Universidad de los Andes
Facultad de Ingeniería
Escuela de Sistemas
Departamento de Computación

MODELO DE UNA AUTORIDAD DE CERTIFICACIÓN DIGITAL RAÍZ BAJO ESTÁNDAR X.509 UTILIZANDO SOFTWARE LIBRE

Br. Paola Ibarra R.
Tutor: Prof. Víctor Bravo

UNIVERSIDAD DE LOS ANDES
FACULTAD DE INGENIERíA

El jurado aprueba el proyecto de grado titulado "**Modelo de una Autoridad de Certificación Digital Raíz bajo estándar X.509 Utilizando Software Libre**" realizado por **Br. Paola Ibarra R.** como requisito parcial para la obtención del grado de **Ingeniero de Sistemas**.

Fecha: Diciembre 2006

Tutor: _____
Prof. Víctor Bravo

Jurado: _____
Prof. Judith Barrios

_____
Prof. Leandro León

A mis padres Martha Eugenia Rodríguez Fonseca y José Rafael Ibarra Niño, por apoyarme y ayudarme desde siempre a conseguir los logros personales y académicos hasta hoy obtenidos, y más importante aún por estar conmigo incondicionalmente en los momentos más difíciles. Estas son algunas de las razones por las cuales deben saber que los amo. Con la obtención de mí primer título profesional espero haber satisfecho las expectativas en ustedes generadas, y que con eso se sientan orgullosos de lo que yo considero una excelente labor como padres y amigos.

Índice general

Índice de cuadros

Índice de figuras

Agradecimientos

Hay cinco personas a las que sin duda debo mencionar porque les estoy enormemente agradecida:

- A **mi tutor Profesor Víctor Bravo**, por su apoyo y confianza, así como por su disposición en todo momento para resolver cualquier duda surgida durante el desarrollo de la tesis.
- Al **Ing. Antonio Araujo**, por su amabilidad y cooperación.
- A **Rafael**, eres un ángel que cayó en mi vida, siempre respondes a mis gritos de auxilio ayudándome. Te quiero
- A **Pedro**, por darme ánimo siempre, eres un excelente amigo.
- A **Carlos**, por ayudarme en el último instante.

También a todas las personas que creyeron en mí y me apoyaron, ayudaron y guiaron en mi formación profesional y en la consecución de mi título de Ingeniero de Sistemas. Estoy consiente de que son pocos, pero antes de olvidar incluir a alguno prefiero generalizar sabiendo inequívocamente que solo sentirán este agradecimiento aquellos que realmente sintieron mi necesidad de ser ayudado y que respondieron a esta sin esperar recibir más que un agradecimiento que espero haya sido bien recibido y que reitero a través de estas palabras: MUCHAS GRACIAS !!!

Capítulo 1

Introducción

La llegada de Internet, permite a cualquier persona, empresa, corporación, administración, etc., realizar transacciones gubernamentales, comerciales o personales entre otras a través de este medio. Dadas las ventajas inimaginables al utilizar internet para relaciones humanas, se está de acuerdo en que es necesario poder implantar el concepto de identidad. La criptografía es una herramienta matemática que ayuda a conseguirlo, para ello proporciona mecanismos y algoritmos que aportan esa identidad a la que se está familiarizado en el mundo real.

En muchas ocasiones en nuestro quehacer cotidiano, se debe establecer contacto personal con un individuo u organización que no hemos visto antes y del que no tenemos ninguna referencia, nuestros sentidos nos permiten percibir gran número de detalles que le caracterizan y cuya combinación muy probablemente le hace irrepetible pero, y a pesar de todo, no sabemos quién es.

La identidad se puede definir como el reconocimiento que se hace de las credenciales físicas o informativas, que ese individuo ofrece para que le acepte como poseedor de una determinada identidad [11]. Las credenciales físicas pueden ser documentos como la Cédula de Identidad, el Pasaporte, la Licencia, etc., ya que en todos ellos se dispone de una fotografía que comparar con la apariencia de nuestro interlocutor, de un nombre, de una

firma manuscrita y, posiblemente, de un número de referencia.

Las credenciales informativas podrían ser ciertas informaciones que sólo conocen unos pocos y cuya expresión por parte del desconocido nos haría pensar sobre su pertenencia a dichos grupos selectos. Ahora bien, si nos presentan credenciales o informaciones que previamente nosotros no conocemos, la identificación de ese individuo es imposible; sólo reconoceremos a aquellos que nos presenten credenciales que ya habíamos visto antes y que, a nuestro entender, son auténticas.

La autenticidad de las credenciales, a su vez, consiste en que encontremos en los documentos presentados, signos reconocibles cuyas características y dificultad de reproducción permitan confiar en que sólo una autoridad conocida ha podido expedirlos y que lo ha hecho en condiciones perfectamente definidas. El ejemplo mas típico de este proceder es el de los billetes de banco.

Al igual que en el mundo real, las transacciones de valor en redes públicas sólo podrán realizarse si dentro de ellas hay agentes especiales, entidades digitales que ofrezcan confianza a los demás agentes de la red. Estas entidades se denominan, en general, Terceras Partes Confiables que pueden ser organizaciones o instituciones de carácter público o privado tales como Servicios Nacionales de Correos, Instituciones Bancarias, etc.

Tener confianza en algo es "la actitud hacía alguién en quién se confía o se espera que haga cierta cosa necesaria para su tranquilidad"[11]. La criptografía, por sí misma, no proporciona ese nivel de "tranquilidad" deseado, por lo que es necesario recurrir a otras herramientas que utilizan criptografía como lo es la firma digital realizada por terceras partes confiables o Autoridades de Certificación, para disponer realmente de ese nivel de confianza digital.

El presente trabajo muestra mediante el uso de técnicas criptográficas, la firma digital,

y la participación de Autoridades de Certificación como proveedores de la confianza digital, es posible transportar a las redes públicas del tipo Internet la emisión de certificados diversos como los de: identidad de los usuarios, de hechos que constan en los expedientes de las administraciones públicas o privadas, la documentación notarial, de la identificación de las partes en el comercio electrónico, etc.

El siguiente trabajo está organizado en 6 capítulos:

- El primer capítulo es una intoducción, aca se explica el por qué es importante plantear el concepto de identidad digital; también se plantean los objetivos y metodologia del trabajo.
- El segundo capítulo define los conceptos de seguridad informática, se estudia los principios involucrados en las técnicas criptográficas basadas en simetría y claves públicas/privadas, se intoducen los conceptos de firma digital y certificados y además se definen los componentes que conforman una infraestructura de clave pública y los distintos modelos de confianza que existen dentro de una infraestructura de clave pública.
- En el tercer capítulo se utilizan herramientas UML (diagramas de casos de uso, de actividades y de despliegue) para el modelado de la autoridad de certificación raíz.
- En el cuarto capítulo se describe los componentes de software y hardware necesarios para llevar a cabo la configuración de una autoridad de certifiación raíz.
- En el quinto capítulo se utiliza ROOTVE para la configuración de la autoridad de certificación raíz, se realiza un experimento el cual consiste en emitir un certificado a un proveedor de servicios de certificación.
- Por último se dan conclusiones y recomendaciones.

