamente a cada uno de sus usos y descargarse la nueva CRL del repositorio de ACCV al finalizar el periodo de validez de la que posean.

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

ACCV proporciona un servidor OCSP para la verificación on-line del estado de los certificados en la URL ocsp.pki.gva.es:80

4.4.12. Requisitos de comprobación on-line de revocación

El servidor OCSP es de libre acceso y no existe ningún requisito para su uso excepto los derivados del uso del propio protocolo OCSP según se define en el RFC 2560.

ACCV dispone también de servicios web de consulta del estado de validez de los certificados expedidos.

4.4.13. Otras formas de divulgación de información de revocación disponibles

Algunas Políticas de Certificación pueden dar soporte a otras formas de información sobre el estado de revocación, como los Puntos de Distribución de CRLs (CDP).

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

Cuando la Política de Certificación que sea de aplicación soporte otras formas de divulgación de información de revocación, los requerimientos para la comprobación de dicha información se especificarán en la propia Política de Certificación.

4.4.15. Requisitos especiales de renovación de claves comprometidas

No hay ninguna variación en las cláusulas anteriores cuando la revocación sea debida al compromiso de la clave privada.

4.5. Procedimientos de Control de Seguridad

4.5.1. Tipos de eventos registrados

ACCV registra todos los eventos relacionados con:

- Intentos exitosos o fracasados de cambiar los parámetros de seguridad del sistema operativo.
- Arranque y parada de aplicaciones.
- Intentos exitosos o fracasados de inicio y fin de sesión.
- Intentos exitosos o fracasados de crear, modificar o borrar cuentas del sistema.

- Intentos exitosos o fracasados de crear, modificar o borrar usuarios del sistema autorizados.
- Intentos exitosos o fracasados de solicitar, generar, firmar, emitir o revocar claves y certificados.
- Intentos exitosos o fracasados de generar, firmar o emitir una CRL.
- Intentos exitosos o fracasados de crear, modificar o borrar información de los titulares de certificados.
- Intentos exitosos o fracasados de acceso a las instalaciones por parte de personal autorizado o no.
- Backup, archivo y restauración.
- Cambios en la configuración del sistema.
- Actualizaciones de software y hardware.
- Mantenimiento del sistema.
- Cambios de personal

4.5.2. Frecuencia de procesado de logs

Se establecen tres niveles de auditorías de control de los eventos registros con una frecuencia diaria, mensual y anual respectivamente.

4.5.3. Periodo de retención para los logs de auditoría

ACCV retendrá todos los registros de auditoría generados por el sistema por un periodo mínimo desde la fecha de su creación de dos (2) años para los pertenecientes a auditorías diarias, cinco (5) años para las mensuales y quince (15) años para los de auditorias anuales

4.5.4. Protección de los logs de auditoría

Cada histórico de auditoría que contenga esos registros se cifra usando la clave pública de un certificado que se emitirá para la función de auditoría de ACCV. Las copias de backup de dichos registros se almacena en un archivo ignífugo cerrado dentro de las instalaciones seguras de ACCV.

La destrucción de un archivo de auditoría solo se puede llevar a cabo con la autorización del Administrador del Sistema, el Responable de Seguridad y del Auditor de ACCV. Tal destrucción se puede iniciar por la recomendación por escrito de cualquiera de estas tres entidades o del administrador del servicio auditado.

4.5.5. Procedimientos de backup de los logs de auditoría

No estipulado.

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

El sistema de recolección de auditorías de la PKI es una combinación de procesos automáticos y manuales ejecutados por los sistemas operativos, las aplicación de la PKI, y por el personal que las opera.

4.5.7. Notificación al sujeto causa del evento

No estipulado.

4.5.8. Análisis de vulnerabilidades

Se establece la realización de un análisis mensual de vulnerabilidades y de seguridad perimetral.

Es responsabilidad de los coordinadores de los equipos de análisis el informar a la ACCV, a través del Responsable de Seguridad, de cualquier problema que impida la realización de las auditorias, o la entrega de la documentación resultante. Es responsabilidad de la ACCV informar a los equipos auditores de la suspensión de los análisis.

4.6. Archivo de registros

4.6.1. Tipo de eventos registrados

Los tipos de eventos registrados son:

- Los registros de auditoría especificados en el punto 4.5.
- Los soportes de backup de los servidores que componen la infraestructura de ACCV.

4.6.2. Periodo de retención para el archivo

Toda la información y documentación relativa a los certificados emitidos por ACCV se conserva durante un periodo de 15 años.

4.6.3. Protección del archivo

El acceso al archivo se encuentra restringido a personal autorizado.

Así mismo los eventos relativos a los certificados emitidos por ACCV se encuentra protegida criptográficamente para garantizar la detección de manipulaciones en su contenido.

4.6.4. Procedimientos de backup del archivo

Se realizan dos copias diarias de los ficheros que componen los archivos a retener.

