”MODELO DE UN PROVEEDOR DE CERTIFICACIÓN DIGITAL BAJO ESTÁNDAR X.509 UTILIZANDO SOFTWARE LIBRE”

Autor: Pedro José Buitrago Castellanos

Tutor Académico: Víctor Bravo

Proyecto de grado presentado ante la ilustre
Universidad de los Andes
Como requisito final para optar al titulo de
Ingeniero de Sistemas

UNIVERSIDAD DE LOS ANDES
FACULTAD DE INGENIERIA DE SISTEMAS
(Mérida, Noviembre 2006)

UNIVERSIDAD DE LOS ANDES

FUCULTAD DE INGENIERIA

El jurado aprueba el proyecto de grado titulado ”**Modelo de un Proveedor de Certificados Digitales Bajo el Estándar X.509 Utilizando Software Libre**“ Realizado por **Br. Pedro J. Buitrago C.** como requisito parcial para la obtención del grado de **Ingeniero de Sistemas**

Fecha: Noviembre 2006

Tutor: _____

Prof. Víctor Bravo

Jurado: _____

Prof. Judith Barrios

_____

Prof. Leandro León

A mis padres Amelia Iris Castellanos de Buitrago y Pedro José Buitrago Alvarado, ejemplo de humildad, honestidad, honradez. Son el pilar fundamental de mi vida, por ustedes soy lo que soy, sin su esfuerzo y sacrificio, no hubiese podido alcanzar este sueño, gracias por confiar y creer en mi, por apoyarme en todo. Le doy gracias a Dios por tener unos padres tan maravillosos. Los Amos con todo mi corazón

Índice General

Índice de tablas

Índice de Figura

Agradecimientos

- A mi tutor Profesor Víctor Bravo, por su ayuda, apoyo y por la confianza que deposito en mí.

- A la Ilustre Universidad de los Andes, a la escuela de Sistemas, en especial a sus profesores por ser parte fundamental en mi formación académica. Gracias por abrirme sus puertas.

- A mis hermanas Iris, Maria y Mireya, el amor y solidaridad siempre ha permanecido con nosotros.

- A Paola, mi gran amiga, siempre tuviste una palabra de aliento para mí.

- A vetis, una persona muy especial para mi, gracias por tu amor, enseñanzas y por confiar plenamente en mí.

1.- Capitulo 1. Introducción

Tras la masiva utilización de Internet, como medio de comunicación de información, y el nacimiento del comercio electrónico, como aplicación de la actividad comercial a nivel mundial, surge la necesidad de asegurar las conexiones que se realizan a través de la red.

En estos momentos surge la demanda en muchas organizaciones de permitir a sus usuarios accéder a determinada información de una manera sencilla y permanente, pero el motor de la demanda ha sido la popularidad de Internet y sus propias características que permiten esa nueva perspectiva en la gestión de la información.

Los protocolos sobre los que se ha construido Internet (TCP/IP) ofrecen muy poco o ninguna tipo de seguridad. Mientras un paquete viaja por varias redes hasta alcanzar su destino, éste se puede leer e incluso modificar fácilmente, lo que supone un problema cuando la información que se transmite es especialmente sensible, como por ejemplo: datos personales, números de tarjeta de crédito, información corporativa confidencial y con propiedad intelectual, etc.

Hay que ser sumamente cuidadoso con las aplicaciones que manejan este tipo de datos, debido a las numerosas implicaciones que pueden surgir debido a problemas de seguridad, en distintos ámbitos, incluido el jurídico. Este último puede comprobarse con la aparición progresiva de leyes en Venezuela como la Ley Sobre Mensajes de Datos y Firmas Electrónicas, y Ley Especial Contra los Delitos Informáticos. [Ref www.asambleanacional.gov.ve/ns2/leyes.asp]

Una de las técnicas más utilizadas en seguridad informática son los certificados digitales que ofrecen algunas soluciones a problemas como: la lectura no

autorizada de correo electrónico, suplantación de personalidad, suplantación de servidores, acceso a datos confidenciales, etc.

En este proyecto de grado se desarrolla un modelo de Proveedor de Certificados Digitales (*PSC*) que permita crear confianza entre los usuarios, tanto en la utilización de nuevas tecnologías tales como las tarjetas inteligentes como realizar de forma segura las transacciones por la red, y efectuar todas las tareas vinculadas a la administración de los certificados digitales.

Este proyecto de grado se ha estructurado en cinco capítulos, En el capítulo 2, se recoge una breve descripción de los temas que se consideran claves en la realización del proyecto, tales como: seguridad informática, introducción al cifrado, firmas digitales, certificados digitales, tarjetas inteligentes, infraestructura de clave pública, entre otros.

En el capitulo 3 se modela el PSC, se apoyó en el lenguaje unificado de modelado (UML) para desarrollar el modelo del proveedor de servicios de certificado donde se describen tres aspectos importantes como son: Software, hardware y políticas.
En el capitulo 4 se extrae de los diagramas del lenguaje de modelado unificado del capitulo 3 los requisitos de software, hardware y personal con el fin de seleccionar software libre y hardware que cubra los requisitos para desarrollar el modelo del proveedor de certificado digital.

En el capitulo 5 se realiza un experimento con el software que se utiliza en el modelo del proveedor de certificado digital y en el capitulo 6, las conclusiones generales del proyecto de grado y recomendaciones.

Anexo A. Este anexo recoge aquellos términos o siglas que se consideran de importancia para la comprensión de este proyecto de tesis. Anexo B. Configuración de algunos módulos y funciones del software libre *OpenCA*. Anexo C. Declaración de prácticas de certificación (DPC) y políticas de certificación

1.1.- Objetivos:

1.1.1.- Objetivo general:

Desarrollar un modelo de un proveedor de certificación digital que brinde los servicios registro del cliente, publicación de los certificados, entrega de las tarjetas inteligentes, firmas de certificados, usando software libre

1.1.2.- Objetivo específicos:

- Desarrollar un conjunto de políticas de certificación: La política de certificación establece y define la dirección que debería seguir la organización respecto de la seguridad de su información considerando los procesos y principios establecidos para el uso de medios criptográficos. También incluye documentos de cómo la organización deberá manejar sus claves a fin de establecer el nivel de control deseado de acuerdo a los riesgos existentes.

- Desarrollar un modelo de Autoridad Certificadora (*AC*): La autoridad certificadora es el componente clave de una infraestructura de claves públicas y es la encargada de realizar la emisión y administración de los certificados durante todo el ciclo de vida de los mismos.

- Desarrollar un modelo de Autoridad de Registro (*AR*): Que es la responsable del registro y la autenticación inicial de suscritores, que son los usuarios a quienes se les expide un certificado después de que les ha sido aprobada una solicitud de registro.

- Configurar un sistema de administración de certificados y distribución, que establece el tratamiento que recibirán los certificados generados, desde el procedimiento de generación hasta su revocación o re-certificación (solo si estuvo suspendido) y la manera en que serán distribuidos los certificados.

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

1.1.3.- Metodología:

- Búsqueda de información, material bibliográfico y estudio de conceptos básicos.

- Estudio y manejo del hardware a utilizar.

- Desarrollo de un marco teórico.

- Desarrollo del modelo de proveedor de certificación.

- Configuración, Implantación del modelo de proveedor de certificación usando software libre.

- Evaluación y validez del modelo.

- Redacción del manuscrito del proyecto de grado.

- Exposición final del proyecto.

2.- Capitulo 2. Marco teórico

En este capítulo se recoge una breve descripción de los temas que se consideran importante para la realización del proyecto tales como: seguridad informática, introducción al cifrado, firmas digitales, certificados digitales, tarjetas inteligentes, infraestructura de clave pública, etc.

2.1.- Internet: su desarrollo en los servicios

Internet ha tenido un impacto en la sociedad. En la manera cómo se utilizaba el Internet, en un principio, muchas empresas utilizaban Internet como una solución complementaria y no productiva, por ejemplo uno de los primeros usos compartiendo bases de datos. Con el afán de interactuar globalmente, se ha cambiado el concepto de la utilización de Internet como medio de intercambio comercial, por tanto se requiere un desarrollo complementario en lo que hay mecanismos de seguridad informática. Se refieren en este momento, una gran cantidad de ellas están integradas completamente con tecnologías basadas en Internet y comercio electrónico.

Algunas de las actividades que se pueden realizar y los requisitos de seguridad que se necesitan tenemos, por ejemplo:

- Las compañías pueden utilizar Internet como un canal de comunicación entre sus diferentes oficinas, o entre sus socios o clientes, éstas comunicaciones suelen tener información corporativa confidencial y con propiedad intelectual, requiriendo que se transmita sin estar expuestas o sin que alguien la pueda falsificar.

- Las compañías pueden expandir sus negocios de comercio electrónico y cerciorarse de que sus transacciones sean seguras.

- Reducir el costo de almacenamiento, reemplazando los documentos firmados físicamente con documentos firmados electrónicamente.

- Aumentar la seguridad de los sistemas, manteniendo inaccesible a usuarios no autorizados a información sensible, necesitando un mecanismo más fuerte de autenticación, autorización y control de accesos.

Ahora se empieza a pensar muchas más en mecanismo que se deben aplicar a la información y a los servicios que necesitamos proteger, y a los cuales se quiere conceder accesos a usuarios autorizados. Estos mecanismos, deben generar un nivel de seguridad que permita realizar todas las actividades y servicios por las grandes redes de manera segura. Estos mecanismos deben cumplir ciertos aspectos de seguridad informática.

2.2.- Seguridad informática

Según K. Charlie [2]. Podemos entender como seguridad una característica que determina que cualquier sistema está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo. Para la mayoría de los expertos el concepto de seguridad en la informática es supuesto, porque no existe un sistema totalmente o 100% seguro. Para que un sistema se pueda definir como seguro debemos de brindar tres características al mismo tiempo:

2.2.1.- Confidencialidad

Se refiere a que se debe mantener inaccesible a todos los usuarios que no estén autorizados a los datos e información, cuando se requiera. Por ejemplo; se estable una comunicación por correo electrónico entre el decano de la Facultad de Ingeniería y el director de una escuela de la misma facultad y donde se le informa

la decisión que tomaron por una determinada situación de carácter urgente, y el único que la puede conocer es el director de la escuela, se debe mantener inaccesible a esta comunicación a una tercera persona que se pueda aprovechar o utilizar para fines deshonestos. (Ver figura 1).

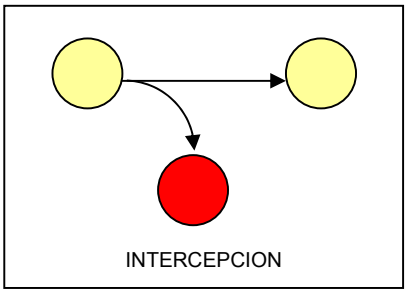

Figura 1. Acceso a la comunicación a una persona no autorizada.

2.2.2.- Integridad

Se refiere a la protección que debe tener la información, datos, sistemas y otros activos informáticos contra cambios o alteraciones en su estructura o contenido ya sean intencionales o causales. Por ejemplo; siguiendo el ejemplo anterior, una vez que s e envía la información por el correo electrónico, el mismo no debe sufrir alteraciones en su contenido que pueda ocasionar una toma de decisión diferente a la planteada en la comunicación que genere malestares. Se quiere que llegue a su destino la información tal cual se generó en la fuente. (Ver figura 2).