En este trabajo, fueron planteados los siguientes objetivos: un objetivo general que es el motor del trabajo y un conjunto de objetivos específicos que permiten que el objetivo general se lleve a cabo.

1.1. Objetivos

1.1.1. Objetivo General

Desarrollar un modelo de Autoridad de Certificación Raíz encargada de firmar, renovar y revocar todos los certificados digitales , utilizando software libre.

1.1.2. Objetivos Específicos

- Seleccionar un modelo de confianza para una Infraestructura de Clave Pública.
- Definir un modelo de autoridad de certificación digital raíz utilizando herramientas UML.
- Configurar un prototipo en relación con el modelo de AC raíz para la integración entre los componentes políticas, software y hardware.

1.2. Metodología

1. Búsqueda de información, material bibliográfico y estudio de conceptos básicos.
2. Desarrollo de un marco teórico.
3. Selección y descripción del software y hardware a utilizar.
4. Desarrollo del modelo de AC raíz.
5. Configuración de una aplicación para gestión de una AC raíz, bajo los principios de software libre.

Capítulo 2

Modelo de seguridad informática

Las transacciones que se efectúan en la vida real entre las personas físicas o jurídicas precisan de un grado elevado de confianza mutua, para que éstas se puedan llevar a buen término. Ciertas actividades humanas tan simples como la negociación de contratos, la votación, la distribución de información e incluso actividades tan lúdicas como jugar a las cartas, requieren altos niveles de confianza entre las partes y, por ello, en muchas ocasiones llevan a exigir la presencia de uno o varios testigos necesariamente imparciales para asegurar la corrección y validez de la transacción.

Las transacciones cotidianas precisan de terceras personas confiables, cuando las partes mutuamente no confían entre sí, circunstancia mucho más extendida de lo que parece querer reconocerse públicamente y que, desde luego, es función creciente con el valor o riesgo que conlleva la transacción. Por ello, continuamente se recurre a la participación de testigos particulares o al notario público en la celebración de contratos, con el fin de obtener actas sobre los hechos que les interesa resaltar a los contratantes, tales como: términos y cláusulas del contrato, autenticidad de la documentación presentada, identificación de las partes, fecha, lugar y hora en la que se firma el contrato, etc. En estos casos, tanto el notario público como los testigos particulares actúan como proveedores de confianza a las partes, ya que en el caso de que surjan conflictos o incumplimientos, aquellos serán requeridos por el demandante para que den fe de los términos y detalles que constituyeron

el contrato o su firma.

En el mundo económico las instituciones financieras, a través de sus informes de estados de cuentas o comportamiento financiero de una determinada entidad, persiguen aportar un alto grado de confianza pública en las transacciones comerciales realizadas por ellos, hasta el punto de que, sin esa información y/o su participación, no es posible realizar la transacción. En estos escenarios, incluso se considera la identidad de la otra parte contratante de carácter secundario, ya que lo fundamental es el aval que aporta la institución financiera con su solvencia.

Tal y como avanzan las tecnologías cada día es más frecuente encontrarnos con portales que nos ofrecen productos y servicios a través de la Red. Y poco a poco, los usuarios empezamos a dar uso a este tipo de servicios, aunque todavía nos sentimos resistentes a revelar nuestros datos privados y bancarios así como así. Esto puede deberse a que la seguridad en unos casos no existe y en otros no se conoce el grado de fiabilidad.

La seguridad, hasta ahora, nunca ha sido uno de los principales aspectos a la hora de tener en cuenta el desarrollo y la evolución de Internet. Parece que este tema tiende a cambiar, y que la seguridad enfocada al comercio electrónico busca la seguridad de los datos de sus usuarios. La incorporación de mecanismos, técnicas y algoritmos adecuados para realizar transacciones electrónicas se hace necesario para evitar los riesgos a los que nos exponemos.

En este sentido, se ha llegado a un consenso sobre lo que significa seguridad, y esta dada por tres conceptos:

Disponibilidad

Se entiende por disponibilidad el grado en que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado, un sistema seguro debe mantener la información disponible para los usuarios. Disponibilidad significa que el sistema, tanto

hardware como software, se mantienen funcionando eficientemente y que es capaz de recuperarse rápidamente en caso de fallo.

Confidencialidad

Es el aspecto de la seguridad que permite mantener en secreto la información y solo los usuarios autorizados pueden manipularla. Igual que antes, los usuarios pueden ser personas, procesos, programas, entre otros

Para evitar que nadie no autorizado pueda tener acceso a la información transferida y que recorre la Red se utilizan técnicas de cifrado o codificación de datos. Hay que mantener una cierta coherencia para determinar cuál es el grado de confidencialidad de la información que se está manejando, para así evitar un esfuerzo suplementario a la hora de decodificar una información previamente codificada.

Integridad

La integridad de la información corresponde a lograr que la información transmitida entre dos entidades no sea modificada por un tercero y un mecanismo para lograrlo es la utilización de firmas digitales.

Mediante una firma digital se codifican los mensajes a transferir, de forma que una función, denominada hash, calcula un resumen de dicho mensaje y se añade a este. La validación de la integridad del mensaje se realiza aplicandole al original la misma función y comparando el resultado con el resumen que se añadió al final cuando se calculo por primera vez antes de enviarlo.

Mantener la integridad es importante para verificar que en el tiempo de viaje por la Red de la información entre el sitio emisor y receptor ningún agente externo o extraño ha modificado el mensaje.

Otros conceptos relacionados con seguridad

Los servicios de **no-repudio** ofrecen una prueba al emisor de que la información fue entregada y una prueba al receptor del origen de la información recibida. Con este aspecto conseguimos que una vez que alguien ha mandado un mensaje no pueda renegar de él, es decir, no pueda negar que es el autor del mensaje.

Es necesario identificar la información que debe conocer cada una de las entidades participantes en el proceso de comercio electrónico y con ello permitir la privacidad de forma fraccionada a las partes autorizadas para su uso.

Conocer y aplicar conceptos, técnicas y algoritmos para implementar un sistema de seguridad es imprecindible para minimizar riesgos y así poder asegurar al usuario que el comercio electrónico es un mecanismo seguro en el cuál puede confiar siempre que se trate con la delicadeza que requiere.

Un último aspecto de seguridad que también podría ser mencionado y no ser dejado por fuera se refiere a la **autenticación**, proceso que consiste en verificar formalmente la identidad de las entidades participantes en una comunicación o intercambio de información. Por entidad se entiende tanto personas, como procesos o sistemas o máquinas. Existen varias formas de autenticarse: basada en claves, en criptografía, entre otras.

De estos dos niveles de autenticación la más segura es la segunda, ya que en el caso de la primera es posible que alguien intercepte la información enviada y pueda suplantar la identidad del emisor de información.

Desde otro punto de vista se puede hablar de formas de autenticarse, como puede ser a través de la biometría (huellas digitales, retina del ojo, la voz...), algo que se sabe (por medio de contraseñas o claves), y por último utilizando algo que se posee (un certificado digital).

La herramienta para implementar estos conceptos de seguridad es la criptografía. A continuación se define el concepto de criptografía y los 2 tipos de criptografía que existen.

