Acción del actor: *AC*	Interfaz de la *AC*
1. Accede a la interfaz del *AC* usando cualquiera de las tres tarjetas inteligentes. 3. Verifica la firma del AR en los certificados aprobados y enviado por el *AR* o por el *PUB*. 5. Firma los certificados digitales. 7. Descarga los certificados firmados al medio de almacenamiento portátil.	2. Autentica y autoriza el acceso a la interfaz de la *AC*. 4. Realiza el proceso de verificar la firma en lote. 6. Realiza el proceso de firmar el lote de certificado. 8. descarga los certificados al medio de almacenamiento portátil.

Tabla 21. Caso de Uso: Acepta los certificados por la AR.

3.5.2.2.- Firma los certificados usando la clave privada del *PSC*

Firma en un lote todos los certificados digitales usando la clave privada del *PSC* que se encuentra almacenado el la bóveda de seguridad. Por razones de seguridad y responsabilidad para acceder a la bóveda de seguridad, es necesario que dos (2) de las tres (3) personas que conforman la *AC* introduzcan al mismo tiempo sus tarjetas inteligentes para realizar el proceso de firmar los certificados.

Acción del actor: *AC*	Interfaz de la *AC*
1. Se dirigen a la bóveda de seguridad donde se encuentra almacenado la clave privada de la *PSC*, para ello debe dirigirse dos de los tres que conforma la *AC*. 2. Acceden a la bóveda de seguridad introduciendo dos de las tres tarjetas inteligentes que conforma la *AC*. 4. Firma los certificados.	3. Autentica y autoriza el acceso a la clave. 4. Firma digitalmente los certificados.

Tabla 22. Caso de Uso: Firma los certificados usando la clave privada de la PSC

3.5.2.3.- Envía los certificados firmados al *PUB*

Envía todos los certificados que firma con la clave privada del *PSC* al *PUB* para que se publique en un repositorios publico, para que puedan ser consultados, verificados por sistemas o terceras personas interesarlas de hacerlos.

.

Acción del actor: *AC*	Interfaz de la *AC*
1. Almacena los certificados firmados en el medio de almacenamiento portátil 3. Envía los certificados firmados al *PUB*	2. descarga los certificados firmados al medio de almacenamiento portátil.

Tabla 23. Caso de Uso: Envía los certificados firmados al PUB

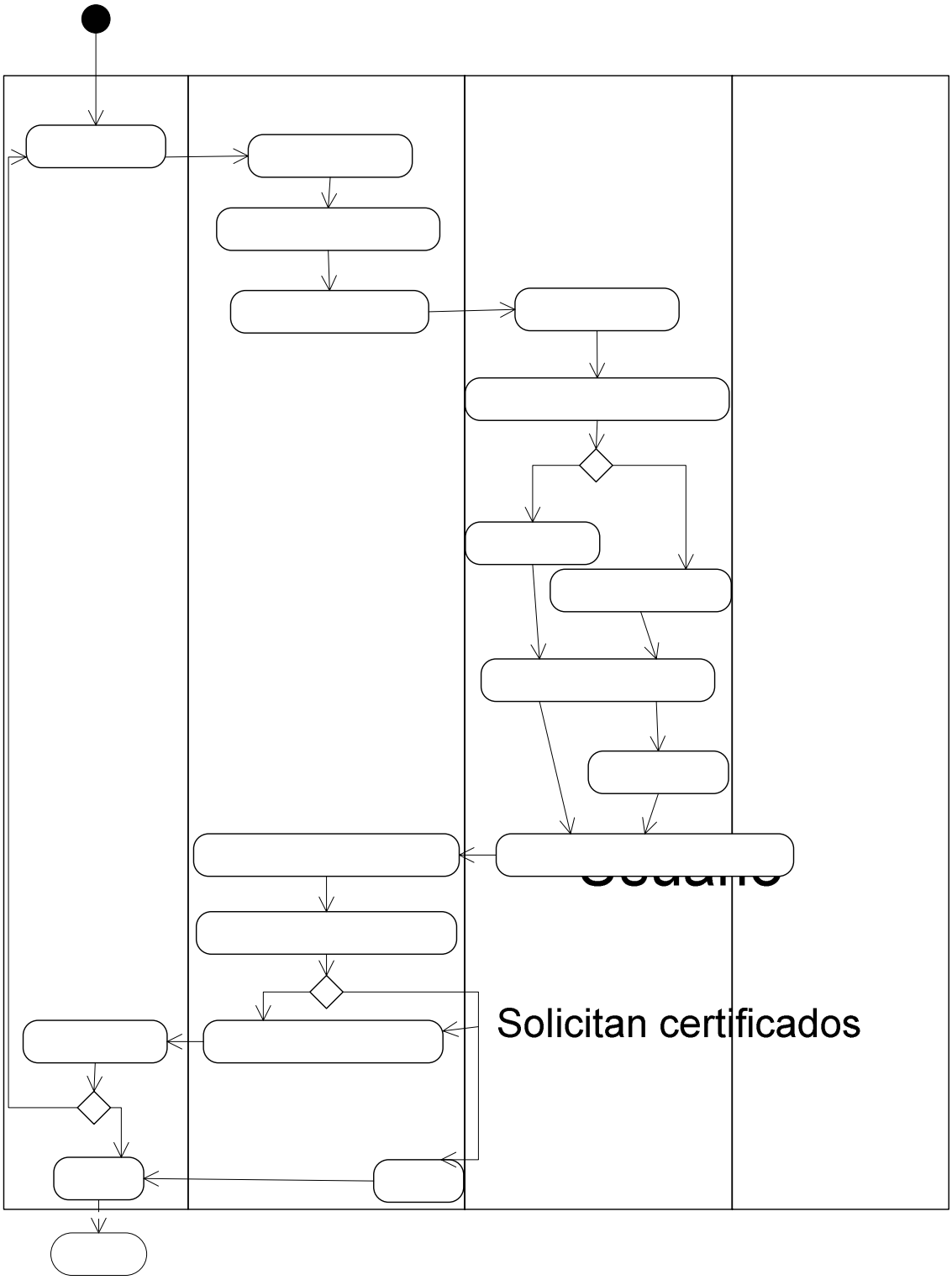
3.6.- Diagrama de Actividades. Expedición de un Certificado Digital en un *PSC*

En el diagrama de actividades que se muestra en la figura 31, se describen las actividades que deben realizar tanto los autores, como ciertos procedimientos de las interfaces que conforma el sistema del *PSC,* que ayudan al *PSC* a gestionar el proceso de expedir los certificados digitales.

En este diagrama se muestran los marcos de responsabilidad, cada marco de responsabilidad representan las actividades que se deben procesar para la expedición de un certificado digital en el *PSC* tanto como el actor como la interfaz responsable de dichas actividades. Cada marco de responsabilidad tiene un nombre único dentro del diagrama.

Nombre	Marco de responsabilidad
Usuario	Muestra todas la actividades que realiza el usuario en solicitar un certificado digital al *PCD*.
Componente *PUB*	Muestra todas las actividades que realizan tanto el *PUB* como su interfaz; cuyo interfaz corresponde a una parte del software que va a utilizar el *PSC*.
Componente *AR*	Muestra todas las actividades que realizan tanto el *AR* como su interfaz; cuyo interfaz corresponde a una parte del software que va a utilizar el *PSC*.
Componente *AC*	Muestra todas las actividades que realizan tanto el *AC* como su interfaz; cuyo interfaz corresponde a una parte del software que va a utilizar el *PSC*.

Tabla 24. Marcos de responsabilidades del diagrama de actividad


Solicitan certificados

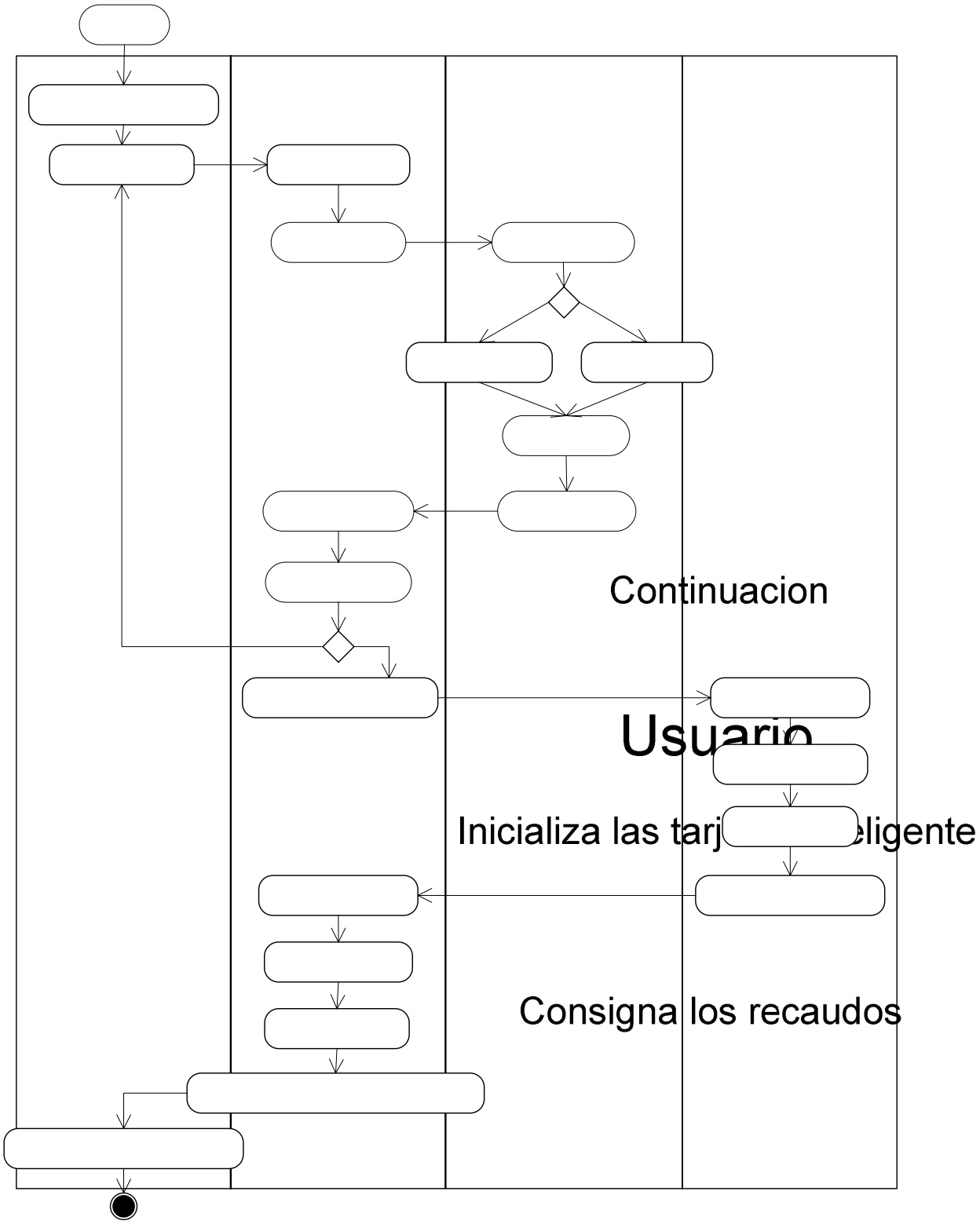


Figura 26. Diagrama de actividades para el proceso de solicitud de certificado digital.

3.6.1.- Actividad

3.6.1.1.- Solicita certificado

- Los usuarios acceden a la *URL* del *PSC* y realizar la solicitud de certificado, ingresando a un formulario datos validos y obligatorios.

- La página web del *PSC* registra la solicitud de los Usuarios, envía las solicitudes al repositorio del *PUB*.

3.6.1.2.- Almacena las solicitudes de certificados

- El interfaz del *PUB* almacena las solicitudes de certificados enviando por el usuario en el portal web del *PSC* en el repositorio.

3.6.1.3.- Verifica inicialmente las solicitudes

- El *PUB* revisa inicialmente las solicitudes que se almacenan en el repositorio, observando el registro y determina si existen algunas inconsistencias en la información, de existir alguna inconsistencia en la información, puede eliminar la solicitud y notificar al usuario, de no existir inconsistencia se envía las solicitudes a la *AR*

3.6.1.4.- Exporta las solicitudes a la *AR*

- El PUB envía las solicitudes que verifico inicialmente a la *AR*.

- El interfaz del *PUB* envía por unidad o por lote las solicitudes al repositorio de la AR.

3.6.1.5.- Almacena las solicitudes

- El interfaz de la *AR* almacena las solicitudes exportado por el *PUB* en el repositorio.

3.2.1.6.- Chequea la información de las solicitudes

- La *AR* chequea la información de las solicitudes que se almacena en el repositorio, donde revisa los registros de las solicitudes y verifica la información como por ejemplo: si se esta certificando a los empleados de una organización, se usa la base de dato de la organización para verificar los datos en el registro de la solicitud.

3.2.1.7.- Niega las solicitudes

- Si la *AR* no pudo verificar la información suministrada por los usuarios en las solicitudes, en el chequeo, negara la solicitud (Estado de la solicitud).