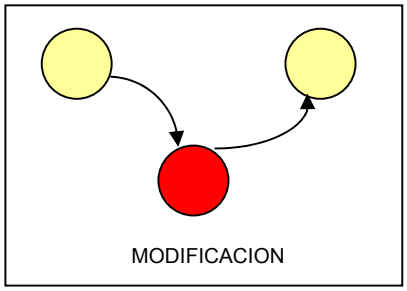

Figura 2. Modificación de la comunicación por persona no autorizada

2.2.3.- Disponibilidad

Se refiere a la capacidad que tenga el sistema para mantener los datos e información el mayor tiempo y lugar posible accesible a todos los usuarios autorizados o pertinentes. Por ejemplo; el sistema de inscripción de la facultad de ingeniería, debe permitir a sus estudiantes inscribirse en cualquier sitio que tenga acceso a Internet y no que tengan que asistir a un laboratorio o sitio de la facultad para poder realizar la inscripción, logrando un compromiso con los aspectos de confidencialidad e integridad. (Ver figura 3).

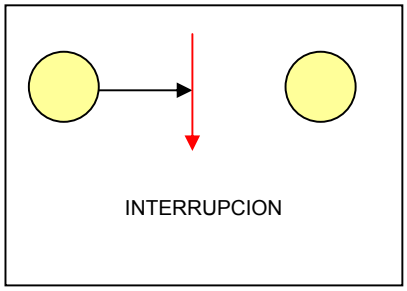

Figura 3. Inaccesible al sistema de lugar posible a los usuarios autorizados.

Existen propiedades vinculadas a los aspectos antes descritos, y que complemente el concepto de seguridad informática, ellos son:

2.2.4.- Autenticación y Autorización

Se refiere a la capacidad que tenga el sistema de probar que un usuario o agente es el que dice ser, con la finalidad de permitirle su acceso. Por ejemplo; que el sistema de administración de notas de los bachilleres de la facultad de ingeniería, a través de cierto mecanismo como por ejemplo una tarjeta inteligente, pueda identificar y permitir el acceso a dicho sistema solo a la(s) persona(s) responsable(s) y autorizada(s) en manipular la información de ese sistema que son delicadas. (Ver figura 4).

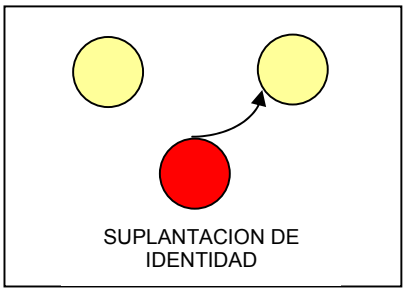

Figura 4. Acceso a persona no autorizado al sistema.

2.2.5.- No Repudio

Se refiere a mecanismo que permita verificar que una persona fue la que envió una determinada información, y que esa persona no pueda negarse de que envió dicha información.

En la actualidad hay muchos sistemas, actividades, servicios, etc, que utilizan Internet para realizar operaciones, y no cumple con estos aspectos de seguridad mencionados, por ejemplo, el más utilizado, el correo electrónico, que es relativamente vulnerable falsificar información con este medio, y la información que se envía fácilmente esta expuesta a tercera personas.

Todo lo que se ha nombrado sobre seguridad informática tiene el objetivo de producir confianza; es decir, la percepción de seguridad que tiene el usuario de los sistemas e información digital con los cuales interactúa.

Para alcanzar los niveles aceptables que conforman diferentes aspectos de seguridad informática, se requiere de la construcción de mecanismos como por ejemplo la Infraestructura de Clave Pública (*ICP*), que utiliza muchas de las nuevas tecnologías usadas en la construcción de soluciones para el comercio electrónico.

2.3.- Introducción al Cifrado

2.3.1.- Cifrado

Según A. Nash [1]. Es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas (algoritmos matemáticos). El cifrado tiene como finalidad, garantizar el secreto en la comunicación entre dos entidades (personas, organizaciones, etc.), asegurar que la información sea enviada por el remitente que realmente dice ser y que el contenido del mensaje enviado, no haya sido modificado en su tránsito.

La información original que debe protegerse se denomina texto en claro. El cifrado es el proceso de convertir el texto claro en un texto ilegible, denominado texto cifrado o criptograma. (Ver figura 5)

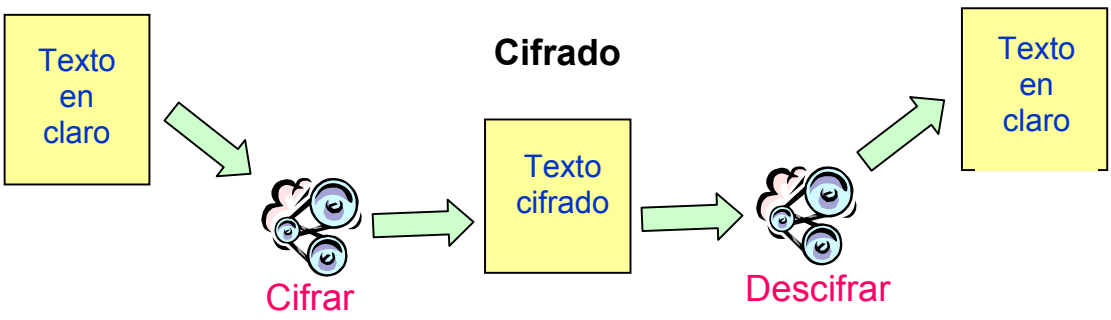

Figura 5. Cifrado

Estos algoritmos matemáticos o de cifrado utilizan claves para cifrar y descifrar los texto en claros, estas claves son similares a una llave física que se usan para cerrar o abrir una puerta, las claves tienen un tamaño en bits que esta determinado de acuerdo al tipo de algoritmo que se este utilizando.

2.3.2.- Tipos de cifrado

2.3.2.1.- Cifrado simétrico

Según A. Nash [1]. Algoritmo de cifrado que usa una misma clave para cifrar y para descifrar mensajes. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez ambas tienen acceso a esta clave, el remitente cifra el mensaje que quiere proteger (texto en claro) usando la clave (clave simétrica), lo envía al destinatario, y éste lo descifra con la misma clave. (Ver figura 6)

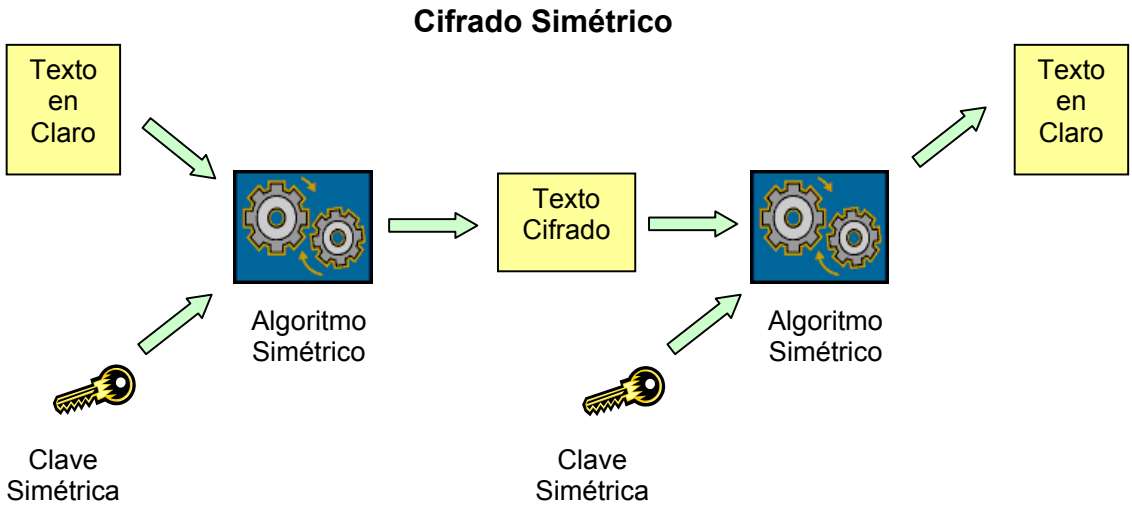

Figura 6. Cifrado Simétrico

Entre las características importantes del cifrado simétrico tenemos:

- El cifrado simétrico utiliza la misma clave para cifrar y descifrar.
- El cifrado simétrico es rápido.
- El cifrado simétrico es seguro.

- El texto cifrado que resulta del cifrado simétrico es compacto.

- El cifrado simétrico requiere una administración compleja de claves.
- El cifrado simétrico no se ajusta a las firmas digitales o a la aceptación.

2.3.2.2.- Cifrado asimétrico

Según A. Nash [1]. Algoritmo de cifrado que usa un par de claves para cifrar y descifrar el mensaje. Las dos claves pertenecen a la persona que ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona. La otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. El remitente usa la clave pública del destinatario para cifrar el mensaje, y una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje. (Ver figura 7)

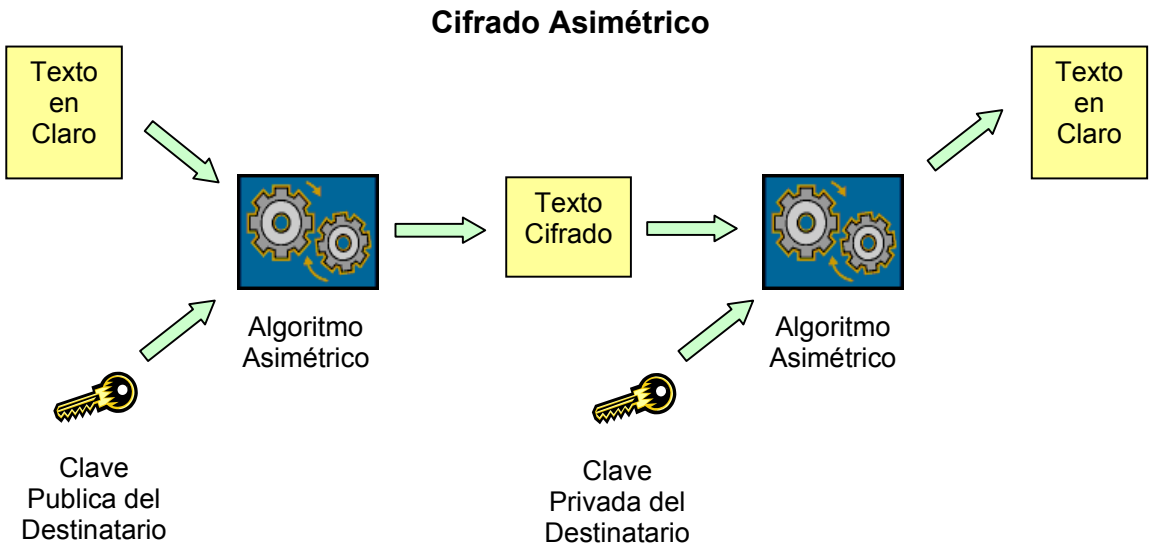

Figura 7. Cifrado Asimétrico

Entre las características importantes del cifrado asimétrico tenemos:

- El cifrado asimétrico utiliza una clave (publica/privada) para cifrar y la otra clave (publica/privada) para descifrar.

- El cifrado asimétrico es relativamente lento.
- El cifrado asimétrico es seguro.
- El cifrado asimétrico expande el texto cifrado.
- El cifrado asimétrico no tiene los problemas complejos de distribución de claves.