2.1. Criptografía

La criptografia [4] es la ciencia de aplicar técnicas complejas sobre un documento con el fin de aumentar y resguardar la seguridad de las transacciones electrónicas. Existen dos tipos de criptografía:

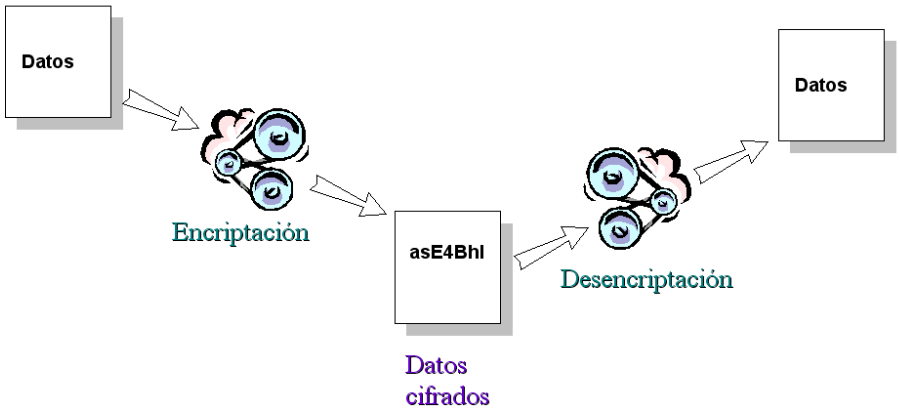

Figura 2.1: Criptografía

2.1.1. Criptografía simétrica:

Los sistemas de criptografía simétrica son aquellos que utilizan la misma clave para cifrar y descifrar un documento. Este tipo de sistema tiene un problema de seguridad y reside en el intercambio de claves entre el emisor y el receptor ya que ambos deben usar la misma clave. Para evitar este problema ambas partes deben formalizar una cita para

el intercambio de claves.

Características de la criptografía simétrica

Estas son algunas de las características de la criptografía simétrica [4]:

- Se utiliza la misma clave para cifrar y descifrar.
- El cifrado simétrico es rápido.
- La criptografía simétrica no se ajusta a las firmas digitales.

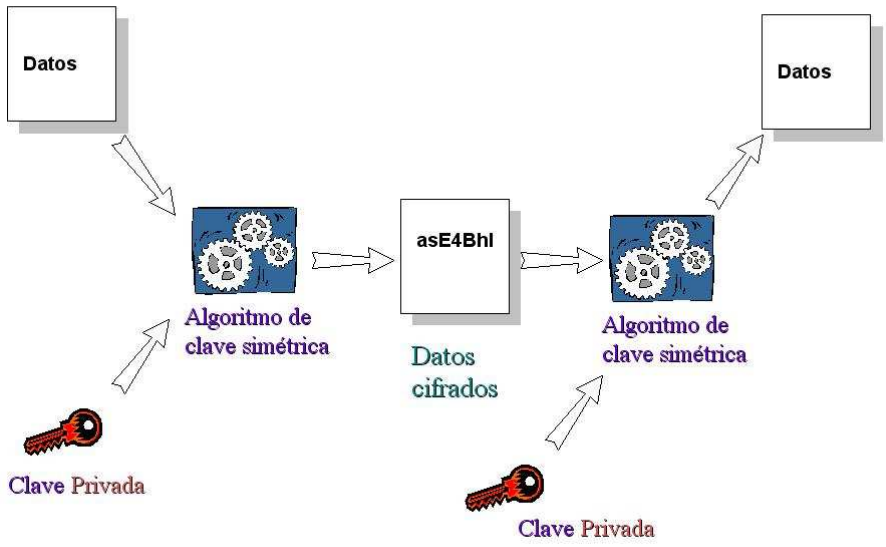

Figura 2.2: Criptografía simétrica

2.1.2. Criptografía asimétrica:

Tambien llamado sistema de cifrado de clave pública, usa dos claves diferentes. Una es la clave pública la cual puede ser enviada a culaquier persona y otra que se llama clave

privada que debe guardarse para que nadie tenga accceso a ella. A diferencia del sistema de cifrado simétrico donde ambas partes deben cuadrar una cita para el intercambio de claves, en este tipo de sistema el remitente usa la clave pública del destinatario para cifrar el documento. Una vez que el documento o mensaje ha sido cifrado solamente con la clave privada del destinatario el mensaje puede ser descifrado. Es por eso que la clave plública puede darse a conocer.

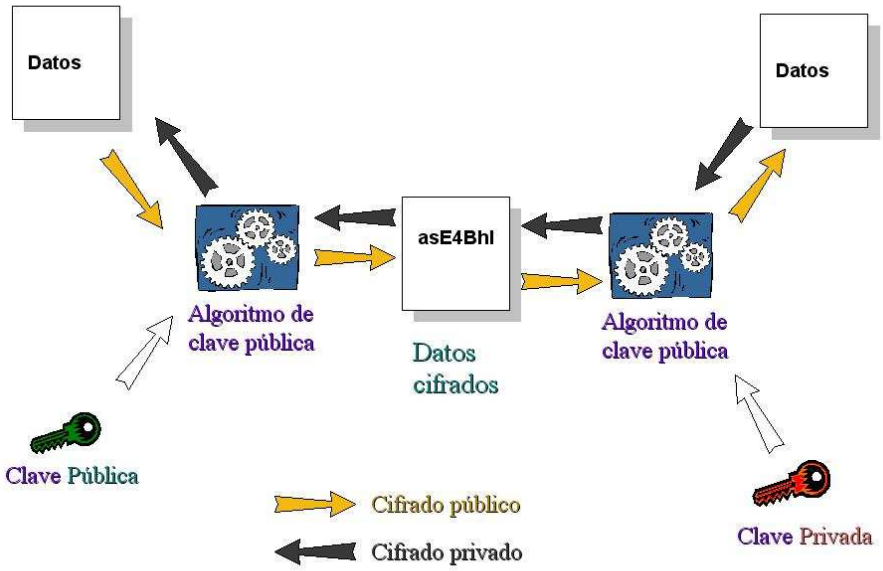

Figura 2.3: Criptografía asimétrica

Características de la criptografía asimétrica

Estas son algunas de las características de la criptografía asimétrica [4]:

- Con la criptografía asimétrica que está cifrada con una clave (pública o privada) sólo se puede descifrar con la otra clave (privada o pública).
- El cifrado asimétrico es seguro.
- Dado que usted no necesita enviar una clave al receptor, la codificación asimétrica no sufre por la intercepción de claves.

- La criptografía asimétrica soporta firmas digitales.

Una técnica que se usa para comprobar que no se ha adulterado un mensaje, usando la criptografía pública es la firma digital y certificados digitales, los cuales se explican con detalle en los siguientes párrafos.

2.2. Firma digital

Una firma digital es un conjunto de datos asociados a un mensaje que permite asegurar la identidad del firmante y la integridad del mensaje. Ver figura 2.4 [4]

Para firmar un documento digital, su autor utiliza su clave secreta, lo que impide que pueda después negar su autoría. La validez de dicha firma podrá ser comprobada por cualquier persona que disponga de la clave pública del autor.