3.2.1.8.- Pre-aprobar las solicitudes

- Si la *AR* pudo verificar la información suministrada por los usuarios en la solicitud, en el chequeo, pre-aprobara las solicitudes (Estado de la solicitud).

3.2.1.9.- Firma las respuestas de las solicitudes

- La *AR* firmar el estado de las solicitudes (pre-aprobado o negado), usando la clave privada de la *AR*; por razones de responsabilidad.

- El interfaz de la *AR* firma digitalmente el estado de las solicitudes (Negado o pre-aprobado) por unidad o lotes utilizando la clave privada de la *AR*.

3.2.1.10.- Solicita los recaudos

- Si la solicitud fue pre-aprobada, la *AR* indica en una lista dentro de la interfaz *AR*, los recaudos que debe presentar los usuarios en función del tipo de certificado solicitado.

3.2.1.11.- Exporta las respuestas de las solicitudes

- La *AR* exporta el estado de las solicitudes firmadas y las solicitudes de recaudos al repositorio de la interfaz *PUB*.

- El interfaz de la *AR* permite que envíe por unidad o por lotes el estado de las solicitudes y las solicitudes de recaudos al repositorio de la interfaz PUB.

3.2.1.12.- Chequea las respuestas de las solicitudes

- El *PUB* chequea: el estado de las solicitudes para saber cual de las solicitudes están: pre-aprobado y cuales son los recaudos que deben presentar esos usuarios, las no aprobadas y La firma digital de la *AR* en el estado de las solicitudes.

- El interfaz del *PUB* chequea por lotes o unidad la firma digital del *AR* en la en estado de las solicitudes de certificados.

3.2.1.13.- Envía las respuestas de solicitud

- El PUB envía a los usuarios correo electrónico, donde indica el estado de la solicitud de certificado, y a los usuarios que tenga la solicitud pre-aprobada los recaudos que deben presentar.

- El interfaz del *PUB* admite que envíe por correo electrónico, el estado de las solicitudes de certificados y los cuales son los recaudos que deben presentar los usuarios con el estado de solicitud pre-aprobado.

3.2.1.14.- Recibe estado de solicitud

- Los usuarios reciben correo electrónico por parte del *PSC,* donde se le indica el estado de la solicitud de certificado y a los que tenga el estado de solicitud pre-aprobada los recaudos que deben presentar.

3.2.1.15.- Envía Kit

- El *PUB* prepara el kit (tarjeta inteligente, lector de tarjeta inteligente, pin, instrucciones de inicialización de la tarjeta inteligente) y se le envía a los usuarios que tienen la solicitud de certificado pre-aprobada.

3.2.1.16.- Recibe Kit

- Los usuarios reciben el Kit (tarjeta inteligente, lector de tarjeta inteligente, pin y instrucciones para inicializar la tarjeta inteligente), que envía el *PSC* de manera segura y verifican que llego completa y en buen estado.

3.2.1.17.- Inicializa las tarjetas inteligentes

- Los usuarios inicializan la tarjeta inteligente, ingresando a la *URL* del *PSC*, y siguiendo las instrucciones de inicialización que se entrego con el kit.

- El portal web del PSC genera de manera segura las claves (publica/privada) y las almacena en la tarjeta inteligente.

3.2.1.18.- Consigna los recaudos

- Los usuarios consigna los recaudos de acuerdo con el tipo de certificado que solicita al *PSC*, tales como: presentarse a la oficina del *PUB* para corroborar que es la persona que realizo la solicitud, fotocopia de la cedula de identidad, etc.

3.2.1.19.- Chequea los Recaudos

- El *PUB* revisa los recaudos que consigna los usuarios y si se presenta a la oficina, para corroborar que no le falte algún recaudo o si no se presenta el usuario a la oficina del *PUB*. Si le falta alguno recaudo, se le notifica a los usuarios para que los consigne.

3.2.1.20.- Exporta Recaudos

- El *PUB* envía los recaudos que consigna los usuarios a la *AR*.

3.2.1.21.- Chequea Recaudos

- El *AR* realiza el chequeo final de los recaudos de los usuarios que envía el *PUB*, verifica que los recaudos corresponde con la información en las solicitudes y se almacenan de forma segura y permanente.

3.2.1.22.- Aprueba las solicitudes

- Si la *AR* pudo chequear y verificar los recaudos de los usuarios, se aprueba la solicitud de certificado.

3.2.1.23.- Niega las solicitudes

- Si la *AR* no puede chequear y verificar los recaudos de los usuarios, no se aprueba la solicitud.

3.2.1.24.- Firma las respuestas

- El *AR* firma las solicitudes que aprueba o las solicitudes que niega; Por razones de responsabilidad.

- El interfaz de *AR* firmar digitalmente las solicitudes que aprueba o niega por unidad o lotes utilizando la clave privada de la *AR*.

3.2.1.25.- Exporta las respuestas

- El *AR* envía el estado de la solicitud de certificado que firma al *PUB*.

- El interfaz de la *AR* admite que envíe por lotes o por unidad el estado de las solicitudes de certificados al repositorio del PUB.

3.2.1.26.- Almacena las respuestas

- Se almacenan en el repositorio del PUB, las repuestas que exporta la *AR*.

3.2.1.27.- Chequea las respuestas

- *PUB* chequea las respuestas, para saber cuales solicitudes aprueba y cuales solicitud no aprueba el *AR*, también chequea la firma digital de cada una de las repuestas que exporta el *AR*.

- El interfaz del *PUB* chequea por lotes o por unidad las firmas digitales de la *AR* en las repuestas que exporta el *AR*.

3.2.1.28.- Exporta los certificados a la *AC*

- El *PUB* exportar los certificados digitales a la *AC*, para que las firmen.

- El interfaz del *PUB* admite que envíe por lotes o unidad los certificados digitales a la *AC*.

3.2.1.29.- Almacena los certificados

- Se almacena en el repositorio del interfaz de la *AC* o en un medio de almacenamiento portátil los certificados digitales que exporta el *PUB*.

3.2.1.30.- Chequea los certificados

- *AC* chequea la firma digital de la *AR* donde aprueba la expedición del certificado digital.

- El interfaz del *AC* chequea por lotes o por unidad las firmas digitales de la *AR*.

3.2.1.31.- firma los certificados

- Dos de las tres personas que componen la *AC* introducen sus respectivas tarjetas inteligentes en el dispositivo que realiza el proceso de firmar los certificados digitales con la clave privada del *PSC* para autenticar y validar el proceso de firmar los certificados.

3.2.1.32.- Exportar los certificados al *PUB*

- El *AC* exportar los certificados digitales al *PUB* para que se publique.

- El interfaz del *AC* admite enviar por lotes los certificados digitales al repositorio del *PUB*.

3.2.1.32.- Almacena los certificados

- Se almacena los certificados digitales firmados por la AC en el repositorio del interfaz del PUB.

3.2.1.33.- Chequea los certificados

- PUB debe chequear la firma digital de la *AC*

- El interfaz del *PUB* debe poder chequear por lotes las firmas digitales de la *AC*.

3.2.1.34.- Publica los certificados

- El *PUB* exporta en un repositorio público los certificados digitales expedidos por el *PSC*.

3.2.1.35.- notifica a los usuarios la expedición del certificado

- El *PUB* notifica a los usuarios por medio de correo electrónico la expedición del certificado.

- El interfaz del *PUB* admite que envíe correo electrónico a los usuarios.

3.2.1.36.- Notifica la expedición del certificado digital

- Los usuarios recibe la notificación de la expedición del certificado digital del *PSC* promedio de correo electrónico.

3.3.- Conclusiones del capítulo

Los diagramas *UML* que se muestran en este capítulo cubren las necesidades de modelado de un PSC, ya que visualizan y organizan acciones y requisitos que

pueden ser traducibles en software, hardware y políticas que forman parte del modelo.

En el siguiente capítulo, se discute los requisitos necesarios que se extraen de los diagramas que se explica en este capitulo para la puesta en marcha de un *PSC* y mas adelante se selecciona un conjunto de herramientas de software con licenciamiento libre que se adapte a los requisitos del modelo propuesto.

4.- Capítulo 4. Requisitos del *PSC*

En este capítulo, se utilizan los diagramas de Casos de Uso y los de Actividades descritos en el capítulo 3, para extraer los requisitos de software y hardware necesarios que permitan realizar todas las tareas vinculadas a la administración de los certificados digitales, con el fin de:

- Seleccionar un conjunto de herramientas de software con licenciamiento libre que se adapte a los requisitos del modelo propuesto.

- Examinar hardware que se complemente con el software y a las necesidades de seguridad.

- Determinar los roles de confianzas que debe cubrir el personal que va a laborar en el *PSC*.

4.1.- Requisitos de Software para el desarrollo del PSC

- Portal web, interfaz para el AC, AR y PUB donde cada uno de ellos pueda realizar sus actividades.

- Solicitud de un certificado por el usuario a través de portal web. El usuario debe ingresar unos datos básicos y obligatorios, por ejemplo, el número de cédula de identidad.

- Envía las solicitudes de certificado y almacenarla en un repositorio.

- Envío de correo electrónico a cada uno de los usuarios indicando el estado de su solicitud.

- Uso tarjetas inteligentes (SmartCard) compatible un nivel dos (2) de seguridad (algo que se tiene) para el control de acceso para los administradores.

- Generación de claves publicas/privadas que pueden ser guardadas en archivos con contraseña o en hardware criptográfico como tarjetas inteligentes y/o HSM.

- Exportación las solicitudes de certificados, certificados a los diferentes componentes del *PSC* (*AC, AR y PUB*) y al directorio donde se almacenarán todos los certificados (validos, revocados, expirados).

- Firma de las solicitudes de certificados y los certificados por lotes o en línea.

- Chequeo de las firmas en las solicitudes de certificado y certificados por lote y en línea.

- Uso del estándar *X.509*

- Exportación de los certificados firmados a un directorio central utilizando un protocolo y repositorio seguro, tal como el *LDAP*. En este directorio se almacenan todos los certificados digitales validos, revocados, caducados, o expedidos por el *PSC*.

- Publicación de un servidor *OCSP* encargado de verificar la validez de un de certificados digitales.

4.2.- Requisitos de Seguridad Lógica

- Autenticación fuerte para los *AC, AR, PUB* usando las tarjetas inteligentes y permitir el accesos a la interfaz de la *AC, AR* y *PUB* administran.

- Soporte del protocolo SSL para que la información que envía los usuarios se realice cifrada.

- Uso del módulo *HSM* donde se almacenara la clave privada del *PSC* y se firman los certificados expedidos por el *PSC*.

Se examina diferente software que administra una infraestructura de clave pública entre los que tenemos:

- *EJBC*, software que no es completamente libre hecho con java. [ref: www.ejbca.org]

- *NEWPKI*, software libre, basado en el *OpenSSL*, no cuenta con todos los componentes requerido en el modelo del *PSC*, ya que le falta el componente *PUB* [ref: www.newpki.org]

- *ROOTVE*, software libre, creado para administrar PSC Raíz, por sus características de seguridad lógica que realiza. [ref: www.ensi.funmrd.gov.ve]

- *OpenCA*, software libre, cuenta con la gran parte de los componentes requerido en el modelo del *PSC* por lo que es el software seleccionado y se describe el *OpenCA* en la siguiente sección. [ref: www.openca.org]

4.3.- Descripción del Software OpenCA

Se trata de un Software libre que esta basado en *CGI Scripts* en *Perl*. Es una herramienta que proporciona un interfaz web para poder administrar una infraestructura de clave publica capaz de manejar certificados *X.509*. El *OpenCA* utiliza varios productos de software de otros diseñadores de la comunidad *Open Source* tales como:

- Apache, servidor web.
- *Mod_ssl* modulo que le provee al servidor apache protocolo *SSL*.
- *OpenSSL* software que le suministrar las librerías de cifrado al *OpenCA*.
- *OpenLDAP* como servidor de directorio.
- *Perl* como lenguaje para el desarrollo de las *CGI Scripts* de los servidores web.

El *OpenCA* Se compone por módulos públicos que permiten la consulta y petición de certificado por parte del usuario, y otros módulos que son privados donde se realizan todas las tareas vinculadas a los certificados digitales de un *PSC*. El acceso a estas módulos esta restringido por nombre-cuenta y contraseña o por tarjeta inteligente de la persona responsable en la administraron del modulo.
Los módulos que maneja *OpenCA* son:

4.3.1.- Módulo *CA*

Por sus siglas en ingles *Certification Authority*. Módulo que tiene la tarea de administrar el uso de la clave privada del *PSC*. En general, la clave privada se usa

únicamente para firmar *CSRs* (*Certificate Signing Request*), *CRRs* (*Certificate Revocation Requests*) y *CRLs* (*Certificate Revocation List*).

Este módulo privado que va a utilizar la *AC*, en ella se realiza los siguientes procedimientos:

- Crea el certificado del *PSC* autoafirmado, en nuestro modelo no vamos a utilizar este procedimiento ya que el certificado se solicita a un *PSC Raíz*.