Una copia se realiza en local y se almacena en una caja fuerte ignífuga dentro del CPD de ACCV.

La segunda copia de los datos se realiza de forma cifrada y remota y se almacena en un CPD alternativo sito en un edificio distinto al del CDP de ACCV.

4.6.5. Requerimientos para el sellado de tiempo de los registros

Los sistemas de ACCV realizan el registro del instante de tiempo en los que se realizan. El tiempo de los sistemas proviene de una fuente fiable de hora. Todos los sistemas de ACCV sincronizan su instante de tiempo con esta fuente.

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

El sistema de recogida de información es interno a la entidad ACCV.

4.6.7. Procedimientos para obtener y verificar información archivada

No estipulado.

4.7. Cambio de Clave

Los procedimientos para proporcionar una nueva clave pública a los usuarios de una CA se especificarán en la Política de Certificación correspondiente a cada tipo de certificado.

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

En el caso de una indisponibilidad de las instalaciones de la Autoridad de Certificación por un periodo superior a seis horas, se procederá a la activación del Plan de Continuación de Operaciones de la Autoridad de Certificación

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

Si los recursos hardware, software, y/o datos se alteran o son sospechosos de haber sido alterados se detendrá el funcionamiento de la PKI hasta el restablecimiento de un entorno seguro con la incorporación de nuevos componentes de eficiencia acreditable. De forma paralela se realizará una auditoría para identificar la causa de la alteración y asegurar la no reproducción de la misma.

En el caso de verse afectados certificados emitidos, se notificará del hecho a los subscriptores de los mismos y se procederá a su recertificación.

4.8.2. La clave publica de una entidad se revoca

En el caso de la revocación del certificado de una entidad de ACCV se generará y publicará la correspondiente CRL, se detendrá el funcionamiento de la entidad y se procederá a la generación, certificación y puesta en marcha de una nueva entidad con la misma denominación que la eliminada y con un nuevo par de claves.

En el caso que la entidad afectada sea una CA el certificado revocado de la entidad permanecerá accesible en el repositorio de ACCV con objeto de continuar permitiendo la verificación de los certificados emitidos durante su periodo de funcionamiento.

Las entidades componentes de ACCV dependientes de la entidad renovada serán informadas del hecho y conminadas a solicitar su recertificación por la nueva instancia de la entidad.

4.8.3. La clave de una entidad se compromete

En el caso de compromiso de la clave de una entidad se procederá a su revocación inmediata según lo expuesto en el punto anterior y se informará del hecho al resto de entidades que componen ACCV dependientes o no de la entidad afectada.

Los certificados firmados por entidades dependientes de la comprometida, en el periodo comprendido entre el compromiso de la clave y la revocación del certificado correspondiente, serán a su vez revocados, informados sus subscriptores y recertificados.

4.8.4. Instalación de seguridad después de un desastre natural u otro tipo de desastre

No estipulado.

4.9. Cese de una CA

Las causas que pueden producir el cese de la actividad de la Autoridad de Certificación son:

- Compromiso de la clave privada de la CA

- Decisión política por parte de la Generalitat Valenciana

En caso de cese de su actividad como Prestador de Servicios de Certificación, ACCV realizará, con una antelación mínima de dos meses, las siguientes acciones:

- Informar a todos los subscriptores de sus certificados y extinguir la vigencia de los mismos revocándolos.
- Informar a todas las terceras partes con las que tenga que haya firmado un convenio de certificación.
- Comunicar al Ministerio de Ciencia y Tecnología el cese de su actividad y el destino que va a dar a los certificados, así como cualquier otra circunstancia relevante relacionada con el cese de actividad.
- Remitir al Ministerio de Ciencia y Tecnología toda la información relativa a los certificados electrónicos revocados para que éste se haga cargo de su custodia.

5. CONTROLES DE SEGURIDAD FÍSICA, PROCEDURAL Y DE PERSONAL

5.1. Controles de Seguridad Física

5.1.1. Ubicación y construcción

Físicamente las instalaciones de ACCV están ubicadas en las oficinas de la Secretaría Autonómica de Telecomunicaciones y Sociedad de la Información, C/Colón, 66, 1ª planta. Cuenta con vigilancia 24 horas al día, 7 días a la semana.

5.1.2. Acceso físico

Esta sala esta protegida por diferentes equipos de seguridad físicas, incluyendo sistemas biométricos, sistemas de grabación, detección de intrusiones, etc.

La sala dispone de una única entrada con cerradura biométrica y cámaras IP para registrar las entradas y las tareas realizadas en el interior de la sala protegida.

5.1.3. Alimentación eléctrica y aire acondicionado

Las instalaciones disponen de un sistema de alimentación ininterrumpida (SAI) con una potencia suficiente para mantener una autonomía de la red eléctrica durante el periodo de apagado controlado del sistema.

El sistema de aire acondicionado está compuesto por varios equipos independientes, con el propósito de redundancia y con mandos y sensores contenidos en la propia sala.

