Presidéncia del Govern Valencià
Direcció General de Telecomunicacions i Modernització

Proyecto *e-firma*GV

Declaración de Prácticas de Certificación (CPS)

Fecha: 10 de septiembre de 2002
Versión: 1.1
Archivo: PKIGVA-KS-P5.08-V3.0.doc
OID: 1.3.6.1.4.1.8149.1.1.5.8.1.2

Tabla de Contenido

1. INTRODUCCIÓN

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 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 Practicas de Certificación (CPS) de la PKI de la Generalitat Valenciana (PKIGVA).
Versión del documento	1.1
Estado del documento	En vigor
Referencia de la CPS/ OID (Object Identifier)	1.3.6.1.4.1.8149.1.1.5.8.1.2 1.3.6.1.4.1.8149.2.1.1
Fecha de emisión	11 de septiembre de 2002
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

Las Autoridades de Certificación que componen PKIGVA 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 PKI. Esta CA no emite certificados para entidades finales.
- "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 PKIGVA

1.3.2. Autoridades de Registro

Las Autoridades de Registro competentes para la gestión de solicitudes de certificación se encuentra definidas en la Política de Certificación correspondiente a cada tipo de certificado.

1.3.3. Entidades Finales

1.3.3.1. Subscriptores

El grupo de usuarios que pueden solicitar la emisión de certificados de PKIGVA 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 suscriptores son el conjunto de ciudadanos de la Comunidad Valenciana.

1.3.3.2. Partes confiantes

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

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 PKIGVA a los empleados, sistemas y aplicaciones 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 Generalitat Valenciana, descrita en el decreto 87/2002, de 30 de mayo.

Nombre	*Direcció General de Telecomunicacions i Modernització Presidència de la Generalitat Valenciana*
Dirección de email	*dgtm@gva.es*
Dirección	*C/ Colón, 66 –64004Valencia (Spain)*
Número de teléfono	*+34·96·386·6319*
Número de fax	*+34·96·386·3773*

Esta CPS está administrada por la Autoridad de Aprobación de Políticas (AAP) de la PKI de la Generalitat Valenciana.

Nombre	*AAP PKI de la Generalitat Valenciana*
Dirección de email	*aap@pki.gva.es*
Dirección	*C/ Colón, 66 – 46004 Valencia (Spain)*
Número de teléfono	*+34·902·482·481*
Número de fax	*+34· 96·386·5899*

1.4.2. Persona de Contacto

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

Nombre de contacto	*Proyecto e-firmaGV*
Dirección de email	*firma@gva.es*
Dirección	*C/ Colón, 66 – 46004 Valencia (Spain)*
Número de teléfono	*+34·96·196·1024*
Número de fax	*+34· 96·386·5899*

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

La Autoridad de Aprobación de Políticas (AAP) de la Generalitat Valenciana es la entidad 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

Las CAs que operan bajo la jerarquía de PKIGVA están obligadas a:

- Realizar sus operaciones en conformidad con esta CPS.
- Proteger sus claves privadas
- Emitir certificados en conformidad con las Políticas de Certificado 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.
- Publicar sin alteración los certificados emitidos en el directorio LDAP de PKIGVA (ldap.pki.gva.es).
- 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 PKIGVA (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
- 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 PKIGVA 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
- El Real Decreto-Ley 14/1999, de 17 de septiembre, sobre 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 el caso de cesar en su actividad, deberá comunicarlo con una antelación mínima de dos meses, a los titulares de los certificados por ellos emitidos.
- Conservar registrada toda la información y documentación relativa a un certificado reconocido durante quince años.

2.1.2. Obligaciones de la RA

Las RAs que operan bajo la jerarquía de PKIGVA están obligadas a:

- Realizar sus operaciones en conformidad con esta CPS.
- Proteger sus claves privadas
- Realizar sus operaciones de acuerdo con la Política de Certificación que sea de aplicación para el tipo de certificado solicitado en cada ocasión.
- Comprobar por si o por medio de una persona física o jurídica que actúe en nombre y por cuenta suyos, la identidad y cualesquiera circunstancias personales de los solicitantes de los certificados relevantes para el fin propio de éstos, utilizando cualquiera de los medios admitidos en derecho.
- Verificar la exactitud y autenticidad de la información suministrada por el subscriptor en el momento de la solicitud o la renovación, en conformidad con la Política de Certificación pertinente.