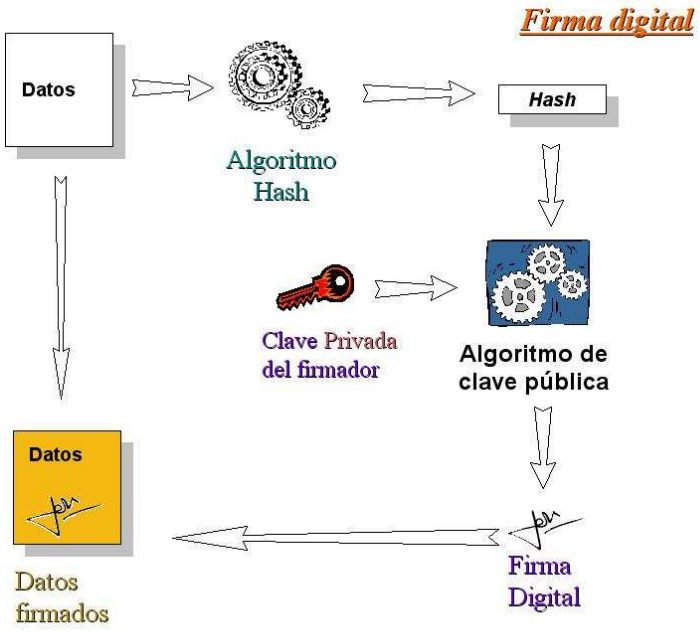

Figura 2.4: Firma digital

Proceso de creación de la firma digital:

1. El software del firmante aplica un algoritmo hash sobre el texto a firmar obteniendo un extracto de longitud fija, y absolutamente específico para ese mensaje. Este algoritmo matemático es unidireccional, es decir, lo encriptado no se puede desencriptar. Un mínimo cambio en el mensaje produciría un extracto completamente diferente. Uno de los algoritmos hash más utilizados para esta función son el MD5, SHA-1 ó SHA:256.

2. El extracto conseguido, cuya longitud oscila entre 128 y 160 bits, en función del algoritmo hash empleado, se somete a continuación a cifrado mediante la clave secreta del autor. El algoritmo más utilizado en este procedimiento de encriptación pública es el RSA. Se obtiene un extracto final cifrado con la clave privada del autor el cual se añadirá al final del texto o mensaje para que se pueda verificar la autoría e integridad del documento por la persona interesada que tenga la clave pública del autor.

3. El software del receptor, con la clave pública del remitente, descifraría el extracto cifrado del autor; a continuación calcula el extracto hash que le correspondería al texto del mensaje, y si el resultado coincide con el extracto anteriormente descifrado se consideraría válida.

Diferencias entre las firmas digitales y las autógrafas:

1. Las firmas autógrafas de una persona son las mismas independientemente del documento que está autentificado. Por el contrario las firmas digitales, deben ser diferentes en función de cada mensaje firmado.

2. Las firmas vienen acompañando un texto en un documento. Estas firmas al ser visibles pueden ser copiadas. Sin embargo las firmas digitales deben ser únicas.

2.3. Certificados digitales

Un certificado digital es un documento de acreditación que permite a las partes tener confianza en las transacciones en internet. Por tanto garantiza la identidad de su poseedor en internet mediante un sistema de claves administrado por una tercera parte de confianza.

Para validar un certificado basta con conocer la clave pública de la tercera parte conocida como la Autoridad de Confianza (A.C). Para cuidarnos de que piratas informáticos cambien su clave pública por la de la autoridad de confianza , la AC debe crear un certificado con su propia información de identidad y a la vez su clave pública y firmar el certificado, este certificado se le conoce como certificado autofirmado.

Dado que los certificados son información pública y lo que se desea es que todos tengan acceso a ellos, pueden hacerse copias del certificado de acuerdo sea necesario.

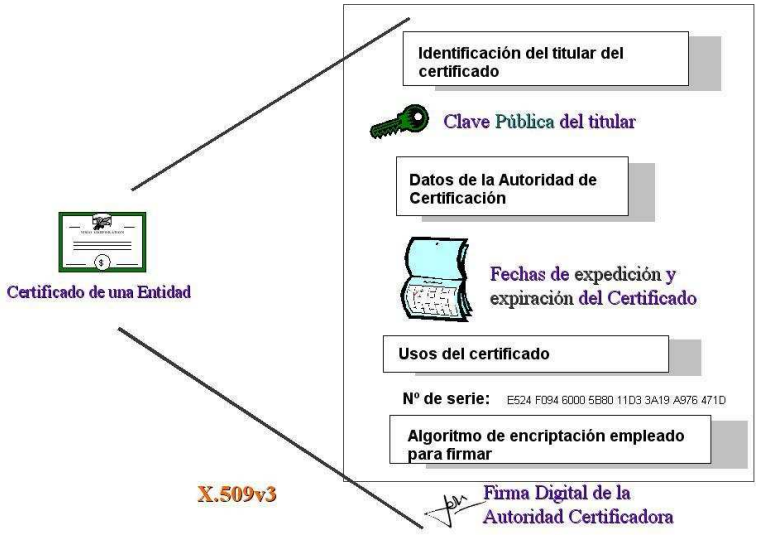

Figura 2.5: Certificado digital X.509

2.3.1. Usos del certificado digital

- Los usuarios pueden añadir firmas electrónicas a los formularios en línea.

- Los destinatarios pueden comprobar la autenticidad del correo electrónico confidencial.
- Los compradores pueden estar seguros de que un website es legítimo.
- Controla el acceso a bancos y comercios online, así como los intranets y extranets.

2.3.2. Contenido de un certificado digital bajo estándar X.509

El estándar internacionalmente aceptado para certificados electrónicos, es el denominado X.509 de la CCITT (*Consultative Committee for International Telephony and Telegraphy*). X.509 especifica, entre otras cosas, formatos estándar para certificados de claves públicas y un algoritmo de validación de ruta de certificación.

X.509 [23] es la pieza central de la infraestructura ICP, y es la estructura de datos que enlaza la clave pública con los datos que permiten identificar al titular. Su sintaxis, se define empleando el lenguaje ASN.1 (*Abstract Syntax Notation One*), y los formatos de codificación más comunes son DER (*Distinguish Encoding Rules*) o PEM (*Privacy Enhanced Mail*). La información que contienen los certificados incluyen lo siguiente:

- **Sujeto:** los nombres y apellidos del individuo o entidad que se van a identificar con el certificado.
- **Clave pública:** correspondiente a la clave privada del sujeto.
- **Expedidor AC:** identifica la fuente de confianza que generó y firmó el certificado.
- **Número de serie:** identifica univocamnete a cada certificado emitido por la AC.
- **Válido desde:** especifica el tiempo desde cuando el certificado puede ser usado.
- **Válido hasta:** especifica hasta que fecha puede ser utilizado el certificado.
- **Uso de Certificado:** describe los usos válidos para la pareja de claves pública/privada.

- **Firma digital:** la firma de la AC, que se generó usando su clave privada,verifica la identidad del sujeto.