5.1.4. Exposición al agua

La sala del CPD dispone de detectores de humedad y sistemas de alarma apropiados al entorno.

5.1.5. Protección y prevención de incendios

La sala del CPD dispone de un interruptor de emergencia protegido y situado en su exterior. En el interior se hallan instalados detectores de calor y humo y sistemas de extinción apropiados al entorno.

5.1.6. Sistema de almacenamiento

Se dispone de una caja fuerte ignifuga y dos armarios seguros dentro de las instalaciones de la PKI para el almacenamiento de documentación y soportes de backup.

5.1.7. Eliminación de residuos

Se utiliza una destructora de documentos para la eliminación de forma segura de toda la documentación confidencial dentro de la sala de la CA, tras su utilización.

5.1.8. Backup remoto

Se realizan copias de bakup remotas cifradas que son almacenadas en un edificio distinto al de la Secretaría Autonómica de Telecomunicaciones y Sociedad de la Información.

5.2. Controles procedimentales

Por razones de seguridad, la información relativa a los controles de procedimiento se considera materia confidencial y solo se explican de forma resumida.

5.2.1. Papeles de confianza

Los roles identificados para el control y la gestión del sistema son:

a. Administrador de Sistemas
b. Administrador de Puntos de Registro de Usuario (PRU)
c. Operador de Autoridad de Certificación
d. Operador de PRU
e. Responsable de formación, soporte y comunicación
f. Responsable de Seguridad
g. Auditor
h. Jurista
i. Responsable de Documentación
j. Responsable de Soporte al Despliegue

5.2.1.1. Administración de Sistemas

Encargado de la instalación y configuración de sistemas operativos, de productos software, del mantenimiento y actualización de los productos y programas instalados.

Deben encargarse de establecer y documentar los procedimientos de monitorización de los sistemas y de los servicios que prestan, así como del control de las tareas realizadas por los Operadores de Autoridad de Certificación.

Deben velar por la prestación de servicios con el adecuado nivel de calidad y fiabilidad, en función de la criticidad de éstos servicios.

Son responsables de la correcta ejecución de la Política de Copias y, en particular, y de mantener la información suficiente como para poder restaurar cualquiera de los sistemas en el menor tiempo posible. Junto con el perfil de Operador de Autoridad de Certificación y, excepcionalmente, de Administrador de PRU, se encargará de llevar a cabo las copias de backup locales.

Deben mantener el inventario de servidores y equipamiento que compone el núcleo de la PKI.

No debe tener acceso a aspectos relacionados con la seguridad de los sistemas, de la red, etc. (altas/bajas de usuarios, gestión de reglas de firewall, gestión y mantenimiento de los sistemas de detección de intrusiones, etc.).

Deben colaborar con los Auditores en todo aquello que les sea requerido.

5.2.1.2. Administrador de PRUs.

Este perfil es similar al de Administrador de Sistemas pero dedicado a las tareas relacionadas con la instalación, mantenimiento y control de los sistemas que componen los Puntos de Registro de Usuario.

Se encargará de las tareas administrativas relacionadas con las autorizaciones de Operadores de PRU, acuerdos de confidencialidad, etc.

Deben mantener el inventario de PRUs y equipamiento que se dedica a las operaciones de los PRUs.

Excepcionalmente colaborará con el perfil de Administrador de Sistemas y Operador de Autoridad de Certificación para llevar a cabo los bakups locales de los sistemas de la PKI.

De igual manera que los Administradores de Sistemas, no debe tener acceso a aspectos relacionados con la seguridad de los sistemas, de la red, etc. (altas/bajas de usuarios, gestión de reglas de firewall, gestión y mantenimiento de los sistemas de detección de intrusiones, etc.).

Deben colaborar con los Auditores en todo aquello que les sea requerido.

5.2.1.3. Operador de Autoridad de Certificación

Darán asistencia a los Administradores de Sistemas y Administradores de PRU en aquellos aspectos técnicos o administrativos que no requieran acceso al CPD.

Deberán prestar asistencia al Responsable de formación, soporte y comunicación en aquellas tareas que les indique.

Deberán prestar la colaboración requerida por los Administradores de PRU, tanto para funciones de inventario, ayuda a la instalación de sistemas componentes de los PRUs, preparación de documentación, colaboración en la formación y soporte de operadores de PRU, etc.

Prestarán colaboración al Responsable de Documentación para el control de documentos existentes, control de archivo de documentación (en papel) y revisión de certificados y contratos.

Colaborarán con el Responsable de Seguridad en tareas administrativas, de inventario y, en general, aquellas tareas técnicas o administrativas.

Junto con el perfil de Administrador de Sistemas y, excepcionalmente, de Administrador de PRU, se encargará de llevar a cabo las copias de backup locales. Esta será la única tarea que el Operador de Autoridad de Certificación desarrolle en el interior del CPD.