- 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 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.
- 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 permanente, 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.
- 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
    - El Real Decreto-Ley 14/1999, de 17 de septiembre, sobre 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.
- Colaborar con las auditorias dirigidas por PKIGVA para validar la renovación de sus propias claves
- 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.
- Realizar auditorias internas de seguridad regularmente.
- 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.
- En el caso de que el prestador de servicios de certificación genere datos de creación de firma, garantizar su confidencialidad durante el proceso de generación.

2.1.3. Obligaciones de los Subscriptores

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 de Valencia 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 PKIGVA:

- 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 PKIGVA
- 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

PKIGVA 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, o actúe con negligencia.

PKIGVA 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.

2.2.2. Deslinde de responsabilidades

Las CAs y RAs de PKIGVA 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 PKIGVA.
- Ocasionados por el uso de la información contenida en el certificado.

2.2.3. Limitaciones de pérdidas

A excepción de lo establecido por las disposiciones de la presente CPS, PKIGVA 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

PKIGVA garantiza disponer de los recursos financieros suficientes para afrontar riesgos por responsabilidad frente a los titulares de sus certificados y las partes confiantes.

2.3.2. Relaciones fiduciarias

PKIGVA 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

PKIGVA 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. Leyes gubernamentales

El funcionamiento y operaciones de PKIGVA, 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 Re-

gistro 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
- El Real Decreto-Ley 14/1999, de 17 de septiembre, sobre 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 CPS las partes se someten expresamente a los juzgados y tribunales de la ciudad de Valencia, con renuncia de su propio fuero si este fuese otro.

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 PKIGVA 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 PKIGVA 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 PKIGVA 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 PKIGVA http://www.pki.gva.es/cps, en formato PDF.

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

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

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

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

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 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 PKIGVA y de su sitio web es libre.

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

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

PKIGVA no utiliza ningún otro repositorio operado por ninguna organización distinta a PKIGVA 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 PKIGVA, 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 PKIGVA 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 PKIGVA.

2.7.3. Relación entre el auditor y la entidad auditada

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

2.7.4. Tópicos cubiertos por el control de conformidad

La auditoría determinará la conformidad de los servicios de PKIGVA 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 tópicos 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 Autoridad de Aprobación de Políticas (AAP) en colaboración con el auditor será la responsable de la determinación de las mismas.

En el caso de una deficiencia grave la Autoridad Aprobadora de Políticas podrá determinar la suspensión temporal de las operaciones 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 Autoridad Aprobadora de Políticas de PKIGVA, al Gestor de Seguridad de PKIGVA, así como a los administradores de PKIGVA y de la entidad en la que se detecten no conformidades.

2.8. Política de Confidencialidad

2.8.1. Tipo de información a mantener confidencial

Toda información no considerada por PKIGVA como pública revestirá el carácter de 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 PKIGVA.
- Las claves privadas de suscriptores de las que PKIGVA mantenga en custodia.
- Toda la información relativa a las operaciones que lleve a cabo PKIGVA.
- Toda la información relativa a los parámetros de seguridad, control y procedimientos de auditoría.
- Toda la información de carácter personal proporcionada a PKIGVA 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 información de carácter personal proporcionada a PKIGVA 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 y declarado un fichero de

datos de carácter personal mediante Orden de 8 de mayo de 2.002 del Conseller de Innovación y Competitividad.

2.8.2. Tipo de información no considerada confidencial

PKIGVA 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
- Lista de certificados revocados (CRL)

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

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 PKIGVA

Esta información también se encuentra disponible en el servidor de validación OCSP de PKIGVA 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 PKIGVA 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 tiene acceso a la información del mismo, y NO está facultado a autorizar el acceso a esa información a otra persona.

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 PKIGVA, 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 PKIGVA, pertenecen y permanecerán en propiedad de PKIGVA.

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.

La Autoridad de Registro propone y aprueba los nombres distintivos para los solicitantes de certificados.

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.

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

3.1.3. Reglas para interpretar varios formatos de nombres

Reglas utilizadas por PKIGVA 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 PKIGVA 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.

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.

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.