2.3.2.3.- Cifrado híbrido

Según A. Nash [1]. Algoritmo de cifrado que usa tanto un cifrado simétrico como uno asimétrico. Emplea el cifrado asimétrico para compartir una clave para el cifrado simétrico. El mensaje que se esté enviando en el momento, se cifra usando la clave simétrica y enviándolo la clave simétrica al destinatario de manera cifrada usando un algoritmo asimétrico. Ya que compartir una clave simétrica no es seguro. De esta manera usando la combinación de las dos soluciones, capturando las fortalezas de cada una sin heredar sus problemas. (Ver figura 8)

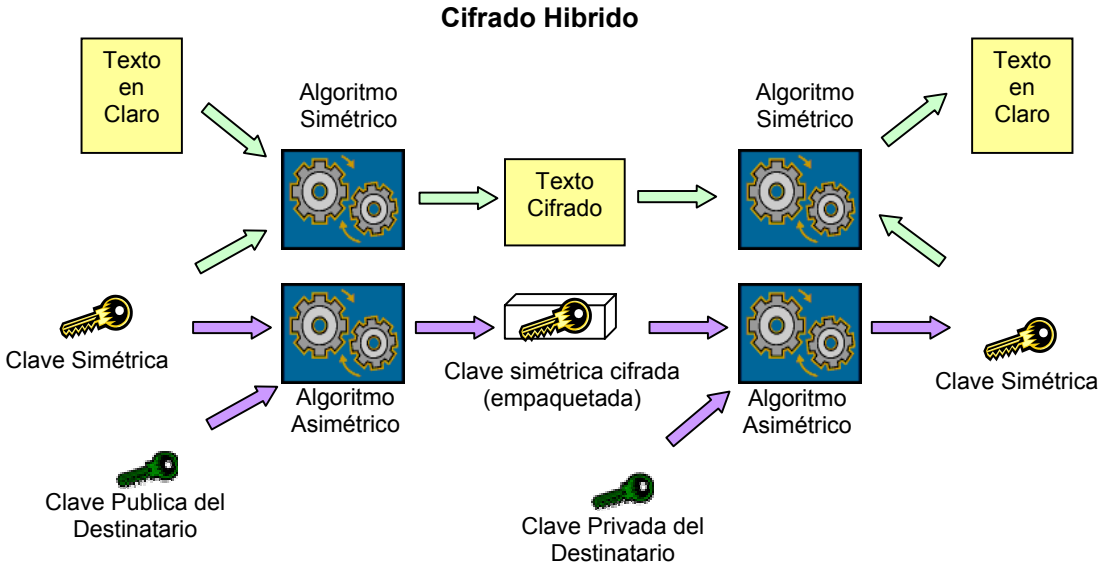

Figura 8. Cifrado Hibrido.

Esta solución ideal debe tener las siguientes características:

- La solución debe ser segura.
- El cifrado debe ser rápido.
- El texto cifrado debe ser compacto.
- La solución no debe vulnerar a la intercepción de claves.
- La solución no debe requerir una relación previa entre las partes para ponerse de acuerdo que clave van a utilizar.
- La solución debe soportar firmas digitales y aceptación.

Con la utilización de la tecnología del cifrado a la información que se quiere proteger se esta logrando la confidencialidad.

2.4.- Firmas digitales

Según A. Nash [1]. La firma digital es el resultado de aplicar cierto algoritmo matemático, denominado función hash, a su contenido. Esta función asocia un valor dentro de un conjunto finito (generalmente los números naturales) a su entrada. Cuando la entrada es un documento, el resultado de la función (reseña) es un número que identifica casi unívocamente al texto. Si se adjunta este número al texto de manera cifrada con algoritmo asimétrico usando la clave privada del que firma, el destinatario puede aplicar de nuevo la función hash y comprobar su resultado (reseña) con el que ha recibido, si ambos son iguales, tiene la seguridad de que el texto no fue modificado una vez que fue firmado y que lo envió la persona dueña de la clave privada que firmo el texto. (Ver figura 9)

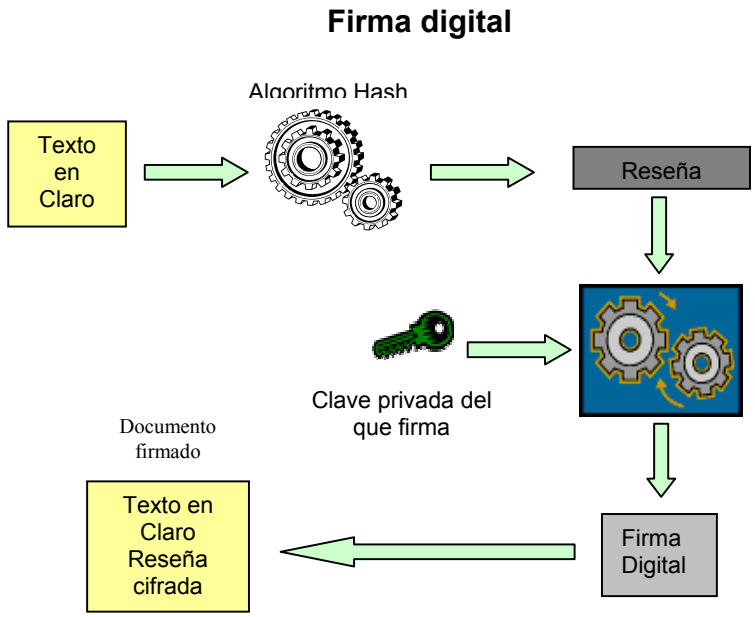

Figura 9. Firma Digital

Con la utilización de la tecnología de las firmas digitales a la información se esta logrando la integridad.

2.5.- Certificados digitales

Según A. Nash [1]. Un Certificado Digital es un documento digital firmado digitalmente por un tercero confiable (una Autoridad de Certificación) el cual garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública. Si el Certificado es auténtico y confiamos en la Autoridad Certificadora (*AC*). Entonces, podemos confiar en que el usuario identificado en el Certificado Digital posee la clave pública que se señala en dicho certificado. Así pues, si un sujeto firma un documento y anexa su certificado digital, cualquiera que conozca la clave pública de la *AC* podrá autenticar el documento.

2.5.1.- Certificado digital X.509 versión 3:

- El estándar, internacionalmente aceptado, para Certificados Digitales, es el denominado X.509, en su versión 3.

- Contiene datos del sujeto, como su nombre, dirección, correo electrónico, etc (Ver figura 10).

- Con la versión 3 de X.509, sucesora de la versión 2, no hace falta aplicar restricciones sobre la estructura del certificaddo gracias a la definición de las extensiones de certificados. Se permite que una organización pueda definir sus propias extensiones para contener información específica dentro de su entorno de operación. Este tipo de certificados es el que usa el protocolo de comercio electrónico SET.

- X.509 y X.500 fueron originalmente diseñados a mediados de los años 80, antes del enorme crecimiento de usuarios en Internet. Es por esto por lo

que se diseñaron para operar en un ambiente donde sólo los computadores se interconectaban intermitentemente entre ellos. Por eso en las versiones

1 y 2 de X.509 se utilizan CRLs muy simples que no solucionan el problema de la granularidad de tiempo.

- La versión 3 introduce cambios significativos en el estándar. El cambio fundamental es el hacer el formato de los certificados y los CRLs extensible. Ahora los que implementen X.509 pueden definir el contenido de los certificados como crean conveniente. Además se han definido extensiones estándares para proveer una funcionalidad mejorada.

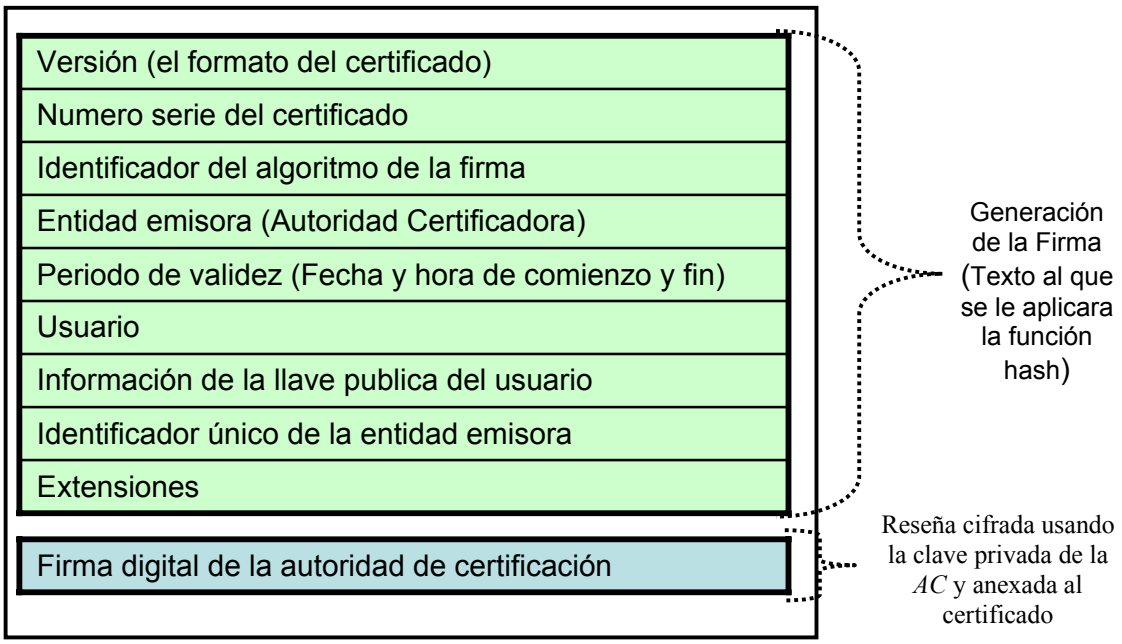

Figura 10. Certificado Digital

Con la utilización de la tecnología de certificados digitales estamos logrando la autenticación y autorización.

Los certificados digitales tienen multitud de usos, entre ellos tenemos:

- Certificado de Servidor (*SSL*): Permite incorporar el protocolo *SSL* a un servidor *web*. Que permite que toda la comunicación entre el cliente y el

  servidor permanezca segura, cifrando la información que se envía cada parte. el certificado del servidor posibilita la autenticación fuerte, es decir, que el servidor puede exigir certificados personales de navegación a los usuarios para acceder a determinadas carpetas, lo que repercute en la seguridad y en la comodida por la ausencia de cuentas y contraseñas para la identificación de los usuarios.

- Certificados personales (Correo y navegación): Un certificado digital personal es la herramienta necesaria para navegar, comprar y enviar/recibir correo a través de Internet, de una manera segura. A través de este certificado se puede firmar o cifrar los mensajes de correo para tener la seguridad que el receptor será el único lector de nuestro mensaje. Se puede aumentar la seguridad y confianza entre el cliente y el servidor web, al autenticarse también al usuario, esto también va a permitir a las empresas la posibilidad de personalizar los contenidos a un usuario concreto, con la certeza que otros usuarios no podrán ver dicho contenido, tales como información confidencial, ofertas especiales, etc.

- Certificado para estampillado de tiempo: Este certificado solo se usa cuando es necesario asegurar la existencia de un documento digital en un instante preciso; para ello, el servidor debe tener una fuente de tiempo fiable, a estos servidores se les conoce como servidores de tiempo o servidores *Timestamp*. Cuando queremos sellar un documento, generamos su *hash* y lo enviamos a un servidor *Timestamp*, que nos devuelve el documento firmado (el servidor nombre_servidor tuvo el conocimiento del documento con el hash nombre_hash el día nombre_dia a las ..), y la firma de dicho documento. Los servidores *Timestamp* mantiene accesible la lista

de todos los sellos que se emiten, para que todos las puedan ver, y así garantizar que nadie modifique el sello de tiempo. En estas listas solo aparece el *has* del documento, que son irreversibles, es decir, que a partir

del valor del *hash* no podemos obtener el documento garantizando la confidencialidad.