- Importar el certificado expedido por *PSC Raíz* en el directorio donde se almacenara.

- Genera los certificados de los administradores de la *AC*.

- Genera el certificado de la *AR*.

Estos procedimientos son necesarios realizarlos para poder operar el *PSC. Este* procedimiento se ejecuta una sola vez.

- Firmar *CSRs, CRRs y CRLs*.

4.3.2.- Módulo *RA*

Por sus siglas en ingles *Registry Authority*. Este modulo es privado y es el que usa la *AR*. La principal función del módulo *RA* es proveer de la interfaz necesaria para la aprobación de las solicitudes que luego serán enviadas a la *CA*. El operador de la *RA*, de acuerdo a las políticas definidas, acreditará cada solicitud y la firmará con su clave privada. En ella se realizan los siguientes procedimientos:

-

- Acceder al directorio *CSRs* y *CRRs* donde se encuentra almacenado las solicitudes de certificado y revocación de certificado respectivamente, puede revisar la información suministrada por el usuario en las solicitudes y poder verificar y autenticar la información.

- Aprobar o anular tanto las solicitudes de certificado como las de revocación.

- Firmar las solicitudes de certificados *CSRs* y la solicitud de revocación de los certificados *CRRs* que fueron aprobadas por la *AR*.

4.3.3.- Módulo *PUB*

Este es el módulo público que va utilizar los usuarios, Consiste en una interfaz de consulta y de solicitud de certificados, solicitud de revocación de certificados, además de algunas otras funcionalidades de interés para usuarios finales.

4.3.4.- Módulo *LDAP*

Posibilita la actualización del directorio *LDAP* donde se encuentra almacenado los certificados validos, caducados y revocados. Es posible agregar y eliminar certificados y *CRLs* del directorio. Dicho directorio puede residir local o remotamente.

4.3.5.- Módulo *Node*

Una instalación distribuida de *OpenCA* consiste en la instalación de componentes distintos de *OpenCA* en máquinas distintas, esto es, la instalación de distintas instancias de *OpenCA* en máquinas distantes. Cuando se usa una instalación de este tipo es necesario instalar en cada máquina la interfaz de administración que permite realizar, entre otras, la sincronización de las bases de datos entre las

máquinas distantes. Este módulo abstrae las funcionalidades comunes para todos los módulos ya mencionados; como por ejemplo la base de datos. Cada nodo posee una base de datos propia idéntica en estructura a la de cualquier otro nodo. Gracias a la interfaz de administración, es posible ver una instalación distribuida de *OpenCA* como un conjunto de nodos que puedes interactuar entre ellos.

4.3.6.- Módulo *BATCH*

Este modulo es utilizado para realizar procesos tales como: Revisar las *CSRs* o *CRRs*, aprobar las *CSRs* o *CRRs*, firmar las *CSRs*, *CRRs* o los certificados digitales que se acumulen en un directorio y poderlos procesarlos por lotes.

4.4.- Uso del sistema para la solicitud de certificado cuando todos los módulos están instalados en una maquina

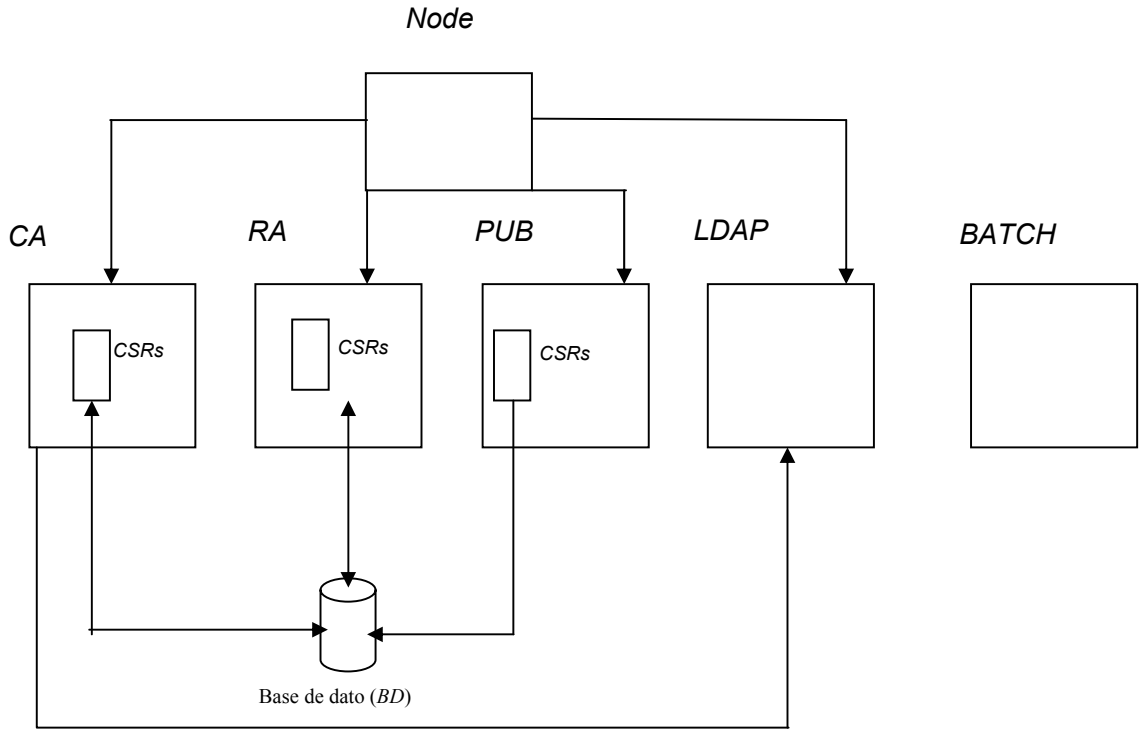


Figura 27. Descripción de los procesos que realizada el software OpenCA para expedir un certificado digital si todos los componentes están instalados en una sola maquina.

Si los componentes de la aplicación están instalados en una misma máquina, la base de datos será común para todos los módulos, de no ser así, cada módulo tendrá una base de datos propia que podrá ser sincronizada con los demás nodos de acuerdo a la configuración propia de los nodos en cuestión

El mecanismo normal de uso es de la figura 27:

1. Un usuario se conecta al servidor público por *SSL*. El navegador le avisará de que no reconoce la autoridad firmante del certificado del servidor. Al entrar seleccionará la primera opción (cargar el certificado del *CA*).

2. El usuario estando dentro de módulo *PUB* realiza el proceso de solicitud de *CSRs*

3. El *CSRs* se almacenara en la *BD*.

4. El *AR* dentro del módulo *RA* accederá a la *BD* y procederá a verificar la información y luego anular o aprobar la *CSRs*.

5. Se almacenara los *CSRs* aprobado por *AR* en la *BD*.

6. El AC dentro del módulo *CA* se conecta a la *BD*.

7. Genera certificados y los firma.

8. Los certificados se almacenan en el módulo *LDAP*.

4.5.- Paquetes de software necesarios para instalar el *OpenCA*

Para poder instalar el *OpenCA*, es necesario instalar previamente unos paquetes de software con licenciamiento libre tales como:

Perl versión *5.8.7-debian* y los siguientes módulos:

Módulo	versión	Módulo	versión	Módulo	versión
libnet-server-perl	*0.90-1*	*libdbi-perl*	*1.50-1*	*libauthen-sasl-perl*	*2.09-1*
libxml-perl	*0.08-1*	*perl-modules*	*5.8.7-10debian1*	*libx500-dn-perl*	*0.28-1*
libxml-regexp-perl	*0.03-7*	*libdbd-mysql-perl*	*3.0002-2build1*	*libcgi-session-perl*	*4.13-1*
libconvert-asn1-perl	*0.19-1*	*libdigest-md2-perl*	*2.03-1*	*libdigest-md4-perl*	*1.5-1*
libdigest-sha1-perl	*2.10-1*	*libio-socket-ssl-perl*	*0.97-2build1*	*libio-stringy-perl*	*2.110-1*
libmime-lite-perl	*3.01-6*	*libmime-perl*	*5.419-1*	*libmailtools-perl*	*1.62-1*

Tabla 25. Módulos de Perl para instalar el openCA

- *Apache* versión y los módulos

Módulo	versión	Módulo	versión	Módulo	versión
libapache-mod-perl	*.29.0.4-2debian*	*libapache-mod-ssl*	*2.8.25-1*	*mod_ssl*	

Tabla 26. Módulos de Apache

- *OpenSSL* versión *0.9.8a-7debian* y el módulo *libssl-dev*
- *OpenLDAP*
- *OpenCA* versión *0.9.2.5*.
- OpenSC-ceres.

4.6.- Requisitos de hardware para el desarrollo del modelo del *PSC*

4.6.1.- Computadora

Componentes	Requisitos
Procesador	PC con procesador de ultima generación
Memoria	> 1 GB de RAM o superior
Disco Duro	> 200 GB
Tarjeta de Red	
Dispositivo Backup	
Sistema Operativo	Red hat fedora, Mandriva, Debian, Knoppix, Ubuntu o una distribución personalizada que derive de Debian sarge para aumentar la seguridad del sistema de la *PSC*

Tabla 27. Requerimiento de las computadoras para el desarrollo del modelo del PSC

4.6.2.- Lectoras de tarjetas inteligentes y Tarjetas Inteligentes marca C3PO modelo LTC31

El kit esta conformado por:

- Lector y grabador externo.
- Tarjeta inteligente.
- Manuales de lector y tarjetas.

- Driver de comunicación.
- Kit de desarrollador para programación de aplicaciones genéricas con tarjetas chip.

Autenticación nivel 2

4.6.3.- Tarjeta *HSM* (Modulo de hardware seguro)

Componentes	Requisitos
HSM modelo nshield806	> Algoritmos estándar tales como SHA1, SHA256, AES,

Tabla 28. Requerimiento de la Tarjeta HSM para el desarrollo del modelo del PSC

4.6.4.- Servidor

Componentes	Requerimientos
Procesador	Doble Núcleo > 2 GHZ
Tarjeta de red	Adaptador de red de doble puerto
Capacidad de red	
Disco duro	Disco duro de 300 GB (10000rpm)
Sistema operativo	Debian sarge 3.1

Tabla 29. Requerimiento de los servidores para el desarrollo del modelo del PSC

4.7.- Arquitectura del hardware en el modelo del *PSC*

En este diagrama (Figura 33) se muestra como se instalan los hardware en función de los módulos del *OpenCA* descrito en la sección 4.3 y a las necesidades del modelo.

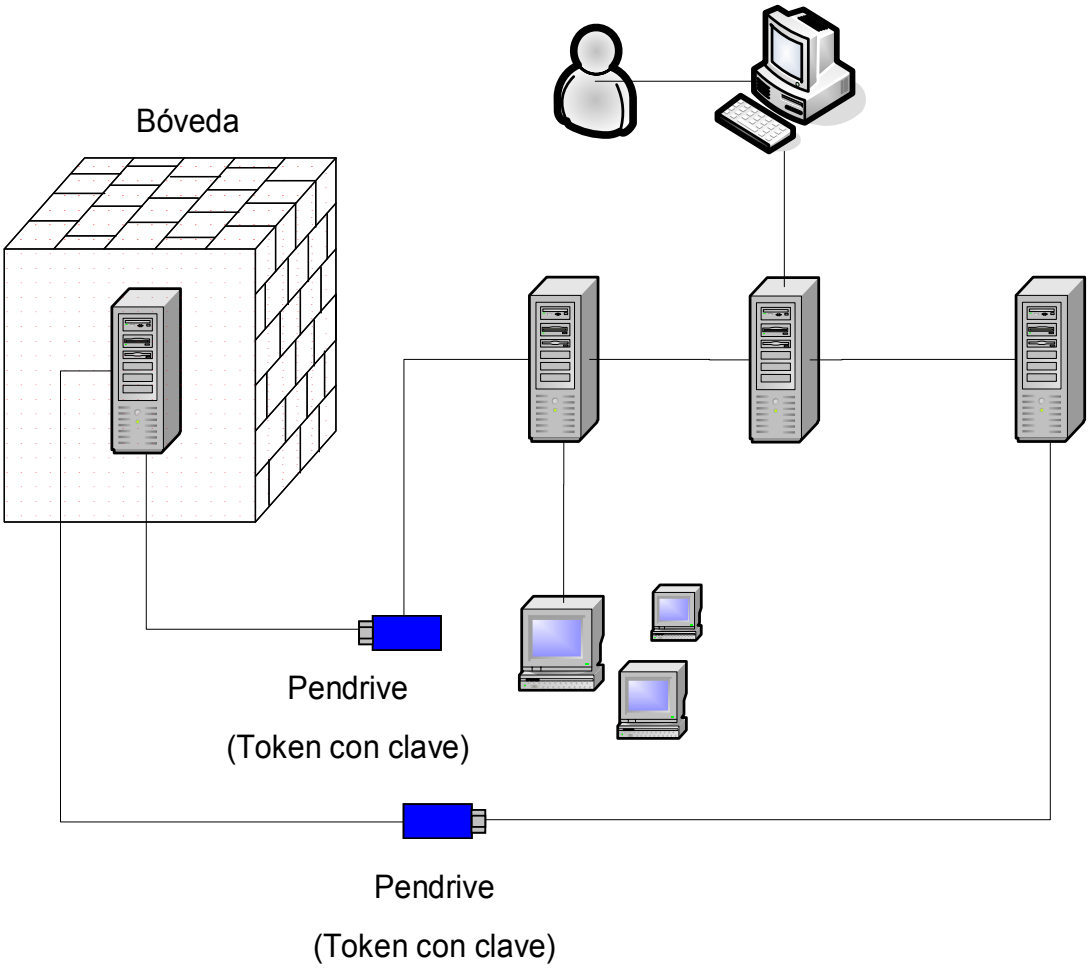


Figura 28. Arquitectura del hardware en el modelo del PSC.