PKIGVA 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 PKIGVA 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 PKIGVA.

4.2. Emisión de certificados

PKIGVA 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 PKIGVA 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 PKIGVA 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 PKIGVA

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 suscriptores 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.
- El subscriptor de un certificado deja de pertenecer al grupo de interés del tipo de certificado que posee, por ejemplo:
  - Un usuario final abandona su puesto en la organización que lo facultaba para la posesión del certificado.
  - Un proveedor de servicios que cesa en sus funciones.
  - La muerte de un usuario final.
- 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. Quien puede solicitar la revocación

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

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

4.4.3. Procedimiento de solicitud de revocación

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 PKIGVA o de 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, 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 PKIGVA, 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 recoge el formulario siguiente:

Solicitud de revocación de certificado Fecha : _____

Sección 1 – Detalles del certificado (si se conocen)

ID certificado: .....

Número de serie del certificado: .....

Tipo de certificado: .....

Sección 2 – Datos del suscriptor del certificado

Nombre: .....

NIF: .....

Sección 3 – Motivo de la revocación *

.....

.....

.....

.....

.....

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

Sección 4 – Autorización

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

……

Firma: .....

4.4.4. Periodo de gracia de la solicitud de revocación

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

Los certificados únicamente se podrán suspender como parte del proceso de revocación para el caso de solicitudes sin origen verificado.

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

4.4.6. Quien puede solicitar la suspensión

PKIGVA no soporta la suspensión de certificados como operación independiente sobre sus certificados. Por tanto nadie puede solicitar la realización de dicha operación.

4.4.7. Procedimiento para la solicitud de suspensión

No aplicable

4.4.8. Límites del periodo de suspensión

El límite para el periodo de suspensión de los certificados dentro del proceso de revocación esta definido en el punto 4.4.3.

4.4.9. Frecuencia de emisión de CRLs

PKIGVA publicará una nueva CRL en su repositorio en el momento que se produzca cualquier revocación, y, en último caso, a intervalos no superiores a 12 horas aunque no se hayan producido modificaciones en la CRL.

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 PKIGVA al finalizar el periodo de validez de la que posean.

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

PKIGVA 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

4.4.13. Otras formas de divulgación de información de revocación disponibles

Algunas CPs pueden dar soporte a otras formas de aviso 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 CP de aplicación soporte otras formas de divulgación de información de revocación, los requerimientos para la comprobación de dicha información se especificarán en la propia CP.

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

PKIGVA 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

PKIGVA 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 encripta usando la clave pública de un certificado que se emitirá para la función de auditoría de PKIGVA. Las copias de backup de dichos registros se almacena en un archivo ignífugo cerrado dentro de las instalaciones seguras de PKIGVA.

La destrucción de un archivo de auditoría solo se puede llevar a cabo con la autorización del Administrador del Sistema, el Gestor de Seguridad y el Administrador de Auditorías de PKIGVA. 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

Una Revisión de Riesgos de Seguridad se ha realizado para la totalidad de PKIGVA. Esta revisión cubre la totalidad de riesgos que pueden afectar a la PKI.Anualmente se repetirán dichos análisis

4.6. Archivo de registros

4.6.1. Tipo de eventos registrados

Los especificados en el punto 4.5

4.6.2. Periodo de retención para el archivo

No estipulado.

4.6.3. Protección del archivo

No estipulado.

4.6.4. Procedimientos de backup del archivo

No estipulado.

4.6.5. Requerimientos para el sellado de tiempo de los registros

No estipulado.

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

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

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 CP correspondiente a cada tipo de certificado.

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

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

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 PKIGVA 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 PKIGVA con objeto de continuar permitiendo la verificación de los certificados emitidos durante su periodo de funcionamiento.

Las entidades componentes de PKIGVA 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 PKIGVA 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

No estipulado.

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 PKIGVA están ubicadas en las oficinas de la Oficina de Ciència i Tecnologia del Govern Valencià, Direcció General de Telecomunicacions i Modernització. Cuentan con vigilancia las 24 horas.

En su interior se ubica una caja fuerte ignífuga, ademas de armarios seguros con varias cajas de seguridad internas que hace las veces de archivo local.