Deben colaborar con los Auditores en todo aquello que les sea requerido.

5.2.1.4. Operadores de Punto de Registro de Usuario

Se encargan única y exclusivamente de las funciones relacionadas con la identificación de solicitantes de certificados, la tramitación de certificados digitales, la revocación de éstos y el desbloqueo de tarjetas criptográficas, todo ello haciendo uso en exclusiva de las herramientas que les proporcionen los Administradores de PRU, y siguiendo estrictamente los procedimientos aprobados.

Dentro de este perfil, existe un subgrupo denominado “Operadores de Suspensión de CallCenter” que únicamente tienen privilegios para suspender certificados, tras recibir la solicitud telefónica de revocación por el supuesto titular del certificado.

Deben colaborar con los Auditores en todo aquello que les sea requerido.

5.2.1.5. Responsable de formación, soporte y comunicación

Se encarga del mantenimiento de contenidos de la web de la Autoridad de Certificación de la Generalitat Valenciana.

Se encarga de la preparación de noticias para paso a prensa o para publicarlas a través de la web.

Se encarga de definir el plan de formación para usuarios finales, para agentes de Call Center y para personal implicado directamente en la operación y administración de la PKI. Colaborará con el Administrador de PRU en la preparación de la formación a Operadores de PRU.

El Responsable de formación, soporte y comunicación será el responsable de la preparación de los contenidos de los cursos impartidos sobre la plataforma corporativa de e-learning.

Debe revisar mensualmente los ficheros de incidencias y respuestas de Call Center, y revisar los argumentarios de los agentes de Call Center.

Debe coordinar la actuación del personal de microinformática y facilitar las herramientas y material necesario para que desarrollen correctamente su labor.

El Responsable de formación, soporte y comunicación podrá contar con la colaboración de los Operadores de Autoridad de Certificación, para aquellas tareas que estime oportuno.

5.2.1.6. Responsable de Seguridad

Debe cumplir y hacer cumplir las políticas de seguridad de la PKI, y debe encargarse de cualquier aspecto relativo a la seguridad de la PKI, desde seguridad física hasta la seguridad de las aplicaciones, pasando por seguridad de la red.

Será el encargado de gestionar los sistemas de protección perimetral y en concreto de la gestión de las reglas de los firewalls.

Debe encargarse de la instalación, configuración y gestión de los sistemas de detección de intrusiones (IDS) y de las herramientas asociadas a éstos.

Es el responsable de resolver o hacer que se resuelvan las incidencias de seguridad producidas, de eliminar vulnerabilidades detectadas, etc.

Es el responsable de la gestión y control de los sistemas de seguridad física del CPD, de los sistemas de control de acceso, de los sistemas de acondicionamiento ambiental y de alimentación eléctrica.

Debe encargarse de explicar los mecanismos de seguridad al personal que deba conocerlos, de concienciar a todo el personal de la PKI y de hacer cumplir las normas y políticas de seguridad.

Debe establecer los calendarios para la ejecución de análisis de vulnerabilidades, ensayos y pruebas de los planes de continuidad del servicio y auditorías de los sistemas de información.

Debe colaborar con los Auditores en todo aquello que les sea requerido.

5.2.1.7. Auditor

Este perfil de auditor es interno. Las auditorías externas se contratarán aparte.

El Auditor debe encargarse de:

- Constatar la existencia de toda la documentación requerida y enumerada
- Comprobar la coherencia de la documentación con los procedimientos, activos inventariados, etc.
- Comprobar el seguimiento de incidencias y eventos
- Comprobar la protección de los sistemas (explotación de vulnerabilidades, logs de acceso, usuarios, etc.).
- Comprobar alarmas y elementos de seguridad física
- Comprobar adecuación a normativa y legislación
- Comprobar conocimiento de los procedimientos por parte del personal implicado

En definitiva, debe comprobar todos los aspectos recogidos en la política de seguridad, políticas de copias, prácticas de certificación, políticas de certificación, etc. tanto en el núcleo de sistemas de la PKI y personal de la PKI, como en los PRUs.

5.2.1.8. Jurista

Se encargará de los aspectos legales de la prestación de servicios de certificación y de la formalización de la prestación de estos servicios a otras entidades, con las que hubiera que establecer convenio de certificación.

Se encargará de llevar a cabo los trámites para la aprobación y publicación de Políticas de Certificación, modificaciones del documento de Declaración de Prácticas de Certificación y, en general, de cualquier normativa pública relacionada con el funcionamiento de la PKI de la Autoridad de Certificación.

Deberá velar por el cumplimiento de la legislación de firma electrónica vigente en cada momento, analizando las Políticas de Certificación y Declaración de Prácticas de Certificación existentes y las que sean objeto de aprobación, e informando de las incoherencias o de los problemas que detectara.

Debe colaborar con los Auditores en todo aquello que les sea requerido.