Servidor *PUB/LDAP*: En este servidor los usuarios gestionan las solicitudes de certificados.

Servidor AR: En este servidor se realizan las actividades de la *AR.*

Servidor AC: En este servidor se realizan las actividades de la *AC* y donde esta instalado en *HSM.*

Servidor *OCSP/CRL:* servidor encargado de verificar la validez de los certificados digitales

Verificadores: Personas que realizan el proceso de autenticar la identidad de los usuarios

4.8.- Diagrama de despliegue

En este diagrama (figura 34) se muestra los software que se instala en los hardware mostrados en la figura 33, para que realice las actividades especificadas.

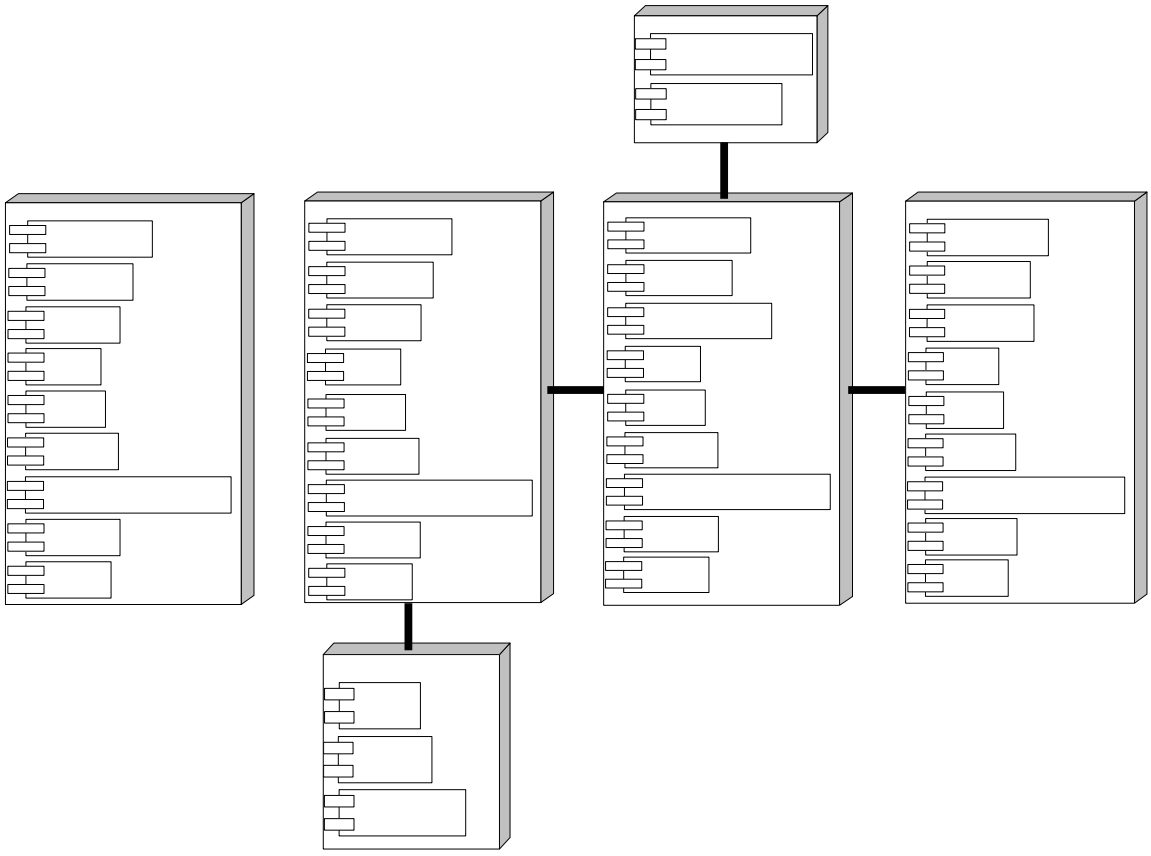


Figura 29. Diagrama de despliegue. Configuración del hardware y software en el modelo del PSC.

4.9.- Requisitos del Personal para el desarrollo del PSC

La *PSC*, debe contar con personal que por sus actividades son sometidos a procedimientos de control especial debido a que su actividad es esencial para el correcto funcionamiento de la *PSC*. Así tiene la consideración de roles de confianzas:

1. Administrador del *HSM*: 1 funcionario tendrá asignado este rol. un administrador del *HSM* esta encargado de:

    - Definición de las claves de administración del *HSM*.
    - Custodiar el *HSM*.
    - Configurar y poner en marcha el *HSM*.

2. Operador HSM: 1 funcionario tendrá asignado este rol. Un operador de HSM esta encargado de:

    - Configurar el acceso a las aplicaciones al *HSM*.
    - Asistir en las tareas de exportación e importación del material cifrado del *HSM*.

3. Operador Backup: 1 funcionario tendrá asignado este rol. El operador del Backup esta encargado de:

    - Ejecutar respaldos del servidor donde está instalado el servicio del CA y de su base de datos.

- Ejecutar recuperaciones del servidor donde está instalado el servicio del CA y de su base de datos.

4. Administrador de Auditoria: 3 funcionarios tendrá asignado este rol. El administrador de auditoria esta encargado de:

   - Configurar las bitácoras de auditoria.
   - Revisar las bitácoras de auditoria.
   - Mantener las bitácoras de auditoria.

5. Administrador de recuperador de claves: 2 funcionarios tendrán asignado este rol. El administrador de recuperador de claves esta encargado de:

   - Restituir una llave privada almacenada en el *AC*.

6. Administrador de certificado: 3 funcionarios tendrán asignado este rol. El Administrador de certificado esta encargado de:

   - Aprobar solicitud de certificado.
   - Denegar solicitud de certificado.
   - Revocar solicitud de certificado.

Estos roles de confianzas son realizados por los actores del *PSC*, tales como: *AC*, *AR*, *PUB*, gerentes, socios, dueños, etc, que tiene una participación dentro de la *PSC*. Un autor puede desempañar varios roles.

4.10.- Conclusiones del Capítulo

Se examinó los requisitos que debe cumplir el software y se logró seleccionar un conjunto de aplicaciones con licenciamiento libre (*OpenCA, Apache, OpenSSL*, *OpenSC-ceres, OpenLDAP*) con unas características en coherencia como las requeridas. A partir de las características descriptas en el capitulo del *OpenCA* y de los requisitos de hardware, se realiza el diagramas de despliegue (figura 34) y otro de configuración física que muestra la forma en que los hardware se instala en el modelo del *PSC* (figura 33).

En el siguiente capítulo se muestra las pruebas de algunos módulos y funciones del software *OpenCA* con el fin de contrastarla con los casos de usos descrito en el capitulo 3.

5.- Capítulo 5. Pruebas de algunos módulos y funciones del *OpenCa*

En este capítulo, se realizan pruebas de algunos de los módulos y funciones software *OpenCa* con el fin de contrastarla con los diagramas de casos de usos descrito en el capitulo 3 y con los requisitos de software y de seguridad lógica para el desarrollo del *PSC* descrito en el capitulo 5. Se realizan las capturas de todas las interfaces que participan en el proceso de solicitar certificado digital.
Se instalan todos los requisitos de software descrito en el capitulo 4 en una máquina de escritorio tales como:

- Sistema operativo *Debian sarge 3.1*
- Servidor *Apache* y el modulo *mod_ssl*.
- *Perl* y sus módulos.
- *OpenSSL*.
- *OpenLDAP*.
- *OpenCA* versión *0.9.2.5*.
- *OpenSC-ceres*.

Donde también se instaló y configuró los componentes de la aplicación *OpenCA* (los módulos *CA*, *RA*, *PUB*, *LDAP*), cuyo funcionamiento se describe en el capitulo 4, figura 27.

La figura 30 corresponde a un modelo que se realizo de portal web de un *PSC,* que correspondería al módulo *PUB* del OpenCA, donde los usuarios realizan consultas y donde realizan las solicitudes de certificado, solicitud de revocación de certificados. Se integro este portal web con los módulos del O*penCA.*

Figura 30. Módulo PUB.

La figura 31 es una de las interfaz del módulo *PUB* traducida a español, donde los usuarios introducen los datos para realizar la solicitud de certificados.

Figura 31. Módulo PUB. Formulario de requisitos para realizar la solicitud

Figura 32 es una de las interfaz del módulo *PUB* traducida a español, donde el usuario puede observar la información que suministro en el formulario y chequearla, si esta de acuerdo con la información se hace click sobre la pestaña continue para enviar y almacenar la solicitud en la base de datos.

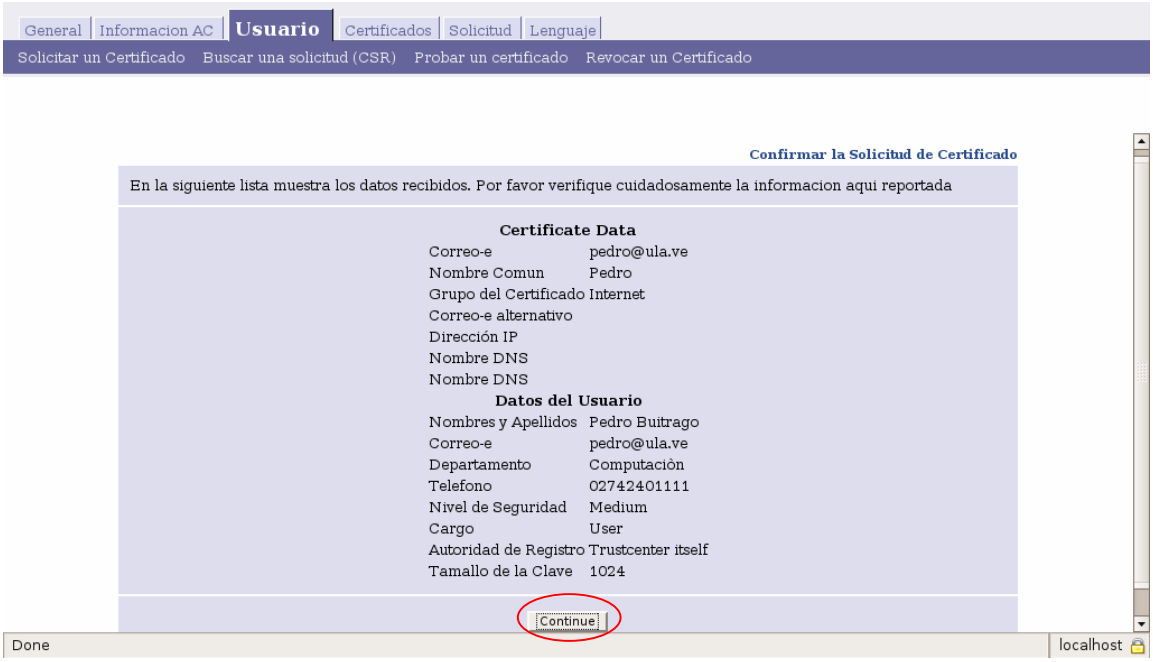


Figura 32. Módulo PUB. Registro de la información introducida por el usuario.

Todos estos pasos correspondería al caso de uso: Solicitud de certificado descrito en la tabla 1 del capitulo 3.
Los pasos que se realizan en las figuras 30, 31 y 32 permite que el usuario:

- Realice la solicitud de certificado por Internet conectándose a la interfaz de la figura 30.

- Envíe la solicitud de certificado y almacenarla en un repositorio.

Y de esta manera cubren dos de los requisitos de software para el desarrollo del *PSC*, descrito en el capitulo 4 sección 4.1.

Figura 33 muestra la restricción que realiza el *OpenCA* al módulo *RA,* autenticando a la *AR* por cuenta y contraseña al módulo *RA*.