- Certificado para firma de código: El certificado para la firma de código, permitirá a un Administrador, Desarrollador o Empresa de Software firmar su software y macros, y distribuirlo de una forma segura. Esta solución de Seguridad es el requisito mínimo que necesitan nuestros clientes o lista de correo, para confiar y tener la seguridad de que el fichero que reciben o se descargan, proviene exclusivamente de una empresa determinada. Con ello se evitan los problemas causados por la suplantación de personalidad y la distribución de objetos dañinos o perjudiciales bajo esta supuesta identidad. Cualquier modificación (por ejemplo: inclusión de un troyano o infección de un virus) sobre el software original lo invalidará, con lo que el usuario tendrá la confirmación para rechazarlo al comprobar que la firma electrónica no corresponde con la del software modificado.

2.6.- Tarjetas inteligentes

Las tarjetas inteligentes o tarjetas de circuito integrado (*TCI*), son similares en tamaño y otros estándares físicos a las tarjetas de créditos con circuito integrado incluido (Ver figura 11). Este circuito puede ser de sola memoria o contener un microprocesador con un sistema operativo que le permite una serie de tareas como:

1. Almacenar

2. Cifrar información.

3. Leer y escribir datos, como un ordenador.

Como mecanismo de control de acceso las tarjetas inteligentes hacen que los datos personales y de negocios solo sean accesibles a los usuarios apropiados, esta tarjeta asegura la portabilidad, seguridad y confiabilidad en los datos.
Entre las características más importantes tiene:

a. Inteligencia: Es capaz de almacenar cualquier información, además es autónoma en la toma de decisiones al momento de realizar transacciones.

b. Utiliza clave de acceso o PIN: Para poder utilizarse es necesario digitar un número de identificación personal, es posible además incorporar tecnología más avanzada como identificación por técnica biométrica, huella digital o lectura de rutina.

Figura 11. Tarjeta inteligente.

2.7.- Lectora de tarjetas inteligentes

La lectora de las tarjetas inteligentes como habitualmente se les conoce, es un dispositivo que frecuentemente están capacitada para realizar la grabación, existen muchos tipos de lectoras de tarjetas inteligentes y sus elección va asociada a la tarjeta inteligente que se utiliza, puede ser mas de una tarjeta. (Ver figura 12). Básicamente se cuenta con dos grandes familias:

1. Universal: Permiten leer más de un tipo de tarjeta.

2. Especializadas: Estas lectoras solo pueden leer unos pocos tipos de tarjetas similares.

3. Normalmente van conectadas a un ordenador, forma que el control de lectura y la alimentación eléctrica a menudo se simplifican.

Figura 12. Lector de tarjetas inteligentes.

2.8.- Modulo de seguridad hardware (*HSM*, por su sigla en ingles, Hardware Security Module)

El *HSM* es un dispositivo que brinda los servicios de cifrado necesario, basado en hardware que genera, almacena y protege las claves de cifrado. El modulo *MSH* ofrece un subsistema de alta velocidad de claves publicas. El cifrado de claves pública se utiliza por lo general para generar y verificar las firmas digitales. El *MSH* puede procesar claves de 320 a 2048 bits. Gracias a estas prestaciones el *MSH* se puede utilizar en sistemas en los que se usen claves de distintas longitud para diferentes funciones, como las firmas digitales y la gestión de claves. (Ver figura 13)

Figura 13. Modulo de seguridad hardware

2.9.- OpenSSL

Es un proyecto de software desarrollado por los miembros de la comunidad Open Source para libres descarga. Consiste en un robusto paquete de herramientas de administración y librerías relacionadas con el cifrado, que suministra funciones de cifrado para otros paquetes como *OpenSSH*, *OpenCA*, y navegadores web (para acceder seguro a sitios *https*). Estas herramientas ayudan al sistema a implementar el Secure Sockets Layer (*SSL*), así como otros protocolos relacionados con la seguridad.

Algunos usos de *OpenSSL* es ofrecer certificados para usar con aplicaciones de software. Estos certificados aseguran que las credenciales de la compañía o individuo son válidas y no son fraudulentos. Si el certificado en cuestión no ha sido verificado por uno de las diversas Autoridades Certificadoras, suele generarse una advertencia al respecto.

2.10.- Infraestructura de claves públicas (*ICP*)

(*PKI*, Por sus siglas en ingles, Public Key Infrastructure) la *ICP* es la combinación de hardware y software, políticas y procedimientos tendientes a proveer un nivel adecuado de seguridad y confianza, para poder realizar transacciones electrónicas de manera segura.

La *ICP* se basa en proveer identificaciones digitales, también conocidas como "certificados digitales", los cuales actúan como pasaportes electrónicos vinculando a su clave pública. Realiza de forma segura todas las tareas vinculadas a la administración de los certificados digitales, establecimiento de un conjunto de mecanismo de seguridad y políticas que permitan alcanzar el nivel de seguridad adecuado.

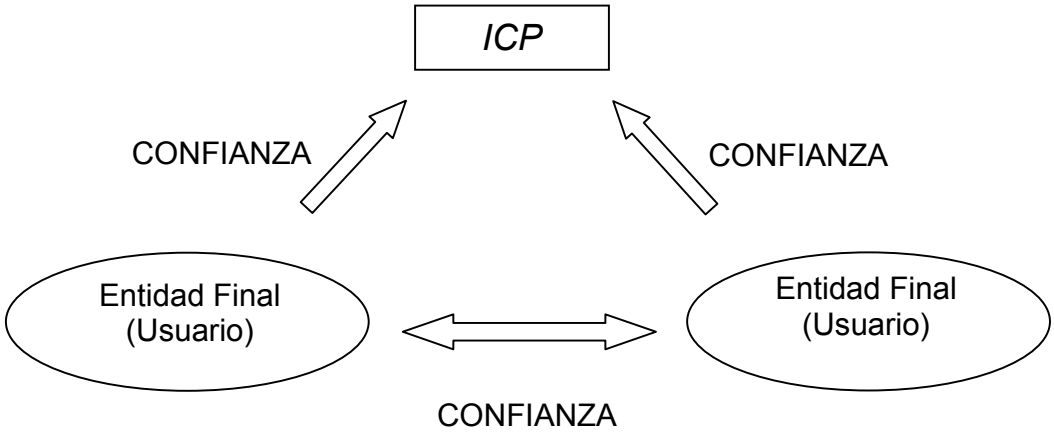

Figura 14. Infraestructura con confianza en un tercero

Como podemos ver en la figura 14 los usuarios depositan su confianza en una tercera persona (*ICP*) que le ofrezca el nivel de seguridad necesario para realizar las transacciones comerciales seguras.

Existen diferentes modelos de implementación de *ICP* que están en función de las necesidades de la población donde se encuentra o del nivel de confianza adecuada que requiera para su aplicación, entre los modelos de *IPC* tenemos el modelo jerárquico, que es como un mecanismo para establecer confianza entre los proveedores de certificados digitales.

2.10.1.- Modelo jerárquico de una ICP

Consiste en generar una estructura de confianza de diferentes niveles que parta desde una Autoridad Certificadora Raíz (*ACRaíz*) de confianza, que será la encargada en controlar toda la infraestructura y certificará a otras *AC* que se

encuentran en un nivel más abajo, éstas *AC* serán las encargadas de certificar a los usuarios (entidades final) que se encuentra en el nivel más bajo de este modelo (Ver figura 15).

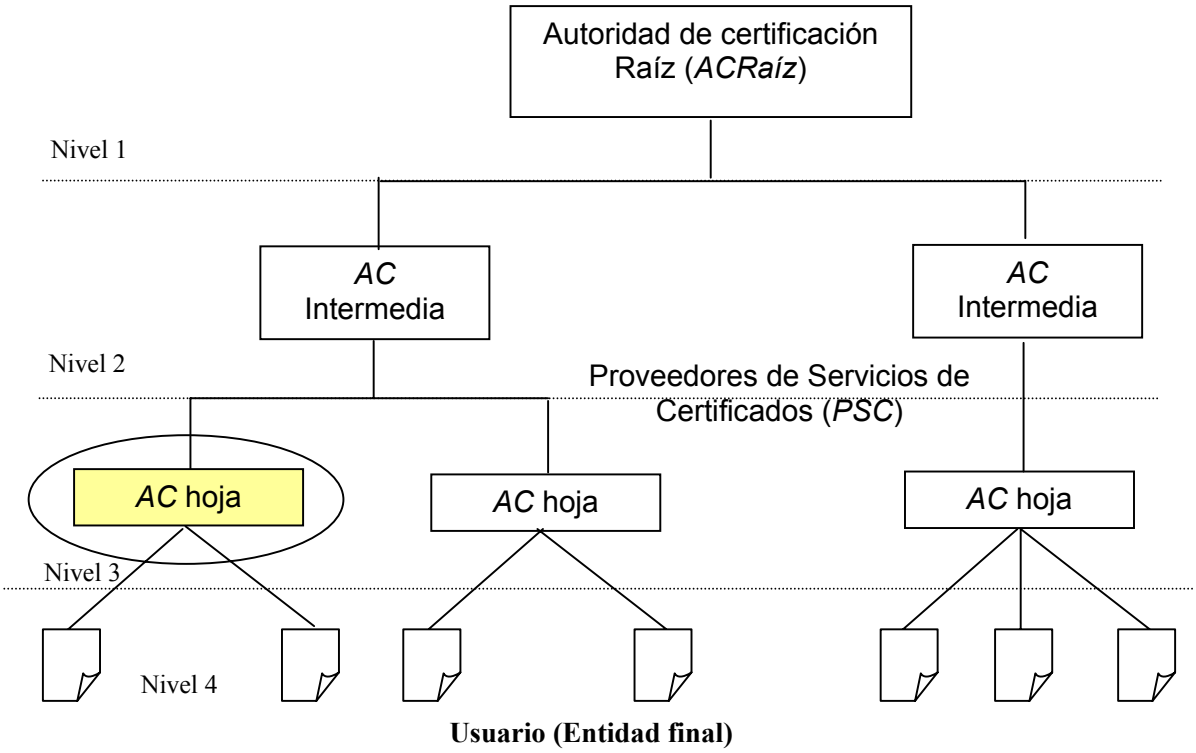

Figura 15. Ejemplo de Modelo jerárquico de una ICP.

En la figura 15 muestra un ejemplo de modelo de jerarquía de una *ICP* de cuatro niveles, y en este proyecto de grado desarrollaremos un *AC* hoja que se denomina como Proveedor de Servicios de Certificados (*PSC)*, que se encuentra en el tercer nivel del modelo, que certificara a los usuarios.

Este modelo de establecimiento de relaciones de confianza, es necesaria entre múltiples autoridades de certificación para garantizar que los usuarios (entidades finales) no tengan que depender y confiar en una sola *AC*, algo que haría imposible el manejo de estabilidad, administración y protección. El objetivo es que las entidades finales que utilizan identidades creadas por una *AC* puedan confiar en ellas, aunque dichas partes tenga una autoridad expedidora diferente.

2.10.2.- Componentes de una ICP

Los componentes más habituales de una infraestructura de claves públicas son: (Ver figura 16)

- Autoridad de certificación (*AC*): La *AC* es el componente responsable de establecer identidades y crear los certificados digitales que forman la asociación entre una identidad y una pareja de claves publica/privada. Es la entidad de confianza que da legitimidad a la relación de una clave pública con la identidad de un usuario o servicio.