5.2.1.9. Responsable de Documentación

Se encargará de mantener el repositorio de documentación electrónica de la PKI y los archivos de documentación en papel.

Controlará que se lleven a cabo la actualización de documentos cuando se requiera y por parte de quien el Responsable de Documentación designe, incluso superando lo especificado en los documentos a actualizar o mantener.

Se encargará de mantener actualizado el fichero de índice de documentos y será el único habilitado para almacenar, borrar o modificar documentos en el repositorio de documentación de la PKI.

Podrá contar con la colaboración de los Operadores de Autoridad de Certificación para llevar a cabo tareas de control o inventario documental.

Deberá garantizar que todo certificado emitido tiene asociado un contrato de certificación en papel.

5.2.1.10. Responsable de Soporte al Despliegue

Se encargará de llevar a cabo un primer nivel de soporte y, cuando sea necesario, pondrá en contacto a Infonova con el grupo de desarrollo en cuestión. De la misma forma, redirigirá las consultas legales al Jurista, después de tratar de resolver aquellas cuestiones legales básicas.

Deberá recabar información suficiente (plantilla de información de proyectos) antes de poner en contacto a Infonova.

Deberá orientar sobre las posibilidades, técnicas y herramientas de desarrollo, teniendo en cuenta los sistemas de información corporativos, política de seguridad, etc.

El Responsable de Soporte al Despliegue deberá orientar sobre la normativa técnica y administrativa existente, sobre el deber de creación de PRUs, la manera de funcionar de éstos, etc. Deberá colaborar con las consellerias o entidades con las que se hubiera establecido el convenio de certificación para analizar mecanismos de distribución de certificados, creación de PRUs, etc.

5.2.2. Número de personas requeridas por tarea

Se requieren dos personas para la activación de claves de los dispositivos criptográficos hardware de generación y almacenamiento de claves, HSM. Los dispositivos criptográficos utilizados para generar y almacenar las claves privadas de los elementos que componen la PKI de ACCV son SureWare Keyper de AEP Systems.

Estos dispositivos vienen equipados con una cerradura que permite habilitar el uso del teclado y display y un lector de smartcards que identifica y autoriza a los Operadores de Seguridad (SO) a realizar sus funciones.

La activación de los servicios implica la autenticación por parte de un Security Officer. La modificación de los parámetros de configuración del HSM implica la autenticación por parte de dos Security Officers, que son asumidos por el Responsable de Seguridad y una personal del grupo de Administradores de Sistemas, con privilegios suficientes.

5.2.3. Identificación y autenticación para cada papel

Todos los usuarios autorizados de ACCV se identifican mediante certificados digitales emitidos por la propia PKI y se autentifican por medio de smart-cards criptograficas y/o dispositivos biométricos.

5.3. Controles de seguridad de personal

Este apartado refleja el contenido del documento Controles de Seguridad del Personal de ACCV.

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

La Autoridad de Certificación requiere que todo el personal que desarrolla tareas en sus instalaciones tenga la suficiente cualificación y experiencia en entornos de prestación de servicios de certificación.

Todo el personal debe cumplir los requerimientos de seguridad de la organización y deben poseer:

- Conocimientos y formación sobre entornos de certificación digital.
- Formación básica sobre seguridad en sistemas de información.
- Formación especifica para su puesto.
- Titulo académico o experiencia en la industria equivalente

5.3.2. Procedimientos de comprobación de antecedentes

No estipulado

5.3.3. Requerimientos de formación

El personal de la Autoridad de Certificación está sujeto a un plan de formación específico para el desarrollo de su función dentro de la organización.

Dicho plan de formación incluye los siguientes aspectos:

1. Formación en los aspectos legales básicos relativos a la prestación de servicios de certificación.
2. Formación en seguridad de los sistemas de información.
3. Servicios proporcionados por la Autoridad de Certificación.
4. Conceptos básicos sobre PKI.
5. Declaración de Prácticas de Certificación y las Políticas de Certificación pertinentes.
6. Gestión de incidencias.

5.3.4. Requerimientos y frecuencia de actualización de la formación

Ante cambios tecnológicos del entorno, introducción de nuevas herramientas o modificación de procedimientos operativos, se llevará a cabo la formación adecuada para el personal afectado.

Ante cambios en la Declaración de Prácticas de Certificación, Políticas de Certificación u otros documentos relevantes, se llevarán a cabo sesiones formativas.

5.3.5. Frecuencia y secuencia de rotación de tareas

No se ha definido ningún plan de rotación en la asignación de sus tareas para el personal de la Autoridad de Certificación.

5.3.6. Sanciones por acciones no autorizadas

En el caso de comisión de una acción no autorizada con respecto a la operación de la Autoridad de Certificación se tomarán medidas disciplinarias. Se considerarán acciones no autorizadas las que contravengan la Declaración de Practicas de Certificación o las Políticas de Certificación pertinentes tanto de forma negligente como malintencionada.