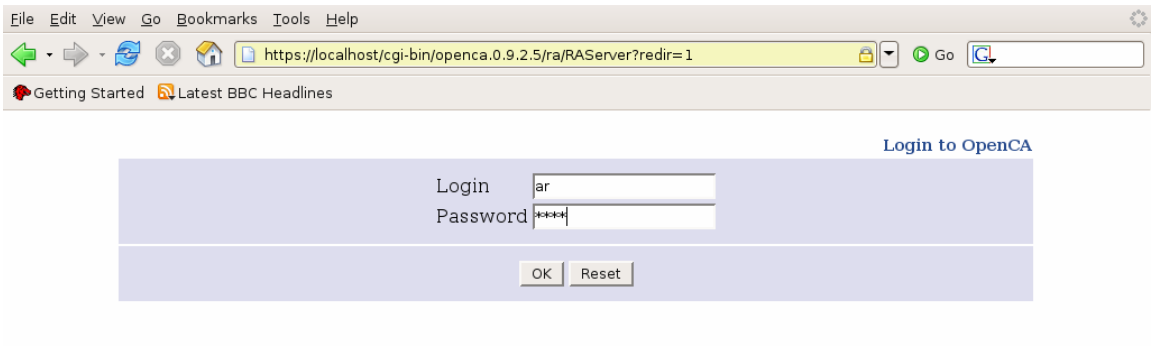


Figura 33. Control de acceso al módulo RA

La restricción que realiza el *OpenCa* en el módulo *RA*, cubre con una de los requisitos de seguridad lógica descrito en el capitulo 4 sección 4.2

Figura 34 muestra el directorio *CSRs* del módulo *RA* traducida a español, donde se almacenan las solicitudes certificados enviada por los usuario a través del módulo *PUB*. En el directorio aparece la solicitud con el serial 9760 que corresponde a la solicitud que se mostró en la figura 31

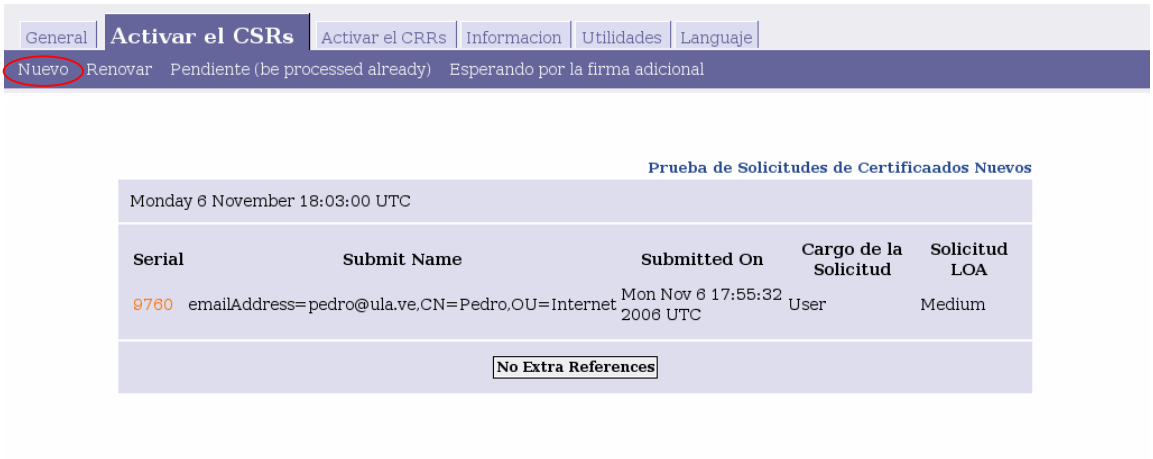


Figura 34. Módulo RA. Directorio CSRs donde se almacena las solicitudes realizadas por los usuarios en el módulo PUB.

Todos los pasos que se realizó en la figura 33 y 34, correspondería al caso de uso: Acepta solicitud de certificado descrito en la tabla 15 del capitulo 3.

Figura 35 es una de las interfaz del módulo *RA* traducida a español, donde se muestra el formato de la solicitud con el numero de serie 9760 del directorio CSRs de la figura 34, realizada por el usuario Pedro donde aparece la información suministrada. *AR* puede chequear la información y poder determinar si aprueba o niega la solicitud de certificado.

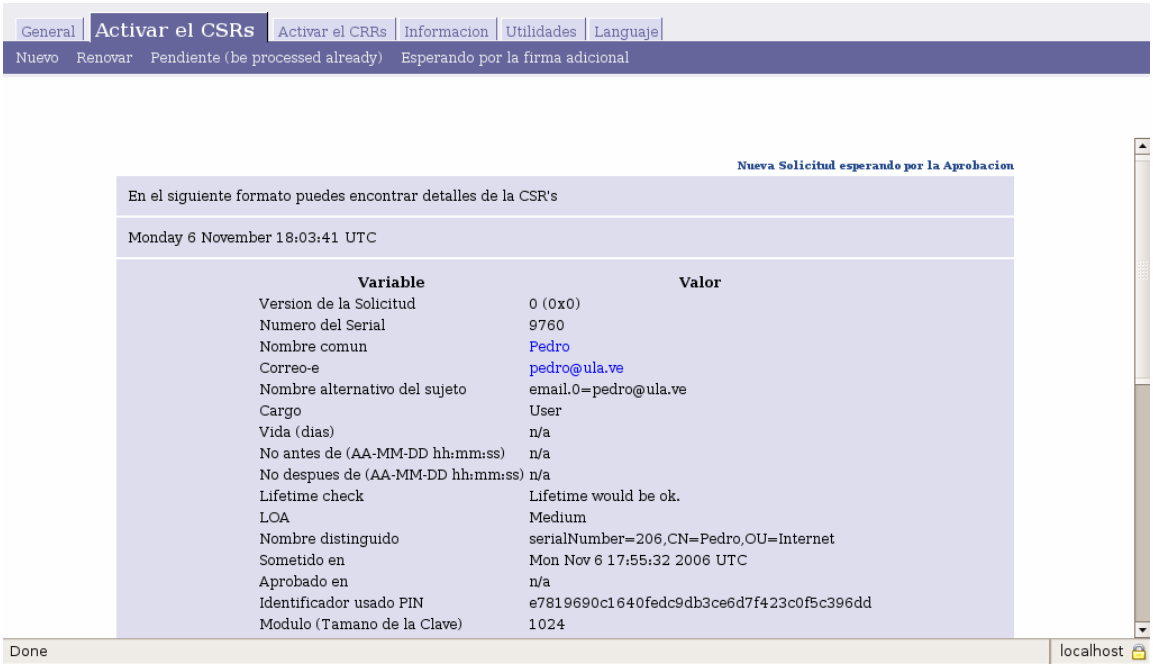


Figura 35. Módulo RA. Registro del usuario.

La figuras 34 y 35 corresponde al caso de uso: Chequear la información de la solicitud de certificado descrito en la tabla 16 del capitulo 3.

Figura 36 muestra como se aprueba y firma o se elimina la solicitud de certificado en el módulo *RA*. Una vez verificado la información se le da click a la pestaña Aprobar solicitud, para aprobar y firmar la solicitud y para eliminar la solicitud se da click en la pestaña Eliminar solicitud. Aparecen otros procesos tales como Editar

solicitudes, donde el *AR,* agregar a la solicitud entre otras cosas, como la fecha, hora en que se expidió y fecha, hora cuando caduca el certificado .

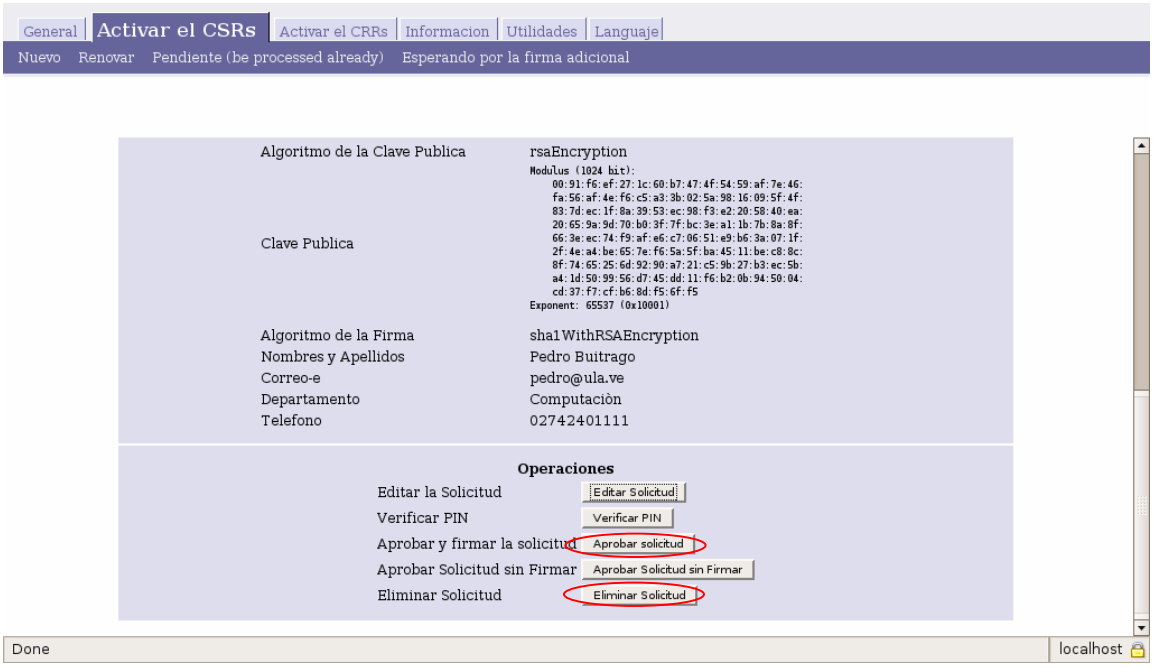


Figura 36. Módulo RA. Aprobar o eliminar solicitud

Este paso correspondería en parte a los casos de usos de uso, aprobar la solicitud de certificado y negar la solicitud de certificados descrito en las tablas 17 y 18 respectivamente del capitulo 3.

Estos procesos que se realiza en las figuras 34, 35 y 36 permiten a la *AR*:

- Verificar la validez de la información suministrada por el usuario que corresponde a una de las responsabilidades principales de la *AR*.

- Agregar a la solicitud información como por ejemplo, la fecha, hora de la expedición

- Aprobar y firmar o negar las solicitudes de certificados si pudo verificar la información

- Exportar las solicitudes aprobadas al módulo *AC.*

Figura 37 muestra la restricción que realiza el *OpenCA* al módulo *CA,* autenticando a la *AC* por cuenta y contraseña al módulo *CA*.

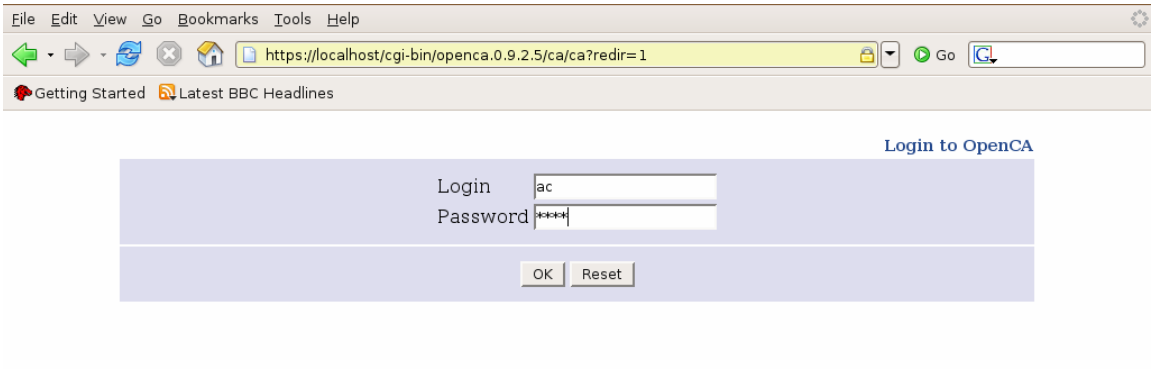


Figura 37. Control de acceso al módulo CA

La restricción que realiza el *OpenCa* en el módulo *CA*, cubre con una de los requisitos de seguridad lógica descrito en el capitulo 4 sección 4.2

Figura 38 Muestra el directorio *CSRs* del módulo *CA* donde se almacenan las solicitudes de certificados aprobado por el *AR* desde el módulo *RA*.

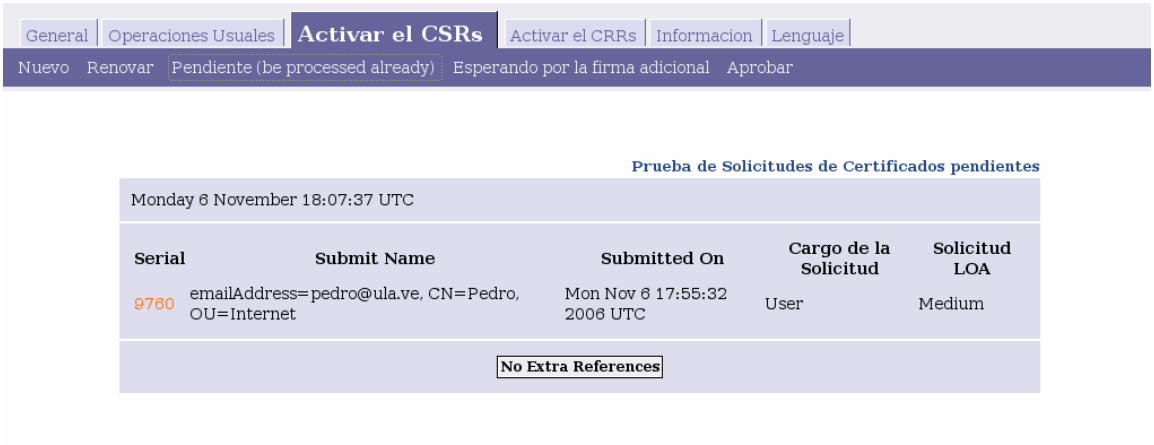


Figura 38. Módulo CA. Directorio CSRs donde se almacenan las solicitudes aprobada por la AR el módulo RA.