- Autoridad de registro (*AR*): La *AR* es el componente responsable de las tareas administrativas asociadas con el registro y la autenticación inicial de los usuarios a quienes se les expide un certificado.

- Administrador Pub (*PUB*): El *PUB* es el componente que funciona como interfaz entre el proveedor y la entidad final y tiene la responsabilidad de gestionar los certificados digitales.

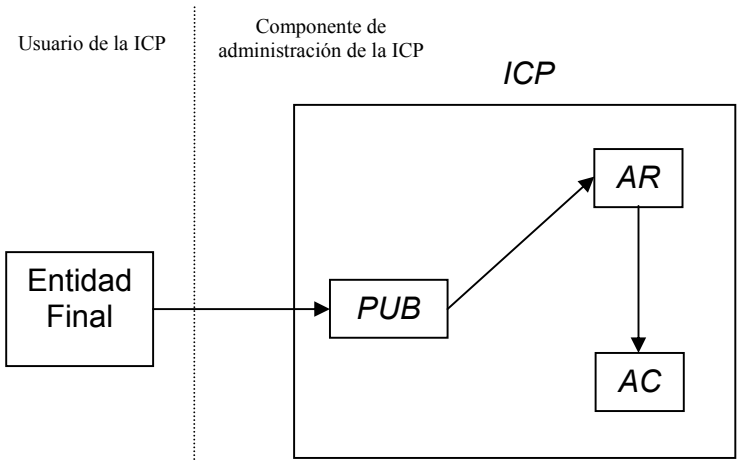

Figura 16. Componentes más habituales de una ICP

2.11.- Software Libre:

El software libre es un asunto de libertad, no de precio. Para que un programa de software concreto se considere como software libre debe cumplir con las siguientes libertades:

Libertad 0: Libertad de ejecutar el programa en cualquier sitio, cualquier propósito, por siempre.

Libertad 1: Liberta de estudiarlo y adaptarlo a nuestras necesidades.

Libertad 2: Libertad de redistribuirlo, logrando ayudar a un amigo o vecino.

Libertad 3: Libertad de mejorar el programa y publicar las mejoras.

2.11.1.- Beneficio del software libre al Usuario Final:

- No depender de un fabricante.
- No confiar en lo que diga el fabricante acerca de sus productos
- Facilidad de probar distintas alternativas.
- Corrección de errores rápida.

2.11.2.- Beneficios del software libre. Administración Pública (Usuario final):

- Integridad
- Disponibilidad
- Seguridad
- Utilidad

- Estándares
- Promueve el crecimiento de las Pequeñas y medianas empresas.
    - Adaptar
    - Mantener
    - Integrar
    - Auditar

2.11.3.- Beneficios del software libre. Desarrollador de Software libre:

- Ser Competitivo
- Fácil Crecimiento
- Le permite obtener ultima tecnología a muy bajo costo
- Aprovechar trabajos previos.
- Rápido desarrollo.
- Colaboración.

2.12.- Introducción al Lenguaje Unificado de Modelado:

(*UML*, Por sus siglas en ingles, Unified Modelling language) es una herramienta que permite diseñar sistemas a las cuales se les conoces como modelos, mediante un conjunto de símbolos y diagramas en donde se plasma las ideas de funcionalidad del mismo. Cada diagrama tienes fines distintos dentro del proceso de desarrollo, su finalidad es presentar diversas perspectivas de un sistema. La clave está en organizar el proceso de diseño de tal forma que los analistas, clientes, desarrolladores y otras personas involucradas en el desarrollo

del modelo lo comprendan y convengan con él. Entre los diagramas se encuentran:

- Diagramas de casos de usos
- Diagramas de actividades
- Diagramas de componentes
- Diagrama de despliegue

2.12.1.- Diagramas de casos de usos:

Según J. Shumuller [3]. Son descripciones de las acciones que debe realizar el usuario en el sistema. Por ejemplo: Usuario que tiene la necesidad de expedir un certificado digital a una *AC* de confianza (Ver figura 17)

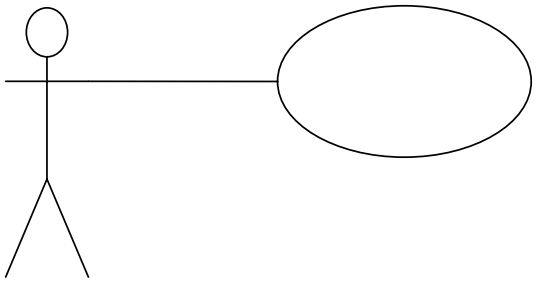

Figura 17. Diagrama de Caso de Uso.

2.12.2.- Diagramas de actividades:

Según P. Muller [5]. Muestran las actividades que ocurren dentro de un caso de uso o dentro de un comportamiento de un objeto. Por ejemplo, las actividades que se realizan para expedir un certificado digital

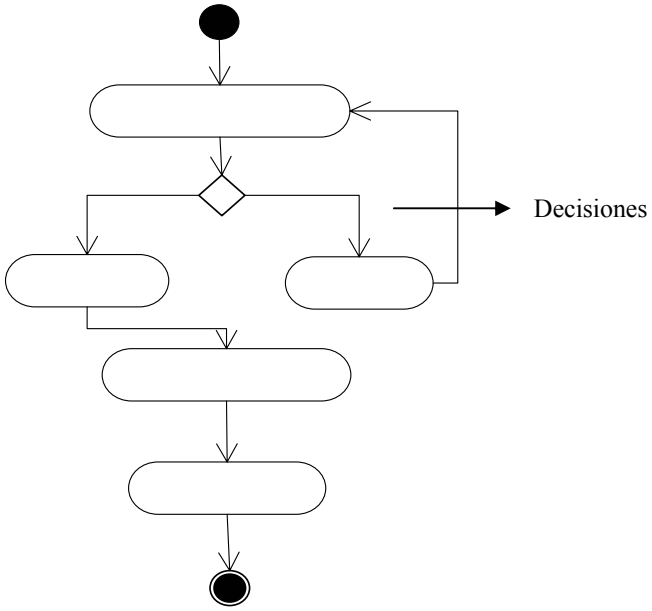

Figura 18. Diagramada de Actividades.

2.12.3.- Diagramas de Componentes:

Según G. Booch [4]. Los Componentes pertenece al mundo material de los bits, son utilizados para modelar los aspectos físicos de los sistemas orientados a objetos. Estos diagramas muestran la organización y las dependencias entre un conjunto de componentes. (Ver figura 19)

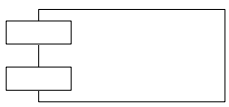

Figura 19. Símbolo que representa a un componente

2.12.4.- Diagramas de Despliegue:

Según G. Booch [4]. Se utilizan para modelar los aspectos físicos de los sistemas. Este diagrama muestra la configuración de los nodos que participan en la ejecución y de los componentes que residen en ellos. (Ver figura 20)

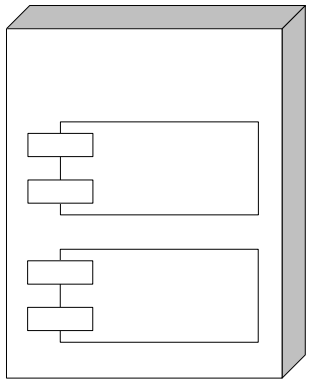

Figura 20. Nodos y sus componentes

3.- Capitulo 3: Modelado del *PSC* usando *UML*

En este capitulo, se estudian las políticas de certificación estándar de un *PSC* (Anexo C) y de otros aspectos que forman parte de la administración de los certificados digitales con el objetivo de modelar el *PSC*, utilizando el lenguaje del *UML*.

El *PSC* es una oficina con características particulares y se modelan tres aspectos importantes de ella como son: software, hardware y políticas, que intervienen en el modelo, que permitan realizar de forma segura todas las tareas vinculadas a la administración de los certificados digitales.

Se utilizarán los diagramas de Casos de Uso y los diagramas de Actividades, para mostrar que acciones y actividades deben realizar los diferentes actores que intervienen en el PSC, con fin de extraer, o conocer los requisitos necesarios para su desarrollo.

En cada diagrama *UML* se muestra las acciones que realizan los actores tanto con el software como el hardware.

3.1.- Diagrama de Caso de Uso. General

En la figura 21 muestra un diagrama de caso general de uso que muestra actores que intervienen en el *PSC.*

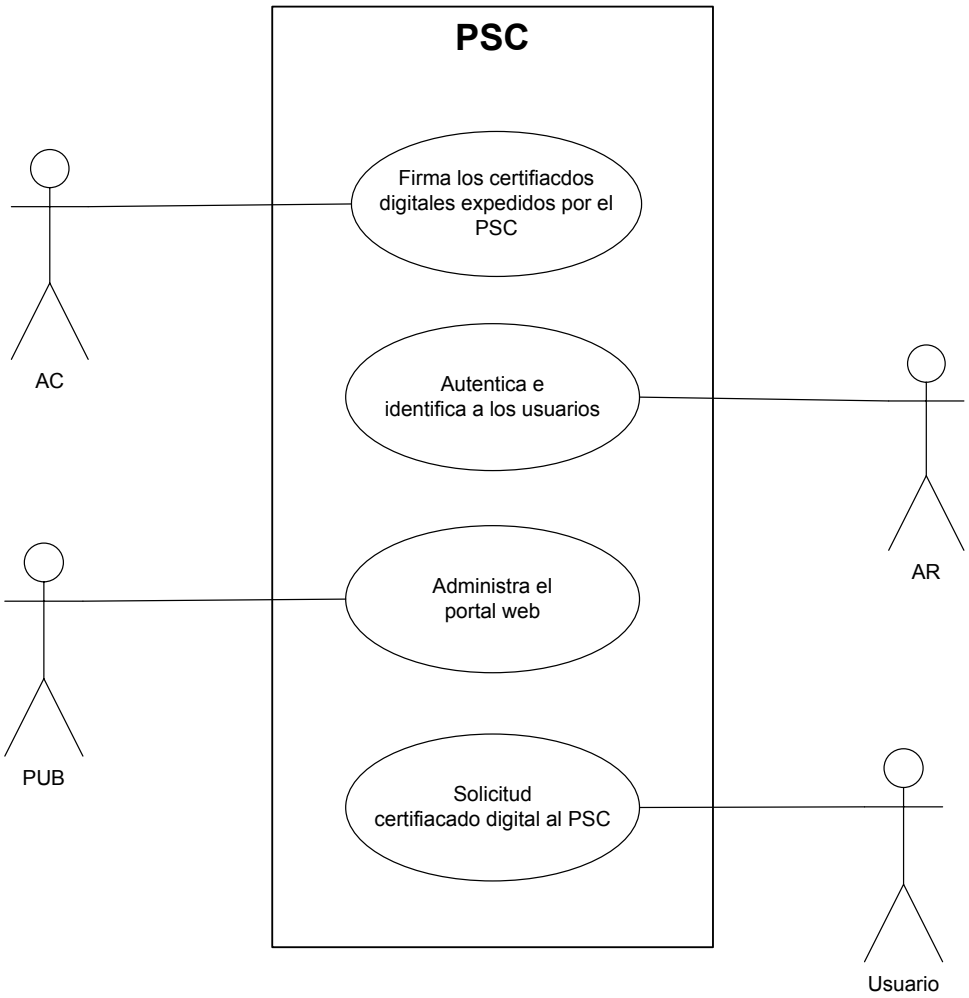

Figura 21. Diagrama de Casos de Uso. Actores que intervienen en el proceso de solicitud de certificado de digital en el PSC

3.2.- Diagrama de Casos de Uso. Solicitud de certificado digital al PSC

El diagrama de la figura 22 muestra las acciones que realiza el actor usuarios para obtener un certificado del *PSC*.