Si se produce alguna infracción, la Autoridad de Certificación suspenderá el acceso de las personas involucradas a todos los sistemas de información de la Autoridad de Certificación de forma inmediata al conocimiento del hecho.

Adicionalmente, en función de la gravedad de las infracciones, se aplicarán las sanciones previstas en la Ley de la Función Pública, convenio colectivo de la empresa, o el Estatuto de los Trabajadores según corresponda a la situación laboral del infractor.

5.3.7. Requerimientos de contratación de personal

Todo el personal de la Autoridad de Certificación está sujeto al deber de secreto mediante la firma del acuerdo de confidencialidad (documento Acuerdo de Confidencialidad con OID 1.3.6.1.4.1.8149.1.1.3.2.x.x) al incorporarse a su puesto. En dicho acuerdo, además, se obliga a desarrollar sus tareas de acuerdo con esta Declaración de Prácticas de Certificación.

5.3.8. Documentación proporcionada al personal

Al personal que se incorpora a la Autoridad de Certificación se le proporciona acceso a la siguiente documentación:

- Declaración de Prácticas de Certificación
- Políticas de certificación
- Política de privacidad

Se facilitará acceso a la documentación relativa a normas y planes de seguridad, procedimientos de emergencia y toda aquella documentación técnica necesaria para llevar a cabo sus funciones.

5.3.9. Controles periódicos de cumplimiento

El control de que el personal posee los conocimientos necesarios se lleva a cabo al finalizar las sesiones formativas y discrecionalmente, por parte del profesorado encargado de impartir estos cursos y, en última instancia, por parte del Responsable de formación, soporte y comunicación.

El control de la existencia de la documentación que los empleados deben conocer y firmar, se lleva a cabo anualmente por parte del Responsable de Documentación.

Anualmente, el Responsable de Seguridad llevará a cabo una revisión de la adecuación de las autorizaciones otorgadas a los efectivos privilegios concedidos a los empleados.

5.3.10. Finalización de los contratos

En caso de finalización de la relación laboral del personal que desarrolla sus funciones en la ACCV, el Responsable de Seguridad procederá a:

1. Eliminar los privilegios de acceso de los sistemas de control biométrico de acceso físico al CPD de la ACCV.
2. Eliminación de usuarios de los sistemas informáticos.
3. Eliminación, en su caso, de los privilegios de operación de las herramientas de tramitación de certificados (sistema XRAO).
4. Remisión de correo electrónico informativo al resto de personal de la ACCV, para dar a conocer la terminación de la relación laboral.

6. CONTROLES DE SEGURIDAD TÉCNICA

6.1. Generación e Instalación del Par de Claves

6.1.1. Generación del par de claves

Los pares de claves para todos los componentes internos de ACCV se generan en módulos de hardware criptográficos con certificación FIPS 140-1 Nivel 4.

Las claves de la Root CA y CAGVA son claves RSA de 2048 bits de longitud

Los pares de claves para entidades finales se generan en función de lo estipulado en la Política de Certificación aplicable.

6.1.2. Entrega de la clave privada a la entidad

En los casos en los que la generación de las claves no se realice mediante medios bajo control de la propia entidad final será la Política de Certificación correspondiente la que especifique el procedimiento a emplear para realizar la entrega de la clave privada a las entidades finales.

6.1.3. Entrega de la clave publica al emisor del certificado

Las claves públicas generadas por medios bajo el control de las entidades finales se envían a ACCV como parte de una solicitud de certificación en formato PKCS#10, firmado digitalmente con la clave privada correspondiente a la clave pública que se solicita certificar.

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

Las claves públicas de todas las CA pertenecientes a la jerarquía de confianza de ACCV se pueden descargar del sitio web http://www.pki.gva.es.

6.1.5. Tamaño de las claves

El tamaño de las claves de la Root CA y CAGVA es de 2.048 bits

El tamaño de las claves para cada tipo de certificado emitido por ACCV se establece en la Política de Certificación que le es de aplicación. En todo caso, su tamaño nunca será inferior a 1.024 bits.

6.1.6. Parámetros de generación de la clave pública

Las claves de la Root CA y CAGVA están creadas con el algoritmo RSA

Los parámetros de generación de claves para cada tipo de certificado emitido por ACCV vienen definidos por la Política de Certificación que le sea de aplicación.

6.1.7. Comprobación de la calidad de los parámetros

Los procedimientos y medios de comprobación de la calidad de los parámetros de generación de claves para cada tipo de certificado emitido por ACCV vienen definidos por la Política de Certificación que le sea de aplicación.

6.1.8. Hardware/software de generación de claves

Las claves para las entidades de la PKI se generan en dispositivos HSM criptográficos con certificación FIPS 140-1 Nivel 4

Los dispositivos hardware o software a utilizar en la generación de claves para cada tipo de certificado emitido por ACCV viene definido por la Política de Certificación que le sea de aplicación.