Todos estos pasos correspondería al caso de uso: Aceptad los certificado por la *AR* descrito en la tabla 22 del capitulo 3.

Figura 39 muestra el formato de la solicitud con el numero de serie 9760 del directorio *CSRs* del modulo *CA* donde aparece la información suministrada por el usuario Pedro

Figura 39. Modulo CA. Registro del Usuario.

Figura 40 muestra como se firma o se elimina el certificado. Una vez verificado la información se le da click a la pestaña Expedir certificado para firmar la solicitud y expórtalo al modulo *LDAP*, para eliminar la solicitud se da click en la pestaña Eliminar solicitud

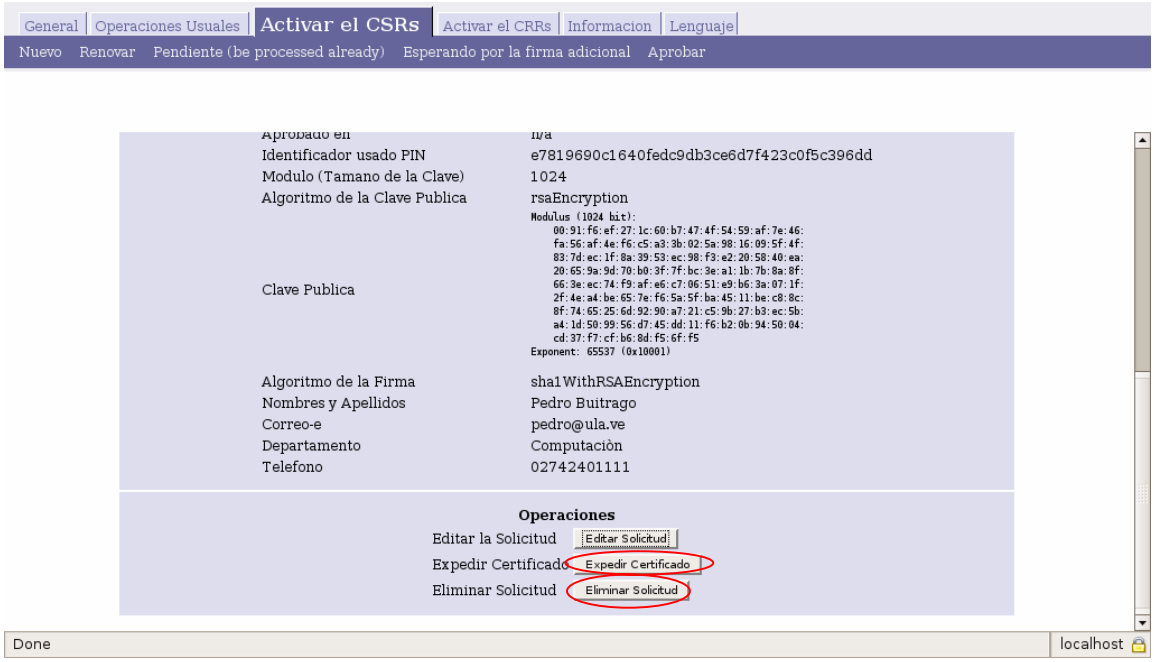


Figura 40. Modulo CA. Firmar o eliminar solicitud

Figura 41 para realizar el proceso de firmar la solicitud se debe ingresar el password del *AC* que seria el *PIN* utilizado en la creación del certificado de la *AC*

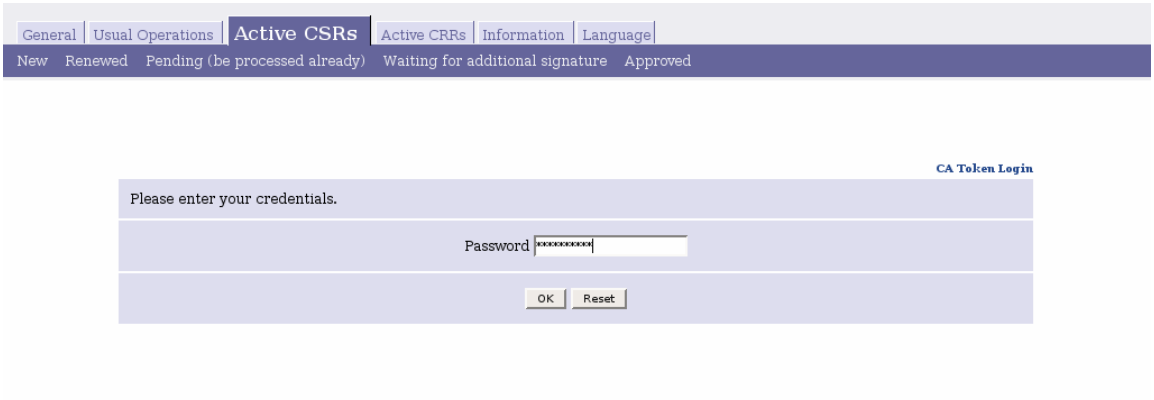


Figura 41. Control de acceso para firmar los certificados

Este paso correspondería en parte a los casos de usos de uso, firmar el certificados usando la clave privada del PSC, descrito en las tablas 23 del capitulo 3.

Estos procesos que se realiza en las figuras 38, 39, 40 y 41 permiten a la *AC*:

- Firmar los certificados digitales expedidos por el *OpenCA*, que corresponde a unas de las responsabilidades principales de la *AC*.

- Exportar los certificados digitales, que en este caso, directamente al módulo *LDAP*.

La figura 42 corresponde al módulo *LDAP* donde muestra los certificados validos expedidos por el *OpenCA*.

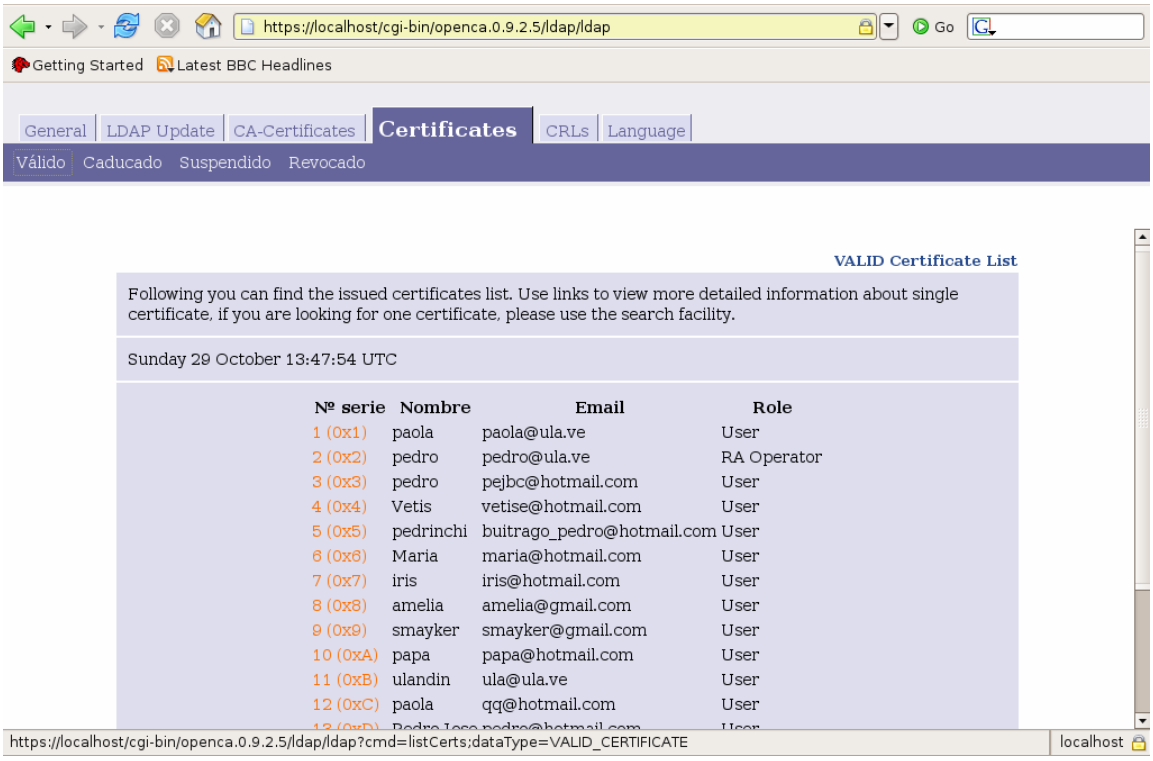


Figura 42. Certificados validos expedidos por el OpenCA

5.1.- Conclusiones del Capitulo

Las pruebas, que se realizaron a algunos módulos y funciones del *OpenCA*, determinaron que cubre con la mayoría de los requisitos, acciones y casos de usos, descrito en el capitulo 3 capitulo 4.
Debido al licenciamiento libre del *OpenCa*, se puede agregar los casos de uso que en su funcionamiento original no realiza y poder adaptarlo a las necesidades del modelo.
Al *OpenCA* se puede configurar para adaptar el *HSM*.
Con las características que nos ofrece el *OpenCA* en relación con:

- Sus componentes integrados por los módulos *CA, RA, PUB, LDAP* y *OCSP* cubren con las interfaces requeridos en el modelo.

- Su funcionamiento, incorporara las actividades que deben realizar la AR, AC y el PUB tales como firmar, chequear, aprobar, enviar, recibir, almacenar, etc.

- El software libre. Entre otras cosas, introducir funciones que el *OpenCA* no realiza para que se adapte al modelo propuesto, permite cambiar el diseño de las interfaces y poder ser objeto de una auditoria.

Se demuestra que el *OpenCA* se puede utilizar como sistema para la administración de los certificados digitales en el modelo del *PSC* propuesto.

6.- Capitulo 6. Conclusiones Generales

Es importante tener conocimiento sobre las características que deben cubrir los sistemas informáticos para que se consideren seguros. Estas características son: confidencialidad, integridad y repudio. Existen en el mercado tecnologías desarrolladas tanto en software y hardware (cifrado, firma digitales, certificados digitales, tarjetas inteligentes, etc), que proporciona las características anteriormente señaladas. Por otro lado la legislación venezolana permite que se pueda implementación de una ICP con el fin de brindar un nivel adecuado de seguridad en las transacciones a través de la red.

Tener como base las políticas de certificación de los PSC, que son estándares para modelar al PSC.

Los diagramas *UML* cubren las necesidades de modelado de un PSC, ya que tienen el objetivo de visualizar y organizar acciones y recursos traducibles en software, hardware y políticas que forman parte del modelo. Se extraen los requisitos que debe cumplir el software y se selecciona un conjunto de aplicaciones con licenciamiento libre (*OpenCA, Apache, OpenSSL*, *OpenSC-ceres, OpenLDAP*) con unas características en coherencia como las requeridas. A partir de las características descritas en el capitulo 4 del *OpenCA* y de los requisitos de hardware, se realiza el diagrama de despliegue (figura 34) y otro de configuración física que muestra la forma como se instalan los hardware en el modelo del *PSC* (figura 33).

Las pruebas, que se realizan a algunos módulos y funciones del *OpenCA*, determinan que cubre con la mayoría tanto de los casos de uso, descrito en el capitulo 3, como los requisitos de software y seguridad lógica descrito en el capitulo 4, para el desarrollo del *PSC*.

Como se tiene el código fuente del *OpenCa*, se pueden agregar los Casos de Uso que en su funcionamiento original no realiza, y poder adaptarlo a las necesidades del modelo.

Al *OpenCA* se puede configurar para adaptar el *HSM*.

Con las características que nos ofrece el *OpenCA* en relación con:

- Sus componentes integrados por los módulos *CA, RA, PUB, LDAP* y *OCSP* cubren con las interfaces requeridos en el modelo.

- Su funcionamiento, incorporara las actividades que deben realizar la AR,AC y el PUB tales como firmar, chequear, aprobar, enviar, recibir, almacenar, etc.

- El software libre. Entre otras cosas, introduce funciones que el *OpenCA* no realiza para que se adapte al modelo propuesto, permite cambiar el diseño de las interfaces y poder ser objeto de una auditoria.

Se demuestra que el *OpenCA* se puede utilizar como sistema para la administración de los certificados digitales en el modelo del *PSC* propuesto.
Finalmente se debe resaltar el hecho de que todos los objetivos propuestos en este trabajo fuéron alcanzados a la altura de las expectativas creadas. Particularmente me siento muy satisfecho y honrado; por haber participados de la forma mas directa en la elaboración y desarrollo de este trabajo, que sin lugar a dudas será utilidad para quien se propone implementar un *PSC*.