2.3.3. Procedimiento general para la obtención de un certificado digital

Figura 2.6: Obtención del certificado digital X.509

1. El usuario debe dirigirse a una oficina de registro.

2. La oficina de registro se encargará de recibir su solicitud y verificar los datos proporcionados por el usuario, si los datos correspondientes al usuario son válidos, la solicitud es enviada a la AC.

3. La AC crea el certificado, lo firma y lo publica en el directorio repositorio.

2.4. Hardware criptográfico HSM

Siglas de "*Hardware Security Module*"(Módulo de Seguridad Hardware).

Un HSM es un dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas y suele aportar aceleración hardware para operaciones criptográficas. Estos dispositivos pueden tener conectividad SCSI / IP u otras y aportar funcionalidad criptográfica de clave pública (ICP) de alto rendimiento que se efectúa dendro del propio hardware [20].

Los más utilizados son: Luna3, nShield y nCipher.

2.5. Tarjeta Inteligente

Es una tarjeta convencional de plástico, que incorpora un chip en su interior. Este chip está formado por un microprocesador, una memoria de programa y una memoria de trabajo estructurada de forma lógica en varias zonas. Opcionalmente puede contener un criptoprocesador el cual permite realizar operaciones criptográficas dentro de la tarjeta inteligente como pueden ser generación de claves RSA, firma digital, cifrado simétrico y/o asimétrico, resumen digital (hash), generación de números aleatorios etc. Las más usadas son: C3po y Gemplus [21].

2.6. Token criptográfico

Dispositivo físico necesario para la autenticación, el cual generalmente permite realizar labores criptográficas (Porta llaves, certificados, cifra, descifra...)[22].

2.7. Infraestructura de Clave Pública (ICP)

ICP es una combinación de hardware y software, políticas y procedimientos que permiten asegurar la identidad de los participantes en un intercambio de datos usando criptografía pública.

Una ICP debe proporcionar los tres conceptos de seguridad mencionados al principio del cápitulo.

Componentes de la Infraestructura de Claves Públicas

Los componentes que conforman la infraestructura de claves públicas son los siguientes:

- Autoridad de Registro (AR).
- Autoridad de Certificación (AC).
- Interfaz con los clientes (PUB).

Autoridad de Registro (AR)

La AR es la responsable del registro y la autenticación inicial de los usuarios a quienes se les expide un certificado después de que se les ha sido aprobada una solicitud de registro.

Autoridad de Certificación (AC)

La AC es la encargada de firmar y revocar todos los certificados digitales. La AC da validez a los certificados mediante la firma digital de éstos con su clave privada.

Interfaz con los clientes (PUB)

La interfaz consiste en un portal web que contiene información del certificado que se expide, de la autoridad certificadora y de sus proveedores de servicios de certificación.

2.8. Funciones de los componentes de la Infraestructura de Clave Pública

Toda infraestructura de clave pública debe contar con funciones o políticas que dirijan el buen curso de dicho sistema.[4]

2.8.1. Autoridad certificadora raíz

La AC raíz tiene el propósito de garantizar en forma segura el uso de las diferentes aplicaciones informáticas a las entidades a las cuales prestara servicios.

La AC raíz emite, firma y administra certificados de llave pública. Esta AC emite certificados para la implementación de otras autoridades de certificación subordinados a él, como cabeza de la jerarquía y núcleo de confianza de los certificados digitales de la infraestructura.

2.8.2. Repositorio

La AC raíz utilizará como repositorio principal sitios Web accesibles desde Internet. Estos sitios tendran publicados la lista de certificados revocados (LCR).

2.8.3. Suscriptores

Los suscriptores utilizan claves privadas emitidas o certificadas por la AC raíz para aplicaciones aprobadas. Los suscriptores de este AC será solamente otras AC que entrarán

a la jerarquía como autoridades de confianza subordinadas de segundo nivel.

Los suscriptores podrán hacer uso del certificado emitido por la AC raíz únicamente para emitir certificados para AC subordinados, los cuales estarán ubicados en un tercer nivel dentro de la jerarquía.

2.8.4. Partes confiantes

Una parte confiante puede ser una AC subordinada a esta AC raíz, o cualquier otro usuario que haya recibido un certificado emitido por una AC que está encadenada de una u otra forma a esta AC raíz.

2.8.5. Notificación de la emisión y revocación de certificados

Luego de su creación, el certificado de la AC suscriptor subordinado será publicado en el directorio X.509. Cuando un certificado sea revocado, éste será incluido en la lista de certificados revocados (LCR) que será también publicada en directorio X.509.

2.8.6. Revocación de un certificado

Los certificados emitidos serán revocados por cualquier razón. Esto incluye a los certificados emitidos para AC subordinadas. Razones para perder la confianza en los certificados incluyen, pero no están limitadas a:

1. Compromiso o sospecha de compromiso de la clave privada y de los usuarios/contraseñas de la AC.
2. Cambio de rol del suscriptor.
3. Cese de actividades de la AC.

4. Incumplimiento de la AC en las obligaciones estipuladas bajo este documento y cualquier política de certificados.

2.9. Modelos de confianza

Las relaciones de confianza, son necesarias entre múltiples autoridades de certificación para que garantizar que los suscriptores de una ICP no tengan que depender y confiar en una sola AC, algo que haría imposible el manejo de escalabilidad, administración y protección. El objetivo es garantizar que las partes que utilizan identidades creadas por una AC puedan confiar en ellas, aunque dichas partes tengan una autoridad expedidora diferente.

Los modelos de confianza ofrecen un marco de referencia para crear y administrar relaciones de confianza.

2.9.1. Modelo de confianza jerárquico

El objeto de estudio de esta tesis es modelar una AC raíz, para comenzar a modelar se definirá un modelo de confianza jerárquico donde la AC raíz esta diseñada como el ancla de confianza común para todas las entidades destino. Como tal, por definición, es la Autoridad de certificación de más confianza y todas las demás relaciones de confianza salen a partir de ella. Certifica el siguiente conjunto más bajo de AC subordinadas con un conjunto de relaciones de confianza unidireccionales. En este modelo, solamente la AC superior expide certificados a sus subordinadas; las AC subordinadas no certifican a sus superiores.