6.1.9. Fines del uso de la clave

Los fines del uso de la clave para cada tipo de certificado emitido por ACCV vienen definidos por la Política de Certificación que le sea de aplicación.

Todos los certificados emitidos por ACCV contienen las extensiones *KEY USAGE* y *EXTENDED KEY USAGE* definidas por el estándar X.509 v3 para la definición y limitación de tales fines.

6.2. Protección de la Clave Privada

6.2.1. Estándares para los módulos criptográficos

Se requiere que los módulos utilizados para la creación de claves utilizadas por Root CA GVA y CA GVA y las RA's de ACCV cumplan con la certificación FIPS140-1 de nivel 4.

6.2.2. Control multipersona de la clave privada

Las claves privadas utilizadas por Root CA GVA y CA GVA se encuentran bajo control multipersonal. Todas ellas se encuentran divididas en varios fragmentos y es necesario un mínimo de dos de esos fragmentos para poder volver a recomponer la clave.

6.2.3. Custodia de la clave privada

No se custodian claves privadas de firma de los subscriptores. Las de encriptación pueden custodiarse de acuerdo con lo dispuesto por la Política de Certificación aplicable.

Las claves privadas de las Autoridades de Certificación y Autoridades de Registro que componen ACCV se encuentran alojadas en dispositivos de hardware criptográfico con certificación FIPS 140-1 de nivel 4.

El resto de claves privadas de entidades componentes de ACCV se encuentran contenidas en smart cards criptográficas en poder de los administradores de cada entidad.

6.2.4. Copia de seguridad de la clave privada

Las copias de backup de las claves privadas de componentes de ACCV se almacenan encriptadas en archivos seguros ignífugos.

6.2.5. Archivo de la clave privada.

Las copias de backup de las claves privadas en custodia encriptadas en archivos seguros ignífugos.

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

Las claves privadas se crean en el módulo criptográfico en el momento de la creación de cada una de las entidades de ACCV que hacen uso de dichos módulos.

6.2.7. Método de activación de la clave privada.

La clave privada de tanto de la Root CA como de CAGVA se activa mediante la inicialización del software de CA.

6.2.8. Método de desactivación de la clave privada

Un Administrador puede proceder a la desactivación de la clave de las Autoridades de Certificación de ACCV mediante la detención del software de CA.

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

ACCV mantiene un archivo de todos los certificados emitidos por un periodo de quince (15) años.

6.3.2. Periodo de uso para las claves públicas y privadas

El certificado de Root CA GVA tiene una validez de veinte (20) años. El de CAGVA de diez (10) años y el de las Autoridades de Registro (XRAO) y el resto de entidades de ACCV de tres (3) años.

El periodo de validez de los certificados de entidades finales vendrá establecido por la Política de Certificación aplicable en cada caso, y en ningún caso superará los cuatro (4) años de validez máxima.

6.4. Datos de activación

6.4.1. Generación y activación de los datos de activación

Los datos de activación de las Autoridades de Certificación de ACCV se generan y almacenan en smart cards criptográficas en posesión de personal autorizado.

6.4.2. Protección de los datos de activación

Solo el personal autorizado conoce los PINs y contraseñas para acceder a los datos de activación.

6.4.3. Otros aspectos de los datos de activación

No estipulado.

6.5. Controles de Seguridad Informática

La datos concernientes a este apartado se considera información confidencial y solo se proporciona a quien acredite la necesidad de conocerlos.

6.6. Controles de Seguridad del Ciclo de Vida.

La datos concernientes a este apartado se considera información confidencial y solo se proporciona a quien acredite la necesidad de conocerlos.

6.7. Controles de Seguridad de la Red

La datos concernientes a este apartado se considera información confidencial y solo se proporciona a quien acredite la necesidad de conocerlos.

6.8. Controles de Ingeniería de los Módulos Criptográficos

ACCV utiliza módulos criptográficos hardware y software disponibles comercialmente desarrollados por terceros.

ACCV únicamente utiliza módulos criptográficos con certificación FIPS o ITSEC.

7. PERFILES DE CERTIFICADO Y CRL

7.1. Perfil de Certificado

7.1.1. Número de versión

ACCV soporta y utiliza certificados X.509 versión 3 (X.509 v3)

X.509 es un estándar desarrollado por la Unión Internacional de Telecomunicaciones (organización internacional de las Naciones Unidas para coordinación de servicios de redes de telecomunicaciones entre Gobiernos y empresas) para las Infraestructuras de Clave Pública y los Certificados digitales.

7.1.2. Extensiones del certificado

Las extensiones utilizadas de forma genérica en los certificados son:

- Key Usage. Marcada como crítica.
- Basic Constraint. Marcada como critica.
- Certificate Policies. Marcada como critica.
- Subject Alternative Name. Marcada como no critica.
- CRL Distribution Point. Marcada como no crítica.