6.1.- Recomendaciones:

- Validar y desarrollar Casos de uso para la generación de la clave del *PSC.*

- Evaluar con la práctica las políticas de seguridad.

- Mejorar aspectos de la aplicación que satisfagan requisitos o acción del PSC no tomadas en el modelo, tales como protocolos de conexión mas seguros para que el servidor *AC* este en línea, o si se desarrolla un software o hardware que mejora la seguridad en las aplicaciones del modelo.

Bibliografía

[1] Andrew Nash, 2002. “PKI Infraestructura de claves publicas (la mejor tecnología para implementar y administrar la seguridad electrónica de su negocio)”. Editorial McGRAW-HILL Interamericana Bogota (Colombia).

[2] Kaufman Charlie. “Network Security Prentice”. Hall 1995 USA.

[3] Joseph Schmuller. “Aprendiendo UML en 24 horas”, Editorial Prince hall,

[4] Grady Booch, 1999. “UML lenguaje Unificado de Modelado”. Editorial Addison Wesley Iberoamericana Madrid (España).

[5]. Pierre-Alain Muller, 1997. “Modelado de objetos con UML”. Editorial Enrolles paris.

Apéndice A. Glosario de términos:

Algoritmo: funciones matemáticas, como las que se usan para cifrar de descifrar información.

Autenticación: la acción de verificar información, como identidad, propiedad o autorización.

Autorización: El otorgamiento de privilegios de acceso apropiados a usuarios autenticados.

***AC*:** Emitirá a petición de la Autoridad de Registro los certificados que se precisen de forma automatizada.

Algoritmo asimétrico: Algoritmo matemático que utiliza dos claves: una (publica/privada), utilizada para descifrar, y la otra (pública/privada), empleada para cifrar.

Algoritmo simétrico: Algoritmo matemático que utiliza la misma clave (clave simétrica) para cifrar y descifrar.

***AR*:** Autorizada por la *AC* para registrar a los usuarios que solicitan los certificados digitales al proveedor de servicios de certificado digitales.

BD: Base de dato

Certificado digital: Es un documento electrónico, en el cual la *AC* acredita mediante su firma digital que la clave pública pertenece a su propietario. También se denominan certificados de usuario y de clave pública.

Cifrado: La transformación de texto claro en una forma aparentemente menos legible (texto cifrado), a través de un proceso matemático.

Clave privada: Clave personal que no es conocida por el resto de los usuarios y que es utilizada para crear firmas digitales y para descifrar mensajes cifrados con la correspondiente clave pública.

Clave pública: Clave de usuario que es conocida por el resto de los usuarios y que es utilizada para verificar firmas creadas con su correspondiente clave pública y se usa para cifrar mensajes que pueden ser descifrados con su correspondiente clave privada.

Clave simétrica: Clave utilizada en los algoritmo simétricos para cifrar y descifrar los mensajes.

CRLs: *Certificate Revocation List*, Listas de Certificados revocados. Definido en la norma X.509.

CRRs**:** *Certificate Revocation Requests*.

CSRs: *Certificate Signing Request*.

Emisión de certificados: Acciones llevadas a cabo por una *PSC* para crear un certificado y comunicárselo al usuario que lo solicitó.

Expiración de un certificado: Fecha y hora especificadas en un certificado cuando termina el período operativo del mismo.

Firma digital: Es un documento electrónico que se genera como resultado de aplicar una función matemática al documento a firmar y posteriormente, cifrar el

resultado con la clave privada del firmante. Es utilizada por el emisor de un mensaje para identificarse.

***ICP*:** Conjunto de mecanismos de cifrado de clave pública basados en la existencia de dos claves (una pública y otra privada) que se utilizan para garantizar la identidad del usuario, la confidencialidad y la integridad de la información transmitida.

***LDAP*:** Light Directory Access Protocol. Protocolo para acceder a datos y buscar contenidos en directorios normalizados.

LMU: Lenguaje de modelado unificado

***OCSP*:** Online Certificate Status Protocol. El protocolo de estado de certificado en línea. Permite la delegación de la validación del certificado. Ofrece repuesta inmediata y actualizada en las consultas de los estados de los certificados.

***PIN*:** Número de Identificación Personal. Número solo conocido por el titular de la tarjeta, y que sirve para empezar a operar con ésta.

***PKI*:** Public Key Infraestructure. Infraestructura de Clave Pública.

Revocación de certificados: Anulación de la validez de un certificado de clave pública antes de finalizar de período de validez.

***SSL*:** Secure Socket Layer. Nivel de conexiones seguras. Es un protocolo para cifrar el tráfico de transacciones en una red.

Tarjeta Inteligente: Tarjeta incluye un microprocesador y es utilizada para proporcionar seguridad de la información.

X509: Norma estándar que define el certificado digital.

Apéndice B. Instalación y Configuración del *OpenCA*

A continuación procedemos a exponer los pasos básicos para realizar una instalación del *OpenCA.*

Prerrequisitos:

Instalación de Perl y módulos necesarios:

```
apt-get install libxml-perl libxml-regexp-perl libdbi-perl perl perl-
modules libldap2 libldap2-dev libdbd-mysql-perl libauthen-sasl-perl
libx500-dn-perl libcgi-session-perl libconvert-asn1-perl libdigest-md2-
perl libdigest-md4-perl libdigest-sha1-perl libio-socket-ssl-perl libio-
stringy-perl libmime-lite-perl libmime-perl libmailtools-perl libnet-
server-perl liburi-perl libxml-twig-perl libintl-perl libnet-ldap-perl
```

Instalación de Apache Web Server

```
apt-get install libapache-mod-perl libapache-mod-ssl
apt-get install apache
dpkg-reconfigure apache (Seleccionamos mod_ssl)
```

Instalación de Openssl

```
apt-get install openssl libssl-dev
```

Instalación del OpenCA

Lo primero que debe hacerse es obtener los códigos fuente de la aplicación. Para ello puede visitarse www.openca.org. Una vez obtenidos los códigos deben descomprimirse con el comando:

root:/usr/local/src# tar xzvf openca-0.9.2.5.tar.gz

De esto resultará un directorio llamado OpenCA-0.9.2.5.

```
#touch config_ra
#touch config_ca
```

y le damos permisos de ejecución

```
#chmod 755 config_ra
#chmod 755 config_ca
```

Ahora editamos config_ra y copiamos y pegamos lo que esta a continuación

```
#!/bin/sh

PREFIX=$1
VER=0.9.2.5

if [ -z "${PREFIX}" ] ; then
      PREFIX=/usr/local/src/openca/openca.${VER}
fi

./configure \
  --prefix=${PREFIX} \
  --with-httpd-user=www-data \
  --with-httpd-group=www-data \
  --with-openca-prefix=${PREFIX}/openca \
  --with-etc-prefix=${PREFIX}/openca/etc \
  --with-httpd-fs-prefix=${PREFIX}/httpd \
  --with-cgi-url-prefix=/cgi-bin/openca \
  --with-module-prefix=${PREFIX}/modules \
  --with-web-host=127.0.0.1 \
  --with-ca-organization="SUSCERTE" \
  --with-ca-country=VE \
  --with-ca-locality=Merida \
  --with-ldap-port=389 \
  --with-ldap-root="cn=root,o=SUSCERTE,c=VE" \
  --with-ldap-root-pwd="openca" \
  --enable-ocspd \
  --enable-db \
  --disable-dbi \
  --disable-rbac \
  --with-hierarchy-level=ca \
  --with-service-mail-account="redondo@funmrd.gov.ve"

  #  --with-openssl-prefix=/usr/local/ssl \
  #  --with-engine=no \
 make
 make install-ra  //instalacion del módulo ra
 make install-pub //instalacion del módulo pub
 make install-node //instalacion del módulo ca
```

Grabamos los datos y ejecutamos

```
#./config_ra
```

Ahora editamos config_ca y copiamos y pegamos lo que esta a continuación

```
#!/bin/sh

PREFIX=$1
VER=0.9.2.5

if [ -z "${PREFIX}" ] ; then
      PREFIX=/usr/local/src/openca/openca.${VER}
fi

./configure \
  --prefix=${PREFIX} \
  --with-httpd-user=www-data \
  --with-httpd-group=www-data \
  --with-openca-prefix=${PREFIX}/openca \
  --with-etc-prefix=${PREFIX}/openca/etc \
  --with-httpd-fs-prefix=${PREFIX}/httpd \
  --with-cgi-url-prefix=/cgi-bin/openca.0.9.2.5 \
  --with-module-prefix=${PREFIX}/modules \
  --with-web-host=127.0.0.1 \
  --with-ca-organization="SUSCERTE" \
  --with-ca-country=VE \
  --with-ca-locality=Merida \
  --with-ldap-port=389 \
  --with-ldap-root="cn=Manager,o=SUSCERTE,c=VE" \
  --with-ldap-root-pwd="openca" \
  --enable-ocspd \
  --enable-db \
  --disable-dbi \
  --disable-rbac \
  --with-hierarchy-level=ca \
  --with-service-mail-account="redondo@funmrd.gov.ve"

  #  --with-openssl-prefix=/usr/local/ssl \
  #  --with-engine=no \
make
make install-ra  //instalacion del módulo ra
make install-pub //instalacion del módulo pub
make install-node //instalacion del módulo ca
```

Grabamos los datos y ejecutamos

```
#./config_ca
```

Despues de ejecutar `make install-<nombre_interfaz>` se crearán algunos directorios, los relevantes por el momento serán el directorio `openca` y el

directorio `httpd`. El primero contiene, entre otros, la configuración de la aplicación. El segundo, como puede intuirse de su nombre, contiene todo lo relacionado con el servidor web.

Una vez instalada la aplicación debe editarse el archivo `openca/etc/config.xml`. Este archivo contiene la configuración de la opciones básicas de OpenCA . Los especificado en `config.xml` será "vaciado" en los archivos definitivos que contendrán la configuración de toda la aplicación al correr el script `openca/etc/configure_etc.sh`, estos archivos estarán ubicados en `openca/etc/servers/*.conf`. Cada vez que se corra `configure_etc.sh` los archivos `openca/etc/servers/*.conf` serán sobre escritos.

Una vez ejecutado `configure_etc.sh` deben crearse algunos enlaces suaves para el acceso correcto a los script de perl a través de CGI así como para el acceso a los documentos HTML. Dentro del directorio `httpd` se encuentran ambos, los scrip CGI (en `httpd/cgi-bin`) y los HTML (`httpd/htdocs`). En Debian es usual usar el directorio `/usr/lib/cgi-bin` para ubicar los scripts usados con CGI. Entonces debemos crear un enlace para redireccionar las solicitudes hasta el directorio de OpenCA:

```
/usr/lib/cgi-bin# ln -s ..../..../httpd/cgi-bin/ openca
```

Por otro lado, en Debian los documentos a desplegar en el servidor web apache están ubicados en `/var/www`, entonces también tenemos que crear un enlace sueva que refiera las solicutudes desde `/var/www` hasta `..../..../httpd/htdocs`; en el caso de el módulo CA:

```
/var/www# ln -s ..../..../httpd/htdocs/ca
```

Una vez hecho todo lo anterior estaremos listos para ejecutar el script de inicalización de OpenCA:

```
openca/etc# ./openca_start
```

Después de haber completado la instalación la aplicación debe ser inicializada. Para este procedimiento es posible usar la misma interfaz de OpenCA. La inicialización de OpenCA consiste básicamente en al generación del certificado de la CA, la inicialización de la base de datos y la creación de los certificados para los operadores (sólo en caso de usar autenticación con x509).

Anexo C. Declaración de prácticas de certificación (DPC) y política de certificados (PC)

1.- Introducción

1.1.- Comunidad de usuarios y ámbito de aplicación

1.1.1.- Autoridad de Certificación (AC)

La presente CPS especifica la actuación de un proveedor de certificados digitales (PCD) como Autoridad de Certificación (AC) la cual se basa en la relación de una determinada clave pública con un sujeto o entidad (entidad final) a través de la emisión de un certificado de conformidad con los términos de esta CPS.

1.1.2.- Autoridad de Registro (AR)

La Autoridad de Registro (AR) del proveedor de certificados digitales (PCD), será la encargada de la identificación de los Solicitantes de Certificados, cabe destacar que dicha identificación se llevara a cabo de acuerdo a las normas y procedimientos de esta CPS y siempre actuara en conjunto con la CA.

1.1.3.- Administrador pub (PUB)

El administrador pub (PUB) del proveedor de certificados digitales (PCD), funciona como interfaz entre el PCD y la entidad final y tiene la responsabilidad de gestionar los certificados digitales

1.1.4.- Suscriptor

Como suscriptor se entiende una entidad física o jurídica y es aquel que se deriva de las prácticas de certificación. El suscriptor estará sujeto a las obligaciones y responsabilidades que se derivan de lo establecido en esta CPS y en las prácticas de certificación de las AR para cada tipo de Certificado.

1.1.5.- Entidades Finales

1.1.5.1.- Solicitante

Como Solicitante se entiende la persona física autorizada para presentar la solicitud de un Certificado. La autorización estará regulada por cada una de las prácticas de certificación establecidas por las AR.