Como la AC raíz en este modelo es el ancla de confianza única y como las relaciones de confianza se construyen desde la AC de más confianza, no existe otra autoridad de certificación que pueda firmar el certificado de la AC raíz. Como resultado, la AC raíz crea un certificado autofirmado por si mísma. En este caso, el sujeto del certificado y quien lo expide serán el mismo. La clave pública certificada en el certificado corresponde a la

clave privada usada para generar la firma en el certificado. De ese modo la clave pública en el certificado se usará para verificar directamente la firma en el certificado cuando éste se vaya a validar. Ver figura 2.7

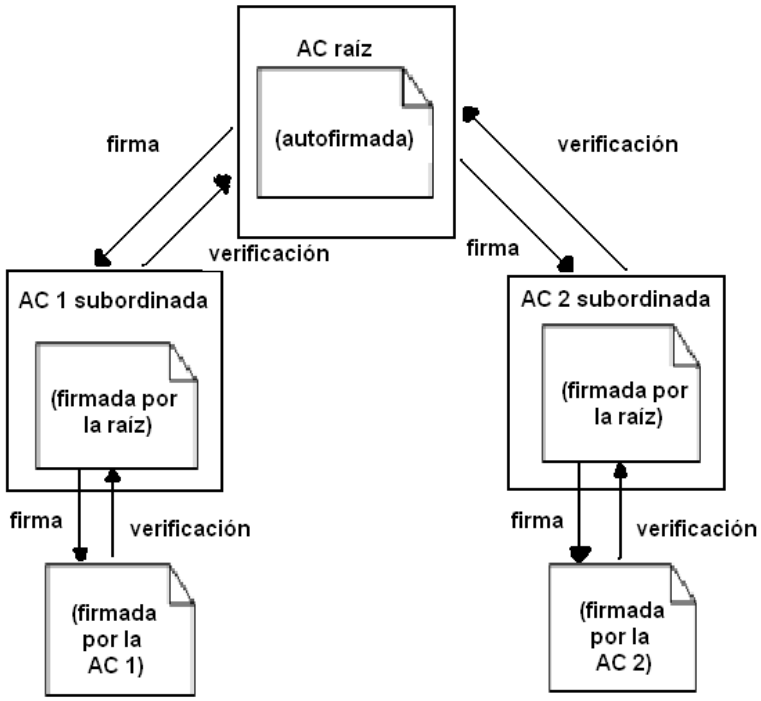

Figura 2.7: Modelo de confianza jerárquico

A continuación se muestran otros modelos de confianza:

2.9.2. Modelo entre iguales

Un modelo de confianza entre iguales asume el establecimiento de la confianza entre dos autoridades de certificación que no se pueden considerar subordinadas entre sí; por el contrario, se consideran iguales. Las dos AC podrían ser parte de una sola empresa o dominio de confianza, pero lo más común es que estén en diferentes empresas o dominios de confianza [4]. Ver figura 2.8

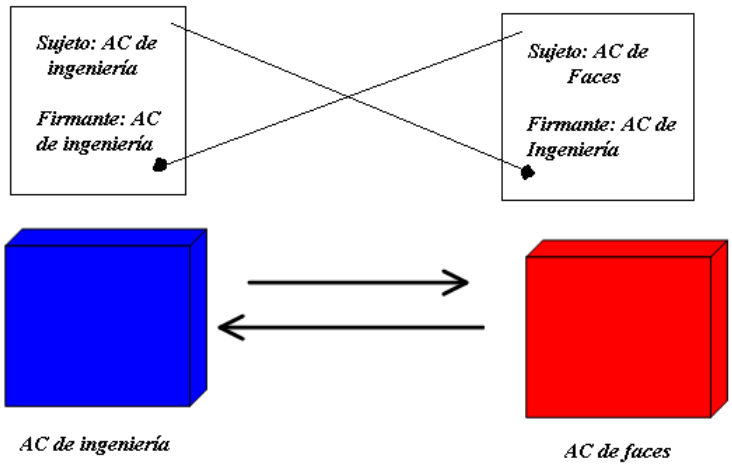

Figura 2.8: Modelo entre iguales

2.9.3. Modelo de mallas

Este modelo permite construir una malla conectada toal o parcialmente, permitiendo mas de dos certificados AC en una ruta de certificación. Se admiten relaciones de confianza bilaterales y cada AC en una ruta ,tiene certificación cruzada con las demás [4]. Ver figura 2.9

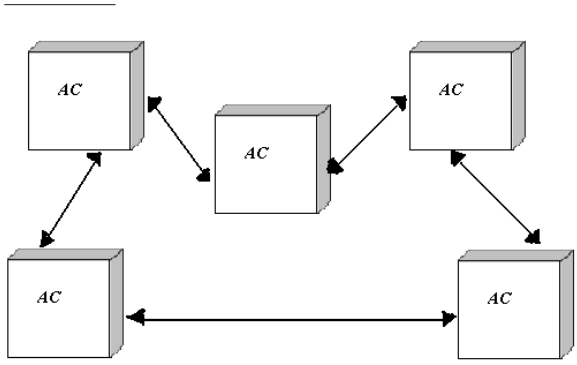

Figura 2.9: Relaciones de confianza bilaterales

2.10. Diagramas UML

UML (*Unified Modeling Language*) es un lenguaje que permite modelar, construir y documentar los elementos que forman un sistema software, por tal motivo se usará para el modelado de los componentes que conforman una estructura de claves públicas (ICP). [1]

Los diagramas UML representan diversas perspectivas de un sistema al cual se le conoce como modelo. Los modelos UML que se usarán para el modelado de la infraestructura son los diagramas de casos de uso, diagramas de actividades y diagramas de despliegue.

2.10.1. Diagramas de casos de uso

Un diagrama de casos de uso [1] muestra la relación entre los actores y los casos de uso del sistema. Representa la funcionalidad que ofrece el sistema en lo que se refiere a su interacción externa. En el diagrama de casos de uso se representa el sistema como una caja rectangular con el nombre en su interior. Los casos de uso están en el interior de la caja del sistema, y los actores fuera, y cada actor está unido a los casos de uso en los que participa mediante una línea.

1.- Elementos: los elementos que conforman los diagramas de casos de uso son: actores, casos de uso y relaciones entre casos de uso. [1]

2.- Actores: un actor es algo con comportamiento, como una persona (identificada por un rol), un sistema informatizado u organización, y que realiza algún tipo de interacción con el sistema, se representa mediante una figura humana. [1]

3.- Casos de uso: un caso de uso es una descripción de la secuencia de interacciones que se producen entre un actor y el sistema, cuando el actor usa el sistema para llevar a cabo una tarea específica, se representan mediante una elipse. [1]

2.10.2. Diagramas de Actividades

Los diagramas de actividades sirven para modelar el flujo de control entre actividades. Estos diagramas contienen: estados de actividad, estados de acción, transiciones y objetos.

1.- Estado de actividades y acción: la representación de ambos es un rectángulo con las puntas redondeadas, en cuyo interior se representa bien una actividad o bien una acción.

2.- Transiciones: las transiciones reflejan el paso de un estado a otro, bien sea de actividad o de acción. Esta transición se produce como resultado de la finalización del estado del que parte el arco dirigido que marca la transición. Como todo flujo de control debe empezar y terminar en algún momento.

3.- Bifurcaciones: un flujo de control no tiene porqué ser siempre secuencial, puede presentar caminos alternativos. Para poder representar dichos caminos alternativos o bifurcación se utilizará como símbolo el rombo. Dicha bifurcación tendrá una transición de entrada y dos o más de salida.

4.- Calles: cuando se modelan flujos de trabajo de organizaciones, es especialmente útil dividir los estados de actividades en grupos, cada grupo tiene un nombre concreto y se denominan calles. Cada calle representa a la parte de la organización responsable de las actividades que aparecen en esa calle.

2.10.3. Diagramas de Despliegue

Un diagrama de despliegue muestra las relaciones físicas entre los componentes hardware y software en el sistema final, es decir, la configuración de los elementos de procesamiento en tiempo de ejecución y los componentes software (procesos y objetos que se ejecutan en ellos)[1].