Las Políticas de Certificación de ACCV pueden establecer variaciones en conjunto de las extensiones utilizadas por cada tipo de certificado.

7.1.3. Identificadores de objeto (OID) de los algoritmos

Identificador de Objeto (OID) de los algoritmos Criptográficos:

- md5withRSAEncryption (1.2.840.113549.1.1.4)
- SHA1withRSAEncryption (1.2.840.113549.1.1.5)

7.1.4. Formatos de nombres

Los certificados emitidos por ACCV contienen el distinguished name X.500 del emisor y el subscriptor del certificado en los campos issuer name y subject name respectivamente.

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

Ha definir por cada Política de Certificación.

ACCV tiene definida una política de asignación de OID's dentro de su arco privado de numeración. El OID de todas la Políticas de Certificación de ACCV comienzan con el prefijo 1.3.6.1.4.1.8149.3

7.1.7. Uso de la extensión "Policy Constraints"

No estipulado

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 practicas que ACCV asocia explícitamente con el certificado. Adicionalmente la extensión puede contener un cualificador de la política.

7.2. Perfil de CRL

7.2.1. Número de versión

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

7.2.2. CRL y extensiones

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

8. ESPECIFICACIÓN DE LA ADMINISTRACIÓN

8.1. Procedimientos de Especificación de Cambios

Ocasionalmente ACCV puede realizar modificaciones en sus Políticas de Certificación o en la presente CPS.

La entidad con atribuciones para realizar y aprobar cambios sobre la CPS y las CP's de ACCV es la Secretaria Autonómica de Telecomunicaciones y Sociedad de la Información, cuyos datos de contacto se encuentran en el apartado *1.4 Datos de Contacto* de esta CPS.

Algunos de esos cambios no reducirán materialmente la confianza que una Política de Certificación o su implementación proporcionan, y se juzgarán por la Secretaria Autonómica de Telecomunicaciones y Sociedad de la Información como que no modifican la aceptabilidad de los certificados que soporta la política para los propósitos para los que se han usado. En tales casos se procederá al incremento del número menor de versión del documento y el último número de Identificador de Objeto (OID) que lo representa, manteniendo el número mayor de la versión del documento, así como el resto de su OID asociado. No se considera necesario comunicar este tipo de modificaciones a los subscriptores de los certificados correspondientes a la CP o CPS modificada.

En el caso que la Secretaria Autonómica de Telecomunicaciones y Sociedad de la Información juzgue que los cambios a la especificación pueden afectar a la aceptabilidad de los certificados para propósitos específicos se procederá al incremento del número mayor de versión del documento y la puesta a cero del número menor de la misma. También se modificarán los dos últimos números del de Identificador de Objeto (OID) que lo representa. Este tipo de modificaciones se comunicará a los subscriptores de los certificados correspondientes a la CP o CPS modificadamediante envío de una notificación a la dirección de correo electrónico que el usuario ha facilitado en la emisión del certificado, con una antelación de al menos 30 días antes de la publicación de la nueva CPS. El usuario puede aceptar las modificaciones o rechazarlas. En caso de rechazarlas, su certificado emitido bajo las instrucciones de la anterior CPS será válido para los propósitos en ella incluidos, pero no para los propósitos específicos que se incluyen en la nueva CPS o CP modificada. Si transcurridos 15 días desde la notificación al usuario no se tuviera respuesta del mismo, se considerará que el usuario no ha aceptado la modificación, aunque puede aceptarla en cualquier momento posterior.

8.2. Procedimientos de Publicación y Notificación

Toda modificación de esta Declaración de Prácticas de Certificación o de los Documentos de Políticas de Certificación se harán públicas en el sitio web de ACCV www.pki.gva.es.

Adicionalmente, cualquier modificación sustancial de esta CPS se comunicará en el Diari Oficial de la Generalitat Valenciana mediante Resolución de la Secretaría Autonómica de Telecomunicaciones y Sociedad de la Información, en su calidad de Autoridad Certificadora de la Generalitat Valenciana.

8.3. Procedimientos de Aprobación de la CPS.

La Secretaria Autonómica de Telecomunicaciones y Sociedad de la Información es la entidad encargada de la aprobación en el momento de su creación de la presente CPS, así como de las Políticas de Certificación (CP).

La Secretaria Autonómica de Telecomunicaciones y Sociedad de la Información también se encarga de aprobar y autorizar las modificaciones de dichos documentos.

Glosario

Partes confiantes

Conjunto de personas o entidades que confían en los certificados emitidos por ACCV

Abreviaturas y Acrónimos

ACCV	Autoridad de Certificación de la Comunidad Valenciana
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
FIPS	
IETF	Internet Engineering Task Force
OID	Object identifier
OCSP	On-line Certificate Status Protocol
PKI	Public Key Infrastructure
PKIGVA	PKI de la Generalitat Valenciana
RA	Registration Authority
RFC	Request For Comment
Sub CA	Subordinate Certification Authority