5.1.2. Acceso físico

Esta sala esta protegida por diferentes equipos de seguridad físicas, incluyendo sistemas biométricos,

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 de suficiente para mantener una autonomía de la red eléctrica durante el periodo deapagado controlado del sistema.

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

5.1.4. Exposición al agua

No existe ninguna medida preventiva, informativa o correctiva contra la exposición al agua de los sistemas

5.1.5. Protección y prevención de incendios

Existen medidas preventivas y correctivas para la protección frente a incendios de la sala protegida.

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 docuementos 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

No se realiza ningún tipo de copia de seguridad de forma remota a la sala de firma.

5.2. Controles procedurales

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:

Administrador de la PKI: Es el responsable último del funcionamiento de la PKI. Sus tareas incluyen la gestión tanto de las máquinas como de las aplicaciones que componen el sistema. La responsabilidad de este perfil incluye la administración del sistema de base de datos, repositorio LDAP y sistema de firewall.

Gestor de Seguridad: Responsable de la definición y verificación de todos los procedimientos de seguridad tanto física como informática.

Autoridad de Aprobación de Políticas: Entidad responsable de la definición y aprobación de las políticas de certificación.

Administrador de Auditoría: Responsable de las tareas de ejecución y revisión de auditorías internas del sistema.

Autoridad de Archivo: Responsable de las tareas de gestión y verificación de archivo tanto local como externo.

Administrador de Backup: Responsable de las tareas de ejecución y revisión de las copias de seguridad del sistema.

5.2.2. Número de personas requeridas por tarea

No existe un número mínimo de personas definido para la realización de tareas dentro de las instalaciones de la PKI.

5.2.3. Identificación y autenticación para cada papel

Todos los usuarios autorizados de PKIGVA 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

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

No estipulado

5.3.2. Procedimientos de comprobación de antecedentes

No estipulado

5.3.3. Requerimientos de formación

No estipulado

5.3.4. Requerimientos y frecuencia de actualización de la formación

No estipulado

5.3.5. Frecuencia y secuencia de rotación de tareas

No estipulado

5.3.6. Sanciones por acciones no autorizadas

No estipulado

5.3.7. Requerimientos de contratación de personal

No estipulado

5.3.8. Documentación proporcionada al personal

No estipulado

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 PKIGVA se generan en módulos de hardware criptográficos con certificación FIPS 140-1 Nivel 4.

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 PKIGVA 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's pertenecientes a la jerarquía de confianza de PKIGVA se pueden descargar del sitio web http://www.pki.gva.es.

6.1.5. Tamaño de las claves

El tamaño de las claves para cada tipo de certificado emitido por PKIGVA viene definido por la Política de Certificación que le sea de aplicación.

6.1.6. Parámetros de generación de la clave pública

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

6.1.8. Hardware/software de generación de claves

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

Todos los certificados emitidos por PKIGVA 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 PKIGVA 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 PKIGVA 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 PKIGVA 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 PKIGVA 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 PKIGVA 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 PKIGVA 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

PKIGVA 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 CA GVA de diez (10) años y el de las Autoridades de Registro y el resto de entidades de PKIGVA de un (1) año.

El periodo de validez de los certificados de subscriptores vendrá establecido por la Política de Certificación aplicable a cada uno.

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 PKIGVA 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

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

PKIGVA 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

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

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 PKIGVA 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 PKIGVA 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.

PKIGVA 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 PKIGVA 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 PKIGVA 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 (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 PKIGVA 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 PKIGVA es la Autoridad de Aprobación de Políticas (AAP). Los datos de contacto de la AAP 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 AAP 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 AAP 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 modificada.

8.2. Procedimientos de Publicación y Notificación

Cuando se realicen modificaciones significativas en la CPS o CP's de PKIGVA estas se notificarán mediante correo electrónico, a los subscriptores de los certificados afectados en el caso de CP's, o de todos los certificados en el caso de esta CPS. Adicionalmente las modificaciones se harán públicas en el sitio web PKIGVA en www.pki.gva.es.

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

8.3. Procedimientos de Aprobación de la CPS.

La Autoridad de Aprobación de Políticas (AAP) de PKIGVA 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 AAP 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 PKIGVA

Abreviaturas y Acrónimos

AAP	Autoridad de Aprobación de Políticas
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