Capítulo 3

Modelo de la Infraestructura de Clave Pública

En este capítulo se utilizan los diagramas de caso de uso y diagramas de actividades para modelar la ICP.

3.1. Autoridad de Certificación Raíz

El actor en este caso esta representado por una persona llamada Autoridad de Certificación Raíz, la cual debe cumplir con las siguientes tareas o funciones:

- **Emisión de certificados**: una vez que el proveedor de servicios de certificación (PSC) cumple con los requisitos requeridos para la otorgación de los certificados, la AC procede a emitir el certificado digital colocando su firma digital en el certificado. Esta firma hace constar la integridad del proveedor de servicios que presta servicios de certificación a terceros.
- **Revocación de certificados no válidos**: la revocación de certificados se realiza cuando la fecha de validación del certificado a caducado o cuando se descubre algún tipo de irregularidad con la manipulación de la clave del usuario o con el certificado.
- **Renovar certificados**: la autoridad de certificación se encargará de renovar un

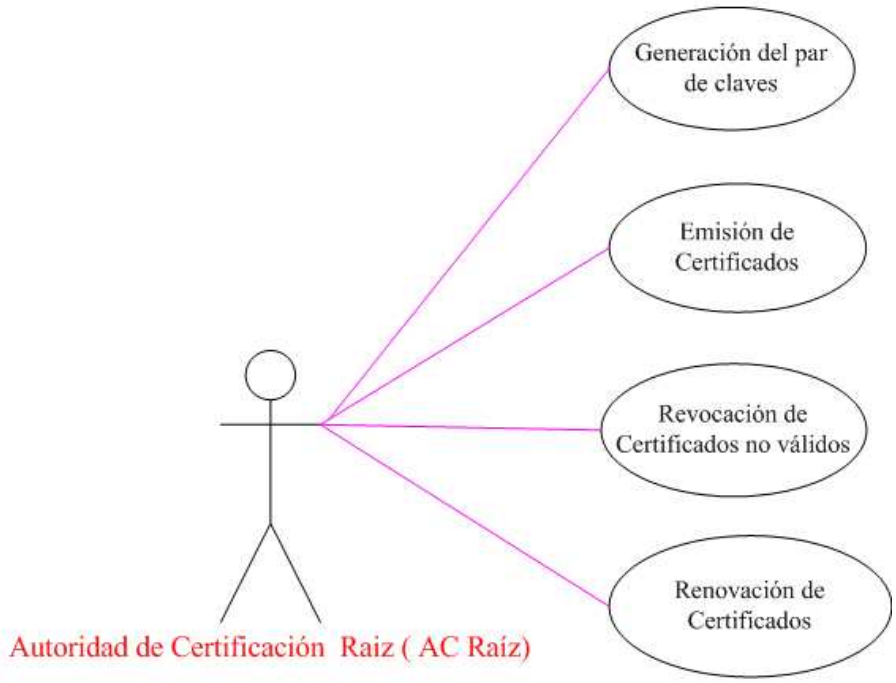

Figura 3.1: Caso de uso de una autoridad de certificación raiz

certificado siempre y cuando el proveedor de servicios de cetrificación (PSC) anticipe que desea renovar su certificado, para ello la autoridad genera un nuevo certificado.

- **Generación del par de claves**: la AC genera su par de clave pública/privada, la clave privada es almacenada en el HSM, solo la AC raíz tiene acceso a la clave privada.

3.1.1. Emisión de certificados

- **Caso de uso: emisión de certificados**

Acción del actor	Respuesta del sistema
1. La autoridad certificadora raíz firma el certificado digital.	2. Se produce un certificado digital.

3. La autoridad certificadora raíz envía el certificado a el administrador PUB.	4. El administrador publica el certificado en el directorio repositorio.

Cuadro 3.1: Emisión de certificados

3.1.2. Renovación de certificado

- **Caso de uso: renovación de certificados**

Acción del actor	**Respuesta del sistema**
1. La AC genera una nueva clave y crea un nuevo certificado.	2. Se crea el certificado con una clave diferente y todos los demás datos.
	3. el certificado está listo para ser usado.

Cuadro 3.2: Renovación de certificados

3.1.3. Revocación de certificados no válidos

- **Caso de uso: revocación de certificados no válidos**

Acción del actor	**Respuesta del sistema**
	1. Una vez que el certificado a caducado, el certificado ya no existe.

	2. El administrador PUB se encarga de publicar el certificado en la lista de certificados revocados LCR.
	3. Si el certificado no es usado con los fines para los que fue solicitado.
4. La autoridad de certificación revoca el certificado.	
5. El certificado revocado es enviado al PUB.	

Cuadro 3.3: Revocación de certificados

3.2. Autoridad de Registro (AR)

El actor representado por la AR también es una persona, los casos de uso de este actor son los siguientes:

- **Recepción de solicitudes**: el proveedor de servicios debe dirigirse a la AR que se encuentra asociada a la AC raíz y hacer la solicitud de que se le sea otorgado un certificado digital.
- **Recepción de recaudos**: una vez que la AR ha autenticado al proveedor, entonces dicha autoridad se encargará de recibir los recaudos exigidos y comprobar que los mismos estan correctos.
- **Envío de la solicitud a la AC:** la AR debe pasar la solicitud realizada por el proveedor de servicios a la AC raíz, en dicha solicitud se anexa la información ya

autenticada del proveedor y a demás debe estar indicado el tipo de uso que se le quiere dar a dicho certificado (para que se necesita el certificado).

3.2.1. Recepción de solicitudes

- **Caso de uso: recepción de solicitudes**

Acción del actor	**Respuesta del sistema**
1. Este caso de uso comienza cuando el PSC llega a la oficina de registro solicitando un certificado.	
2. La AR atiende la solicitud.	
3. La AR da a el proveedor una lista de recaudos.	

3.2.2. Recepción de recaudos

- **Caso de uso: recepción de recaudos**

Acción del actor	**Respuesta del sistema**
1. La Autoridad de Registro recibe los recaudos.	
2. Comprueba que dichos recaudos sean válidos y esten completos.	

Cuadro 3.5: Recepción de recaudos

3.2.3. Entrega de la solicitud a la AC

- **Caso de uso: envío de la solicitud a la AC Raíz**

Acción del actor	Respuesta del sistema
1. La Autoridad de Registro envía la solicitud del certificado a la AC Raíz.	
2. La AC raíz recibe dicha solicitud.	
	3. La solicitud puede ser aceptada, o rechazada.

Cuadro 3.6: Envío de la solicitud a la AR

3.3. Proveedor de Servicios de Certificación

El actor esta dado por el proveedor de servicios de certificación, el cual representa una empresa u organización. Ver figura 3.3

- **Solicitar certificado firmado por la AC raíz**: el proveedor de servicios debe dirigirse a la AR que se encuentra asociada a la AC raíz y hacer la solicitud de que se le sea otorgado un certificado digital.
- **Consignar los recaudos exigidos por la AC raíz**: una vez que la AR ha autenticado al proveedor, entonces dicha autoridad se encargará de recibir los recaudos exigidos y comprobar que los mismos estan correctos.