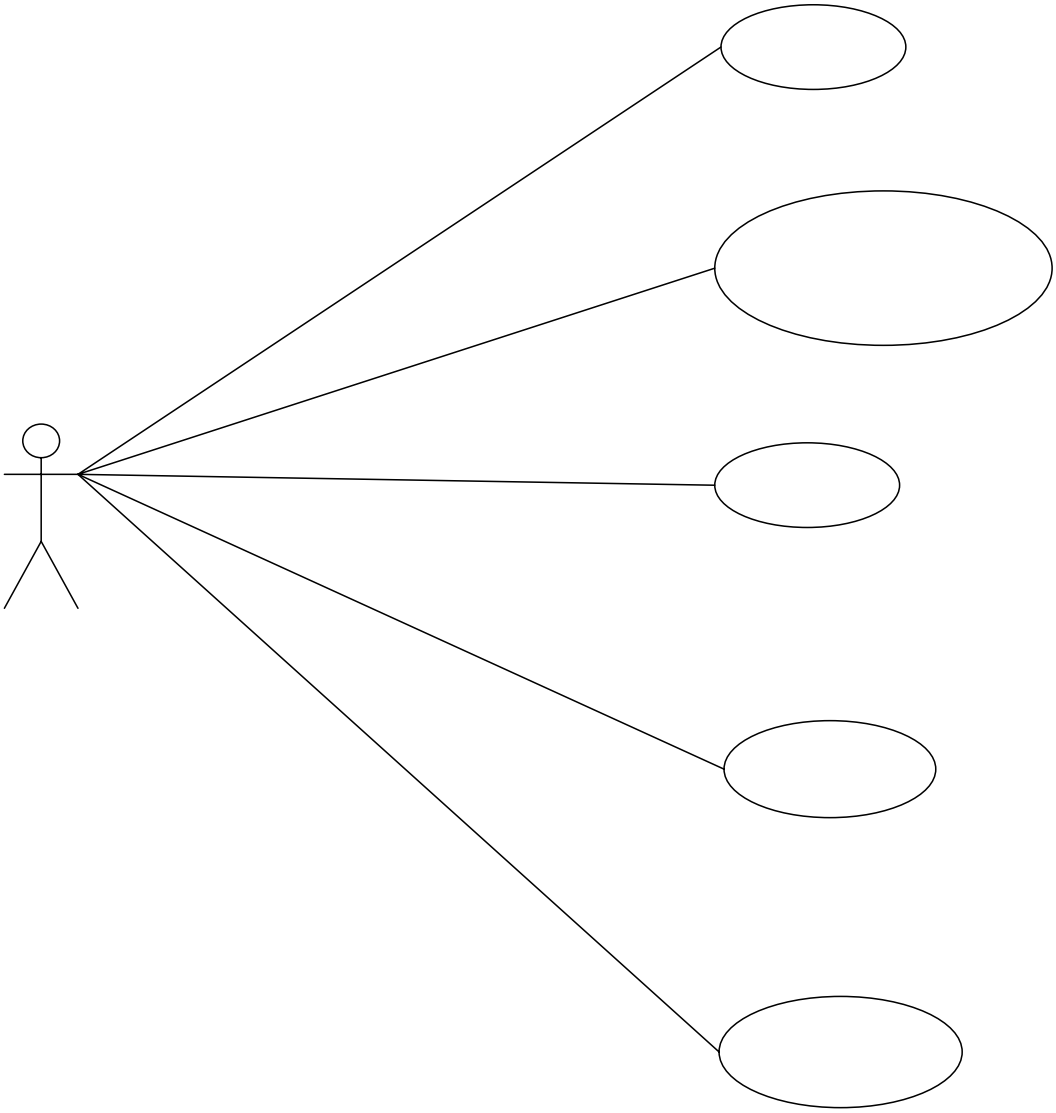

Figura 22. Diagrama de Caso de Uso para el proceso de solicitud de certificado digital por parte del usuario (entidad final)

Descripción del diagrama de la figura 22.

3.2.1.- Usuario (Entidad final)

Persona natural o jurídica que voluntariamente confía y hace uso de los certificados del PSC, y realiza las siguientes responsabilidades:

- Conserva y utiliza correctamente el certificado.
- Custodia el certificado, de forma diligente, tomando las precauciones razonables para evitar su pérdida, revelación, modificación o uso no autorizado.
- No revela la clave privada ni el código de activación del Certificado.
- Se asegura de que toda la información contenida en el Certificado es cierta y cualquier cambio o variación que haya sufrido cualquiera de los datos que aportó para adquirir el Certificado, notificar inmediatamente al *PSC.*

3.2.2.- Caso de Uso

3.2.2.1- Solicita Certificado

Los usuarios tienen la necesidad de poseer un certificado digital para que realice transacciones digitales de manera segura, por ejemplo, para firmar y cifrar los mensajes por correo electrónicos. Los usuarios se dirigen a un *PSC* de confianza a través de su *URL*, y realizan las solicitudes de certificados, ingresando un registro inicial de su identidad y el tipo de certificado digital que desea expedir.

Acción del actor: Usuario	Interfaz de la *PSC*
1. Accede al *URL* del *PSC* y realizar la solicitud. 2. Introduce los requisitos necesarios para que realice la solicitud de certificado. 4. Envía la solicitud	3. Registra la solicitud de certificado por medio de un formulario de requisito. 5. Envía y almacena las solicitudes de certificado en el repositorio de la interfaz del *PUB*

Tabla 1. Caso de Uso: Solicita Certificado

3.2.2.2.- Acepta pre-aprobación o negación de la solicitud de certificado

Los usuarios reciben del *PSC* por medio de un correo electrónico o una llamada, donde le informa el estado (pre-aprobado o negado) de la solicitud de certificado digital.

Pre-aprobado: Si la información suministrada en la solicitud de certificado es aceptada por *PSC*, pasa a la otra instancia del proceso de la expedición del certificado.

Negado: Si la información suministrada en la solicitud de certificado no fue aceptada por del *PSC*, debe realizar las correcciones del caso y volver a solicitar el certificado digital.

Acción del actor: Usuario	Interfaz de la *PSC*
2. Revisa el correo electrónico que le envía el *PSC* para tener conocimiento del estado en que se encuentra su solicitud	1. Envía correo electrónico al usuario informando el estado de la solicitud.

Tabla 2. Caso de Uso: Acepta pre-aprobación o negación de la solicitud de certificado

3.2.2.3.- Acepta kit

Recibe del *PSC* el kit que contiene: tarjeta inteligente, lector de tarjeta inteligente, pin, instrucciones para que inicialice la tarjeta inteligente. El usuario revisa que el kit llegue en buen estado y que contenga todas las partes. Los usuarios que tienen el estado de solicitud pre-aprobado reciben el kit.

Acción del actor: Usuario	Interfaz de la *PSC*
1. Recibe el kit por parte de la *PSC*	2. verifica que el usuario recibió el kit.

Tabla 3. Caso de Uso: Acepta kit

3.2.2.4.- Inicializa tarjeta inteligente

Se refiere a la generación del par de claves (pública/privada). por políticas de seguridad, y responsabilidad el usuario debe ser quien inicialice la tarjeta inteligente, ya que el es el único que puede conocer la clave privada y es responsable de custodiar.

Acción del actor: Usuario	Interfaz de la *PSC*
1. Accede a la *URL* de la PSC, en la sección inicializar tarjeta inteligente. 2. Introduce la tarjeta inteligente al lector de tarjeta. 4. Comienza el proceso de inicializar de la tarjeta inteligente	3. Reconoce la tarjeta inteligente. 5. Genera el par de clave (publica/privada). 6. Almacena el par de clave en la tarjeta inteligente. 7. Almacena la clave publica.

Tabla 4. Caso de Uso: Inicializa tarjeta inteligente.

3.2.2.5.- Consigna recaudos

De acuerdo al tipo de certificado digital solicitado debe consignar ciertos recaudos como por ejemplo: presentarse en la oficinas del PSC, Fotocopia de la cedula de identidad, fotografía, fotocopia del rif (si se trata de una entidad), carta de autorización del Suscriptor al solicitante (si se trata de una entidad), otros.

Acción del actor: Usuario	Interfaz de la *PSC*
1. Consigna los recaudos solicitados por la *PSC* al *PUB* físicamente o electrónicamente	2. recibe y almacena los recaudos consignados electrónicamente.

Tabla 5. Caso de Uso: Consigna recaudos

3.3.- Diagrama de casos de uso expedir un certificado en el PSC por parte del *PUB*.

En el diagrama de la figura 23 se muestras las acciones que realiza el *PUB* en el proceso de expedir un certificado en el *PSC*.

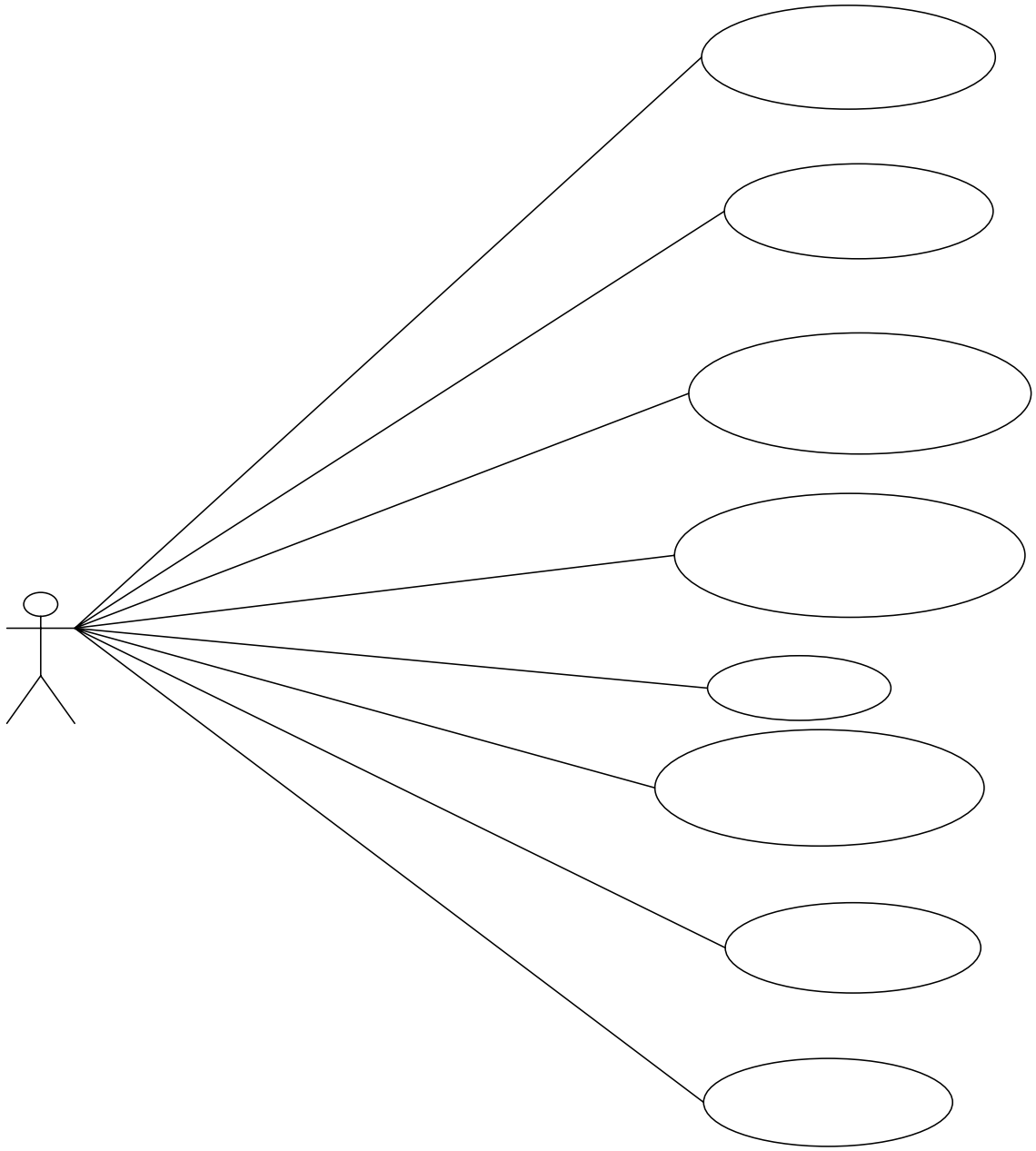

Figura 23. Diagrama de Caso de Uso para el proceso de solicitud de certificado digital por parte del PUB

Descripción del diagrama de la figura 23.