1.1.5.2.- Usuarios

Como Usuario del Certificado se entiende la persona voluntariamente confía y hace uso de los Certificados de la AC.
Cuando el Usuario decida voluntariamente confiar y hacer uso del Certificado le será de aplicación la presente CPS.

1.1.6.- Ámbito de Aplicación

1.1.6.1.- Tipos de Certificados

Los distintos tipos de certificados emitidos por el PCD dentro del ámbito de esta CPS están definidos en cada una de sus respectivas prácticas de certificación. Cada una de las prácticas de certificación regula la aplicabilidad de un certificado en relación a una comunidad de usuarios y unos usos determinados con unos requerimientos de seguridad comunes.

1.1.6.2.- Limitaciones de uso

Los usos autorizados de los Certificados emitidos por la AC vienen especificados en cada una de las prácticas de certificación correspondientes a cada tipo de certificado. Cualquier otro uso que se le dé se considerará una violación de esta

CPS y constituirá una causa de revocación del certificado digital y de terminación del contrato con el suscriptor.

El suscriptor considera y acepta que los productos y servicios que se anuncian son tal y como se ofrecen individualmente, que no existe ningún tipo de información implícita que implique servicios o prestaciones adicionales a los expresamente mencionados y que la utilización de los mismos es de su exclusiva responsabilidad.

Si durante el periodo de vigencia parte o toda la información contenida en el certificado digital pierde actualidad o validez, el suscriptor deberá iniciar el procedimiento de revocación del mismo de conformidad con lo establecido en la sección de Revocación de certificados digitales de esta CPS.

1.1.6.3.- Servicios ofrecidos

Entre los servicios de certificación ofrecidos por ID-digital se incluyen:

- Firma de certificados
- Emisión de certificados
- Revocación de certificados
- Suspensión de certificados
- Publicación de los Certificados emitidos

2.- Provisiones generales

2.1.- OBLIGACIONES

2.1.1.- Obligaciones de la CA

La AC del PCD está obligada a operar según las obligaciones que impone la presente CPS, y de acuerdo a la normativa aplicable sobre Certificación Digital y Firma Digital en Venezuela.

2.1.2.- Obligaciones de la AR

La AR del PCD está obligada a operar siempre dependiendo de la AC del PCD y cumpliendo las siguientes obligaciones:

- Operar según las obligaciones que impone la presente CPS.

- Identificar y autenticar correctamente al Suscriptor y/o Solicitante y a la organización que represente, conforme a los procedimientos que se establecen en esta CPS y en las Prácticas de Certificación específicas para cada tipo de Certificado, utilizando cualquiera de los medios admitidos en derecho.

- Almacenar de forma segura y por un periodo razonable la documentación aportada en el proceso de emisión del Certificado y en el proceso de suspensión/revocación del mismo.

- Deberá permitir el acceso a la AC del PCD a la información y a los procedimientos de conservación asumidos por la AR, y ante cualquier indicio o sospecha de infracción de la presente CPS y/o de las Prácticas de Certificación por parte de la AR o cualquier poseedor de un Certificado a investigar sobre este hecho.

- La AR estará obligada a informar a la AC de cualquier indicio o sospecha de infracción de la presente CPS y/o de las Prácticas de Certificación.

2.1.3.- Obligaciones del PUB

La PUB del PCD está obligada a operar siempre dependiendo de la AC del PCD y cumpliendo las siguientes obligaciones:

- Formalizar el Contrato de Certificación pertinente con el Suscriptor según los términos establecidos por la Política de Certificación de la AC.

- Enviar el kit a la entidad final e informarle el estado en que se encuentra la solicitud de certificado o el certificado, y los recaudos exigidos por la AR según el tipo de certificado solicitado.

2.1.4.- Obligaciones del Solicitante

- Abonar las tasas de registro que correspondan en virtud de los servicios que se soliciten.

- Solicitar el Certificado según se estipula en al CPS, las Prácticas de Certificación y en atención a las instrucciones de PCD.

2.1.5.- Obligaciones del Suscriptor

- Conservar y utilizar correctamente el Certificado

- Custodiar el Certificado, tomando las precauciones razonables para evitar su pérdida, revelación, modificación o uso no autorizado.

- Solicitar la suspensión / revocación del Certificado cuando se cumpla alguno de los supuestos previstos en el epígrafe titulado "suspensión y revocación de certificados" de la presente CPS.

- No revelar la clave privada.

- Asegurarse de que toda la información contenida en el Certificado es cierta y notificar inmediatamente a la AC en caso de que se haya incluido

cualquier información incorrecta o inexacta o en caso de que, de forma sobrevenida, la información del Certificado no se corresponda con la realidad. Asimismo, deberá comunicar de manera inmediata el cambio o variación que haya sufrido cualquiera de los datos que aportó para adquirir el Certificado, aunque éstos no estuvieran incluidos en el propio Certificado.

- Informar inmediatamente a la AC acerca de cualquier situación que pueda afectar a la validez del Certificado.

- Realizar un uso debido y correcto del Certificado, según se desprende de esta CPS y de las Prácticas de Certificación. Será responsabilidad del Suscriptor el uso indebido que éste haga del mismo.

- Cualquier otra que se derive de la ley, del contenido de esta CPS o de las prácticas de certificación.

2.1.6.- Obligaciones de los Usuarios

- Los Usuarios que pretendan confiar y usar los Certificados emitidos por la AC deberán verificar la validez de las firmas emitidas por los Suscriptores.

- En el supuesto de que los Usuarios no procedieran a verificar las firmas a través de la LCR (Lista de Certificados suspendidos o revocados), la AC no se hace responsable del uso y confianza que los Usuarios hagan de estos Certificados.

- Obligación de conocer las garantías y responsabilidades aplicables en la aceptación y uso de los certificados, condiciones y límites contenidos en esta CPS y en las prácticas de certificación, por los cuales se garantiza la prestación de los servicios de certificación.

2.2.- Responsabilidad

2.2.1.- Responsabilidad de la AC

La AC no asume ninguna responsabilidad en los siguientes casos:

- Por daños derivados de o relacionados con la no ejecución o ejecución defectuosa de las obligaciones a cargo de la AR, del PUB, del Suscriptor, del Solicitante, o del Usuario.

- Por el uso indebido o fraudulento de los Certificados y las claves, ni de cualquier daño indirecto que pueda resultar de la utilización del Certificado o de la información suministrada por la AC.

- Por los posibles errores existentes en el Certificado que deriven de la información facilitada, habiendo actuado siempre con la máxima diligencia posible.

- Daños ocasionados por el uso de certificados incumpliendo las limitaciones de uso que se señalan en esta CPS y en las prácticas de certificación aplicables en cada caso.

- De la no ejecución o retraso en la ejecución de las obligaciones establecidas en la CPS si esto fuera consecuencia de un supuesto de fuerza mayor, caso fortuito o, en general, cualquier circunstancia sobre la que la AC no pueda tener un control razonable.

- Del contenido de aquellos documentos firmados digitalmente por certificados del PCD, ni de aquellas páginas web que hagan uso de un certificado.

2.2.2.- Responsabilidad de la AR

Es responsable de la realización de aquellas funciones que le corresponden en conformidad a la presente CPS y, en concreto, se asume toda la responsabilidad por la correcta y exacta autenticación y validación del Solicitante y del Suscriptor, asumiéndose las mismas limitaciones establecidas en el apartado anterior con relación a la AC.

2.2.3.- Responsabilidad del PUB

Es responsable de la realización de aquellas funciones que le corresponden en conformidad a la presente CPS.

2.2.3.- Responsabilidad del Suscriptor

En caso de incurrir en actos u omisiones culposos o dolosos por su parte, se compromete a indemnizar a la AC por los daños o perjuicios ocasionados, incluyendo los gastos judiciales, costas de Abogados y Procuradores, en que la AC pudiera incurrir por esta causa.

2.2.4.- Responsabilidad del Usuario

Asumir toda responsabilidad en la correcta verificación de las firmas y certificados digitales, y por tanto de los riesgos derivados de la aceptación de un Certificado sin haber realizado previamente dicha verificación, dejando exenta a la AC de responsabilidad por dicho concepto.

2.3.- Publicación y depósito

2.3.1.- Publicación de información de la AC

El contenido de esta CPS, así como de toda la información que se publique, estará expuesta a título informativo en la URL del PCD y los originales estarán depositados en las oficinas de la AC.
Igualmente, tanto los Usuarios como los Solicitantes / Suscriptores podrán tener acceso de forma fiable a la información de la AC dirigiéndose a sus oficinas, o bien, solicitándolo a la dirección de correo a través de la cual se remitirá la información.

2.4.- Confidencialidad y protección de datos

2.4.1.- Confidencialidad de las claves de firma digital

El Suscriptor garantiza la confidencialidad frente a terceros durante el proceso de generación de las claves (publica/privadas), la AC se abstendrá de almacenar, copiar o conservar cualquier tipo de información que sea suficiente para reconstruir dichas claves.

2.4.2.- Confidencialidad en la prestación de servicios de certificación

Tanto el PUB, AC como la AR mantendrán la más estricta confidencialidad de toda información recibida por los Solicitantes y Suscriptores de Certificados, siempre que la publicación o comunicación a terceros de dicha información no sea necesaria para la correcta prestación de los servicios de certificación. La AC solicitará la autorización de Solicitantes y Suscriptores cuando precise utilizar los datos para otros fines.

2.4.3.- Protección de datos

A los efectos de lo dispuesto en la normativa sobre tratamiento de datos de carácter personal, se informa al Suscriptor / Solicitante que existe un fichero donde serán almacenado los datos de carácter personal, el responsable de fichero compromete a poner los medios a su alcance para evitar la alteración, pérdida, tratamiento o acceso no autorizado a los datos de carácter personal contenidos en el fichero. Cualquier otra utilización de los datos de carácter personal contenidos en el fichero, requerirá previo consentimiento del Suscriptor / Solicitante. Asimismo, se informa sobre el derecho que asiste al Suscriptor para acceder, rectificar o cancelar sus datos de carácter personal .

3.- REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS

La revocación y suspensión de Certificados son instrumentos a utilizar en el supuesto de que por alguna causa establecida en la presente CPS se deje de confiar en el Certificado antes de la finalización de su período de validez originalmente previsto.

3.1. Supuestos de revocación

Los Certificados deberán ser revocados cuando concurra alguna de las circunstancias siguientes:

- Solicitud voluntaria del Suscriptor.

- Pérdida o inutilización por daños del soporte del certificado.

- Fallecimiento del signatario o de su representado, incapacidad sobrevenida, total o parcial, de cualquiera de ellos, terminación de la representación o extinción de la persona jurídica representada.
- Cese en su actividad del prestador de servicios de certificación salvo que los certificados expedidos por aquel sean transferidos a otro prestador de servicios.

- Inexactitudes graves en los datos aportados por el signatario para la obtención del certificado, así como la concurrencia de circunstancias que provoquen que dichos datos, originalmente incluidos en el Certificado, no se adecuen a la realidad.

- Que se detecte que las claves privadas del Suscriptor o de la AC han sido comprometidas, bien porque concurran las causas de pérdida, robo, hurto, modificación, divulgación o revelación de las claves privadas, bien por cualquiera otras circunstancias, incluidas las fortuitas, que indiquen el uso de las claves privadas por persona distinta al titular.

- Por incumplimiento por parte de la AR, AC o el Suscriptor de las obligaciones establecidas en esta CPS.

- Por la resolución del contrato tal y como esta se regula en el apartado 8 de la presente CPS.

- Por cualquier causa que razonablemente induzca a creer que el servicio de certificación haya sido comprometido hasta el punto que se ponga en duda la fiabilidad del Certificado.

- Por resolución judicial o administrativa que lo ordene.

- Por la concurrencia de cualquier otra causa especificada en la presente CPS o en las correspondientes Prácticas de Certificación establecidas para cada tipo de Certificado.
- En el caso de los Certificados de Apoderados de Empresa, también será causa de revocación el cese del Representante de la Persona Jurídica representada.

- En el caso de los Certificados de Apoderados de Empresa, además será causa de revocación la extinción de la Persona Jurídica representada.

- En el caso de los Certificados de Empresa sin Poderes, también será causa de revocación la propia revocación de la autorizaciónal suscriptor para la utilización del certificado en virtud del cual se identifica en el mercado como persona relacionada con dicha entidad.

3.1.1.- Efectos de la revocación

El efecto de la revocación del Certificado es la pérdida de fiabilidad del mismo, originando el cese permanente de la operatividad del Certificado conforme a los usos que le son propios y, en consecuencia, de la prestación de los servicios de certificación.
La revocación de un Certificado impide el uso legítimo del mismo por parte del Suscriptor.
La revocación del Certificado por causa no imputable al Suscriptor originará la emisión de un nuevo Certificado a favor del Suscriptor por el plazo equivalente al restante para concluir el período originario de validez del Certificado revocado.
La revocación del Certificado tendrá como consecuencia la notificación a terceros de que un Certificado ha sido revocado, cuando se solicite la verificación del mismo.