3.3.1.- *PUB*

Persona empleada del *PSC*, que tiene la función de servir de enlace entre los usuarios y el *PSC*. Entre las responsabilidades que realiza el *PUB*:

- Administra el portal Web del *PSC.*
- Atiende reclamos, sugerencias y comentarios de los usuarios.
- Gestiona las solicitudes realizadas a través del portal, chequear las solicitudes pendientes, válidas, no válidas, enviar kit, etc.
- Formaliza el Contrato de Certificación pertinente con el usuario según los términos establecidos por la Política de Certificación del *PSC*.

El *PUB* posee un certificado digital expedido por la *PSC*, almacenado en una tarjeta inteligente, que es utilizado para autenticar y autorizar el acceso a la interfaz del *PUB*

3.3.2.- Caso de Uso

3.3.2.1.- Acepta las solicitudes de certificados enviadas por los usuarios

El *PUB* recibe las solicitudes de certificados que gestionan los usuarios a través del portal web del *PSC*, que están almacenadas en el repositorio del *PUB* y las procesas.

Acción del actor: *PUB*	Interfaz del *PUB*
1. Accede a la interfaz del *PUB* usando la tarjeta inteligente del *PUB*. 3. Accede al repositorio donde se encuentra almacenado las solicitudes de certificados enviadas por los usuarios. 5. Revisa si existe alguna inconsistencia en la información suministrada en las solicitudes	2. Autentica y autoriza el acceso a la interfaz. 4. Se conecta al repositorio.

Tabla 6. Caso de Uso: Acepta las solicitudes de certificados enviadas por los usuarios

3.3.2.2.- Envía las solicitudes de certificados a la *AR*

El *PUB* envía por lotes o por unidad las solicitudes de certificados procesadas a la encargada de verificar la identidad inicial de los usuarios, que en nuestro caso es la *AR*.

Acción del actor: *PUB*	Interfaz del *PUB*
Estando dentro de la interfaz del *PUB* 1. Envía las solicitudes procesadas a la *AR*.	2. Envía y almacena las solicitudes enviadas por el *PUB* en el repositorio de la interfaz de la *AR*.

Tabla 7. Caso de Uso: Envía las solicitudes de certificados a la AR

3.3.2.3.- Recibe respuestas de las solicitudes de certificados por parte de la *AR*

Recibe de la *AR* la pre-aprobación o negación de las solicitudes de certificado (estado de la solicitud de certificado, explicado en el diagrama de la figura 27)

Acción del actor: *PUB*	Interfaz del *PUB*
Estando dentro de la interfaz del *PUB* 1. Accede al repositorio donde se almacena la repuesta de solicitud enviada por la *AR*.	2. Se conecta al repositorio.

Tabla 8. Caso de Uso: Recibe respuestas de las solicitudes de certificados por parte de la AR.

3.3.2.4.- Notifica a los usuarios el estado en que se encuentra la solicitud de certificado

Notifica por medio de un correo electrónico o una llamada telefónica a los usuarios, el estado en que se encuentra la solicitud de certificado (estado de la solicitud de certificado, explicado en el diagrama de la figura 27).

Acción del actor: *PUB*	Interfaz del *PUB*
Estando dentro de la interfaz del *PUB* 1. Envía a los usuarios el estado en que se encuentra la solicitud.	2. Envía correo electrónico a los usuarios.

Tabla 9. Caso de Uso: Notifica a los usuarios el estado en que se encuentra la solicitud de certificado

3.3.2.5.- Empaqueta Kit

Prepara los kit que contiene: la tarjeta inteligente, el lector de la tarjeta inteligente, un pin, las instrucciones para inicializar la tarjeta inteligente, y envía el kit de manera segura (por ejemplo: custodiada por una empresa de blindados) a los usuarios que tengan las solicitudes pre-aprobadas.

Acción del actor: *PUB*	Interfaz del *PUB*
1. Prepara los kit. 2. Envía los kit.	3. Marca a los usuarios que se le va enviar el kit.

Tabla 10. Caso de Uso: Empaqueta Kit

3.3.2.6.- Notifica a los usuarios de los recaudos y la expedición de certificado.

Avisa a los usuarios por medio de correo electrónico o una llamada, los recaudos que debe enviar o presentar los usuarios, de acuerdo al tipo de certificado que este solicitando o notificando la expedición del certificado.

Acción del actor: *PUB*	Interfaz del *PUB*
Estando dentro de la interfaz del *PUB* 1. Notifica a los usuarios los recaudos que debe consignar al *PSC*.	2. Envía correos electrónicos a los usuarios la información de los recaudos que debe consignar.

Tabla 11. Caso de Uso: Notifica a los usuarios de los recaudos

3.3.2.7.- Envía los certificados a la *AC* para que los firme

Envía por lotes todos los certificados que se procesan y aprueba la *AR,* a la *AC* que es la encargada de firmar los certificados digitales que son expedido.

Acción del actor: *PUB*	Interfaz de la *PUB*
Estando dentro de la interfaz del *PUB* 1. Envía los certificados a *AC*	2. Envía los certificados y los almacena en el repositorio del *AC*

Tabla 12. Caso de Uso: Envía los certificados a la AC para que los firme.

3.3.2.8.- Publica los certificados firmados

Publica los certificados que se expiden en un repositorio publico, para que puedan ser consultados, verificados por sistemas o terceras personas interesarlas de hacerlos.

Acción del actor: *PUB*	Interfaz de la *PUB*
Estando dentro de la interfaz del *PUB* 1. Publica los certificados que se expiden en el repositorio público.	2. Almacena los certificados expedido en un repositorio público.

Tabla 13. Caso de Uso: Publica los certificados firmados

3.4.- Diagrama de caso de uso Proceso de expedir un certificado en el *PSC* por parte de la *AR.*

En el diagrama de la figura 24 muestra las acciones que realiza la *AR* en el proceso de expedir un certificado.

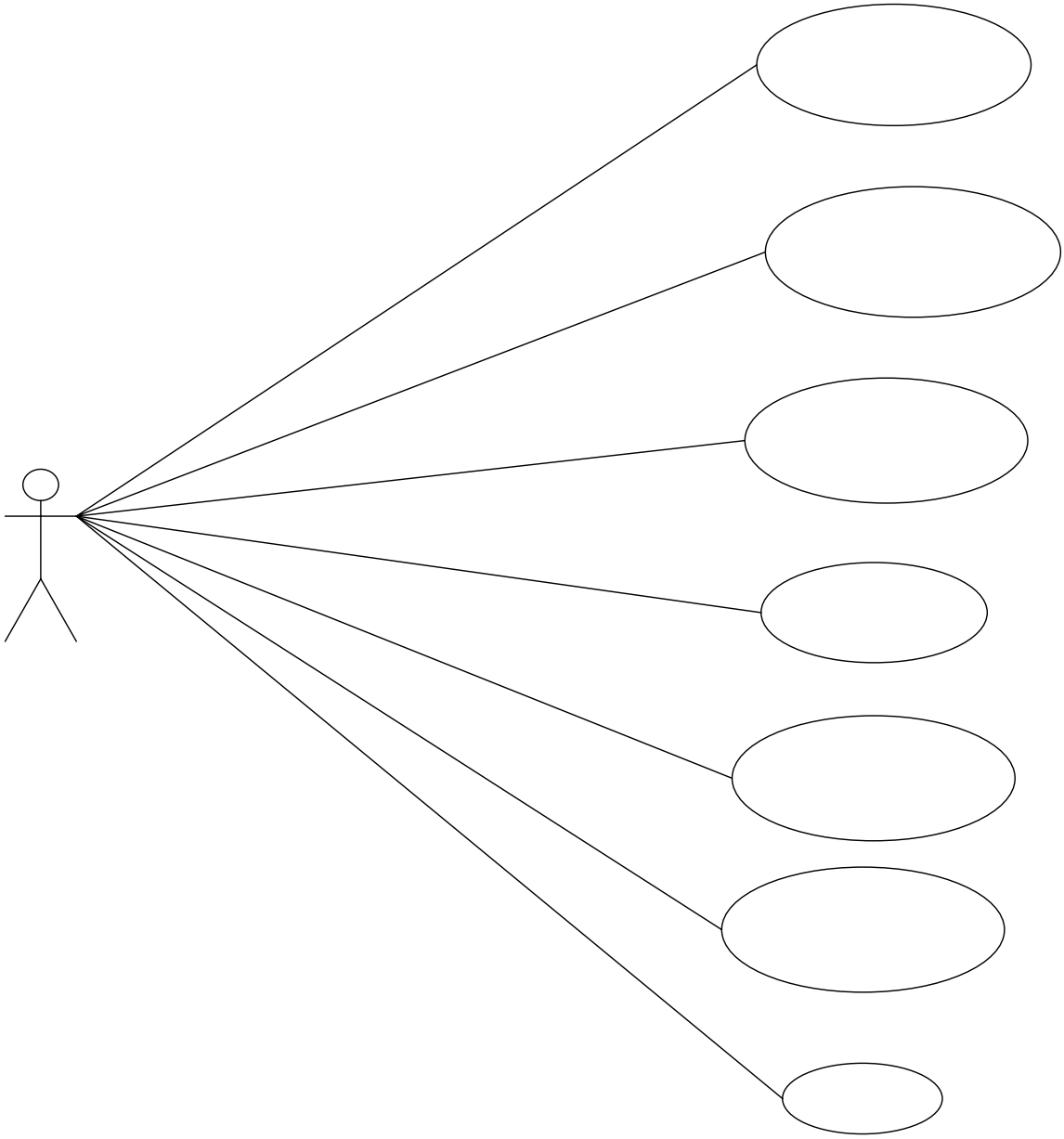

Figura 24. Diagrama de Caso de Uso para el proceso de solicitud de certificado digital por parte de la AR.

Descripción del diagrama de la figura 24.

3.4.1.- *AR*

Persona empleada del *PSC*, entre las responsabilidades que realiza:

- Autentica e identifica a los solicitantes de certificados digitales.
- Verifica la validez de la información suministrada por los solicitantes.
- Verifica que el usuario en realidad posee la clave privada que se va a registrar. Por lo general se conoce como prueba de posesión (*POP*).
- Almacena de forma segura y permanente (el periodo que quede estipulado en la política de certificación) la documentación aportada por el usuario para los procesos de emisión de certificación y de suspensión/revocación del mismo.

La *AR* posee un certificado digital expedido por la PSC, que se almacena en una tarjeta inteligente, que es utilizado para autenticar y autorizar el acceso a la interfaz de la *AR* y para realizar algunos procesos dentro del interfaz como por ejemplo firmar.

Por razones de responsabilidad, la *AR* debe firmar los procesos que realiza para verificar la validez de la información suministrada por los usuarios, con su clave privada. Si se llega a darse el caso que la identidad de un usuario es falsa y la *AR* aprobó la solicitud, es el único responsable y puede verificarse con la firma de la aprobación.

3.4.2.- Caso de Uso

3.4.2.1.- Acepta solicitud de certificado por parte del PUB

Recibe por lotes o por unidad las solicitudes de certificados que chequeo inicialmente el *PUB* y la envío al repositorio del interfaz de la *AR*.

Acción del actor: *AR*	Interfaz de la *AR*
1. Accede a la interfaz de la *AR* usando la tarjeta inteligente del *AR*. 3. Accede al repositorio donde se encuentra almacenado las solicitudes enviadas por el *PUB*.	2. Autentica y autoriza el acceso a la interfaz de la *AR*. 4. Se conecta al repositorio.

Tabla 14. Caso de Uso: Acepta solicitud de certificado por parte del PUB

3.4.2.2.- Chequear la información de la solicitud de certificado

Por razones de responsabilidad, el *AR,* chequea la información que suministra los usuarios en la solicitud de certificado (Registro inicial de la identidad del usuario) para verificar la información, para ello puedo apoyarse de una base de datos de una organización a la que se le esta certificado las personas que laboran en la organización.

Acción del actor: *AR*	Interfaz de la *AR*
Estando dentro de la interfaz de la *AR* y en el repositorio. 2. Selecciona la solicitud a chequear. 4. Chequea la información inicial suministrada por el usuario en la solicitud	1. Lista de solicitudes. 3. despliega la información suministrada en la solicitud seleccionada.

Tabla 15. Caso de Uso: Chequea la información de la solicitud de certificado.

3.4.2.3.- Pre-aprueba la solicitud de certificado

Si se autentica la información inicial suministrado por los usuarios en las solicitudes de certificados, el *AR* pre-aprueba esas solicitudes de certificado y las firma digitalmente usando la clave privada de la *AR;* por razones de responsabilidad, y envía al *PUB* la pre-aprobación de la solicitud de certificado.

Acción del actor: *AR*	Interfaz de la *AR*
Estando dentro de la interfaz de la *AR* 1. Pre – aprueba las solicitudes (Estado de solicitud). 2. Firma las pre-aprobación. 2.1 Accede a la sección de firmar e introduce la tarjeta inteligente de la *AR* para que comienza el proceso de firmar.	3. Autentica y autoriza que se realice el proceso de firmar. 4. Firma digitalmente la pre-aprobación de las solicitudes.

Tabla 16. Caso de Uso: Pre-aprueba la solicitud de certificado

3.4.2.4.- Niega la solicitud de certificado

Si no se pudo autenticar la información inicial suministrado por los usuarios en las solicitudes de certificados, el *AR* no aprueba esas solicitudes de certificado y las firma digitalmente usando la clave privada de la *AR;* por razones de responsabilidad, y enviara al *PUB* la no aprobación de la solicitud de certificado.

Acción del actor: *AR*	Interfaz de la *AR*
Estando dentro de la interfaz de la *AR* 1. Niega las solicitudes (Estado de solicitud). 2. Firma la negación de las solicitudes. 2.1 Accede a la sección de firmar e introducir la tarjeta inteligente de la *AR* para comenzar el proceso de firmar.	3. Autentica y autoriza que se realice el proceso de firmar. 4. Firma digitalmente la negación de las solicitudes.

Tabla 17. Caso de Uso: Niega la solicitud de certificado.

3.4.2.5.- Aprueba la solicitud de certificado

Si los recaudos presentados por los usuarios fueron validos, el *AR* aprueba esas solicitudes de certificado y la firma digitalmente usando la clave privada de la *AR;* por razones de responsabilidad, y envía al *PUB* la aprobación de la solicitud de certificado.

Acción del actor: *AR*	Interfaz de la *AR*
Estando dentro de la interfaz de la *AR* 1. Aprueba las solicitudes. 2. Firma la aprobación de solicitudes. 2.1 Accede a la sección de firmar e introducir la tarjeta inteligente de la *AR* para comenzar el proceso de firmar.	3. Autentica y autoriza que se realice el proceso de firmar. 4. Firma digitalmente la aprobación de solicitudes.

Tabla 18. Caso de Uso: Aprueba la solicitud de certificado.

3.4.2.6.- Niega la solicitud de certificado

Si los recaudos presentados por el usuario no se pudo autenticar, el *AR* no aprueba la solicitud de certificado y la firma digitalmente usando la clave privada

de la *AR;* por razones de responsabilidad, y envía al *PUB* la no aprobación de la solicitud de certificado.

Acción del actor: *AR*	Interfaz de la *AR*
Estando dentro de la interfaz de la *AR* 1. Niega las solicitudes. 2. Firma la negación de solicitudes. 2.1 Accede a la sección de firmar e introducir la tarjeta inteligente de la *AR* para comenzar el proceso de firmar.	3. Autentica y autoriza que se realice el proceso de firmar. 4. Firma digitalmente la negación de solicitudes.

Tabla 19. Caso de Uso: Niega la solicitud de certificado

3.4.2.7.- Solicita los recaudos

Solicita los recaudos necesarios que debe consignar los usuarios de acuerdo al tipo de certificado solicitado, para que el certificado pase a la siguiente instancia del proceso de expedición de certificado digital, estos recaudos van a depender del tipo de certificado solicitado.

Acción del actor: *AR*	Interfaz de la *AR*
Estando dentro de la interfaz de la AR 1. Envía al *PUB* los recaudos que debe consignar el usuario.	2. Envía las solicitudes de recaudos y los almacena en el repositorio del *PUB*.

Tabla 20. Caso de Uso: Solicitud de recaudos

3.5.- Diagrama de casos de uso proceso de expedir un certificado en el *PSC* por parte de la *AC.*

En este diagrama muestra las acciones que debe realizar la *AC* del *PSC* en el proceso de expedir un certificado.

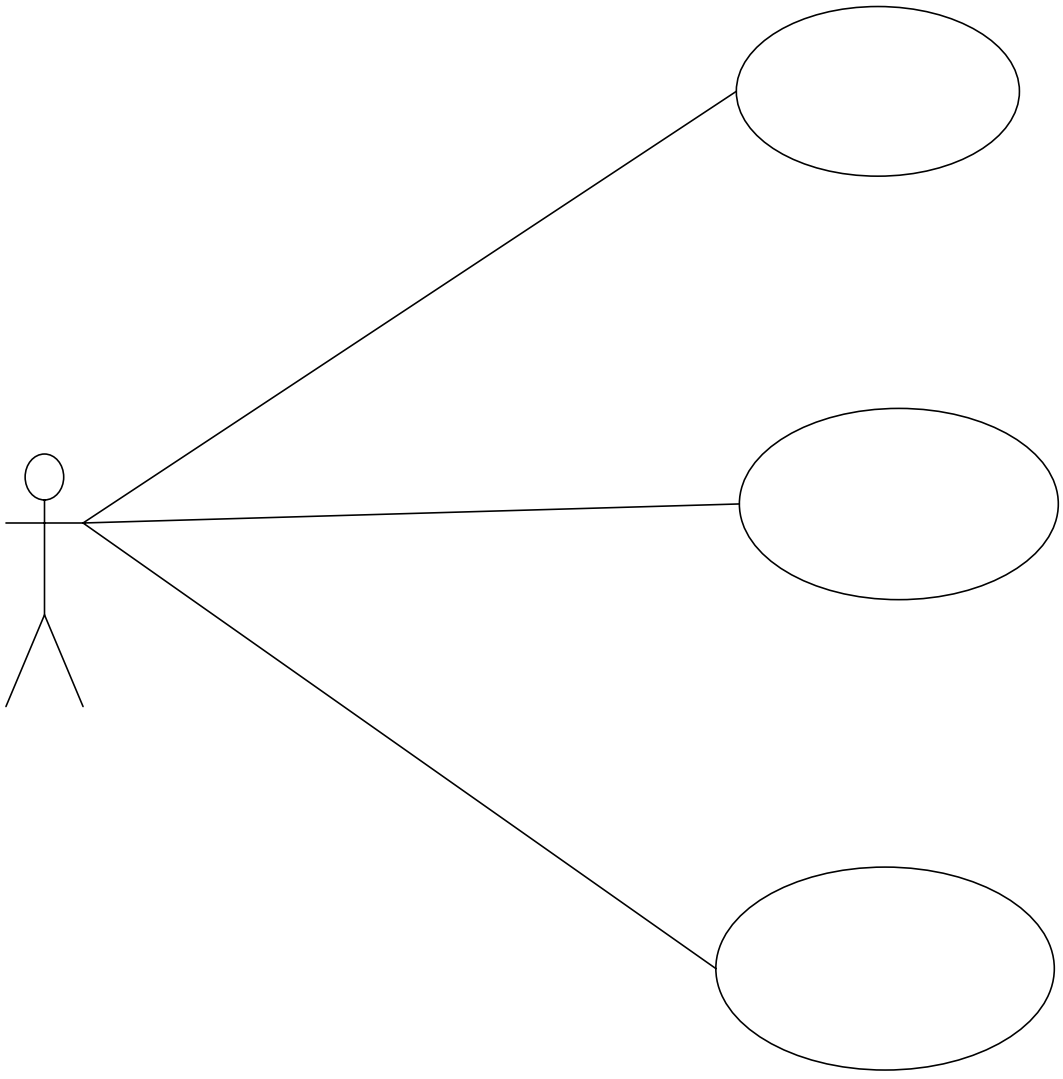

Figura 25. Diagrama de Caso de Uso proceso de expedir un certificado digital en el PSC por parte de la AC

Descripción del diagrama de la figura 25.

3.5.1.- *AC*

Personas empleadas del *PSC*, responsables en firmar los certificados digitales expedidos y custodiar la clave privada del *PSC*. En este modelo por razones de seguridad la *AC* esta formada por tres (3) personas, cada uno con certificados digitales diferentes, que se almacenan en tarjetas inteligentes, que se utiliza para autenticar y autorizar el acceso a la interfaz de la *AC* y realizar algunos procesos dentro del interfaz como por ejemplo firmar los certificados, donde se requiere que dos (2) de las tres (3) tarjetas, introduzcan las tarjetas inteligentes, para autenticar y validar el proceso de firmar. La clave privada del *PSC* debe estar bien protegida por un dispositivo de software o bien por un dispositivo de hardware como por ejemplo un *HSM*. Es recomendable que este dispositivo se encuentra en un lugar seguro como por ejemplo: una bóveda de seguridad, con una fuerte autenticación, autorización y control de accesos, Y que permanezca fuera de línea para evitar compromisos de la clave privada.

3.5.2.-Caso de Uso

3.5.2.1.- Acepta los certificados por la *AR*

Recibe en un lote, los certificados que han sido procesados y aprobados por la *AR*, para que sea expedido. Por razones de responsabilidad; se verifica la firma de *AR* en los certificados aprobados y luego firma los certificados. Como el interfaz de la *AC* esta fuera de línea, es necesario almacenar el lote de certificados en un dispositivo de almacenamiento portátil como por ejemplo, pendrive (token con clave), para que se descargué en el interfaz de la *AC.*