- **Recibir aprobación o rechazo de la AR**: cuando se han entregado los recaudos la autoridad de registro debe informar al proveedor si su solicitud ha sido aceptada o simplemente negada.
- **Recibir certificado firmado por la AC raíz**: si la solicitud del certificado ha sido aprobada, entonces el certificado es colocado en un directorio repositorio donde se tiene acceso a él vía internet.

3.3.1. Solicitar certificado firmado por la AC raíz

- **caso de uso: solicitar certificado firmado por la AC raíz**

Acción del actor	Respuesta del sistema
1. El PSC se dirige a la AR asociada a la AC raíz y pide solicitud del certificado.	2. La AR recibe solicitud.

Cuadro 3.7: Solicitud de certificado firmado por la AC raíz

3.3.2. Consignar recaudos exigidos por la AC raíz

- **caso de uso: consignar recaudos exigidos por la AC raíz**

Acción del actor	Respuesta del sistema
1. El PSC consigna los recaudos.	2. La AR recibe los recaudos, los revisa y luego los acepta o rechaza.

Cuadro 3.8: Consignar recaudos exigidos por la AC raíz

3.3.3. Recibir aprobación o rechazo de la AR

- **caso de uso: recibir aprobación o rechazo de la AR**

Acción del actor	Respuesta del sistema
	1. La AR informa al PSC si su solicitud de certificado fue aprobada o negada.

Cuadro 3.9: Recibir aprobación o rechazo de la AR

3.3.4. Recibir certificado firmado por la AC raíz

- **caso de uso:recibir certificado firmado por la AC raíz**

Acción del actor	Respuesta del sistema
	1. El certificado está disponible en un directorio repositorio.

Cuadro 3.10: Recibir certificado firmado por la AC raíz

3.3.5. Administrador Portal web (PUB)

El administrador de la infraestructura será un portal Web donde se encuentra el directorio repositorio de certificados emitidos y revocados por la autoridad de certificación raíz, a parte el portal brinda información sobre la casa certificadora. Ver figura 3.4

3.3.6. Publicación de certificados en el directorio repositorio

- **caso de uso: publicar certificados en el directorio repositorio**

Acción del actor	Respuesta del sistema
1. El administrador coloca los certificados válidos y no válidos en el directorio repositorio.	2. El portal Web muestra la lista de certificados.

Cuadro 3.11: Publicación de certificados en el directorio repositorio

3.4. Diagrama de Actividades para generar un certificado de un PSC

En la figura 3.5 se puede ver el diagrama de actividades para generar un certificado de PSC.

El PSC genera el par de clave pública y privada, seguidamente puede hacer solicitud del certificado a la AR, la AR recibe los recaudos y los debe inspeccionar antes de enviar la solicitud del certificado a la AC raíz, si los recaudos están completos entonces la AR enviará la solicitud a la AC raíz, en caso contrario la AR debe notificar al Proveedor que su solicitud ha sido negada. La AC raíz firma el certificado y ésta lo envía al administrador PUB el cual pública la lista de certificados. Ver figura 3.5

Este capítulo mostró a través de los casos de uso y diagrama de actividades el modelado de las gestiones que debe realizar cada uno de los componentes que intregan una

infraestructura de clave públicas, a través del modelado se puede observar que cada autoridad tiene roles distintos dentro de la infraestructura, se describen sus roles: ¿ quién es el actor? y las acciones o funciones que debe cumplir ese actor; permite extraer los requerimientos de software y hardware necesarios para una ICP.

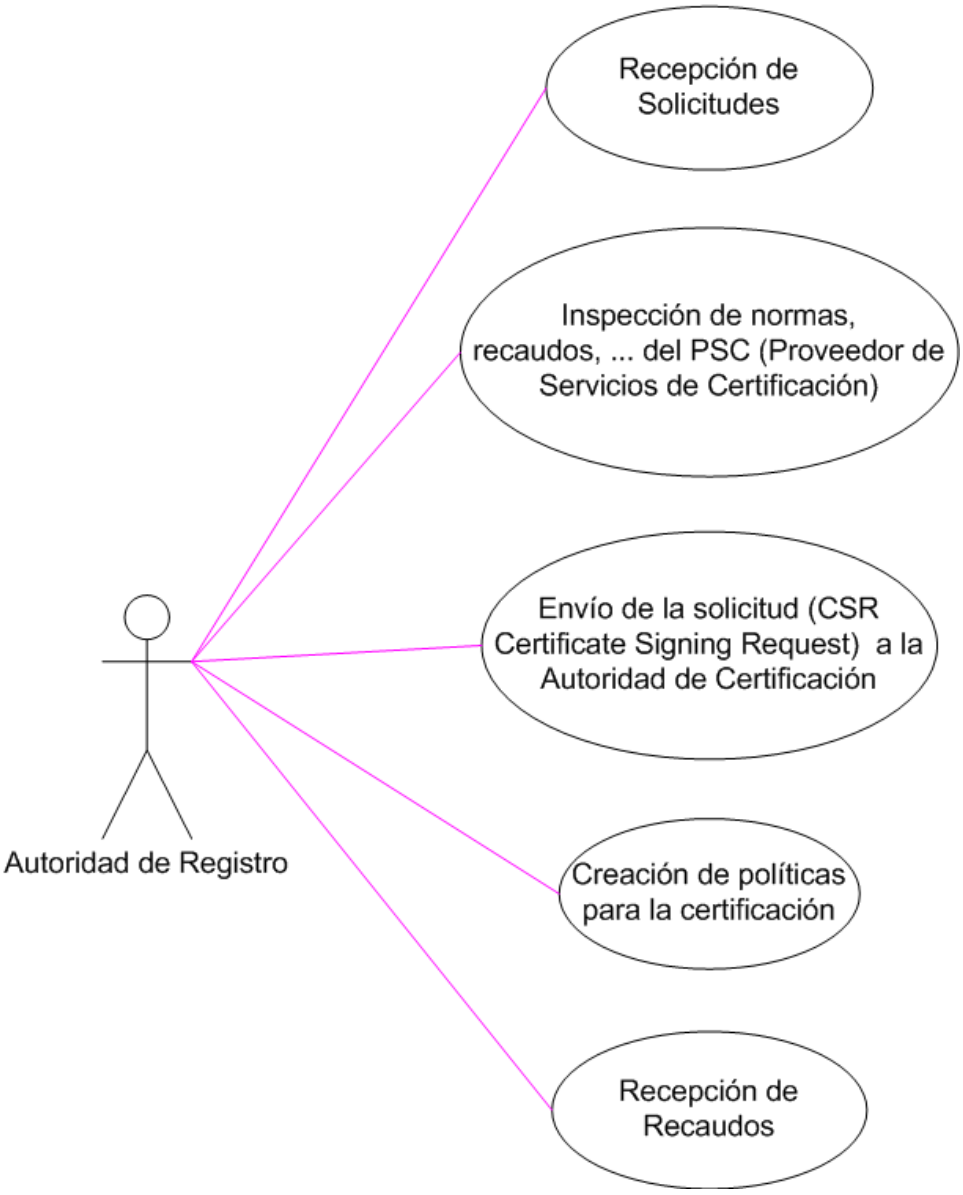

Figura 3.2: Caso de uso de una autoriddad de registro

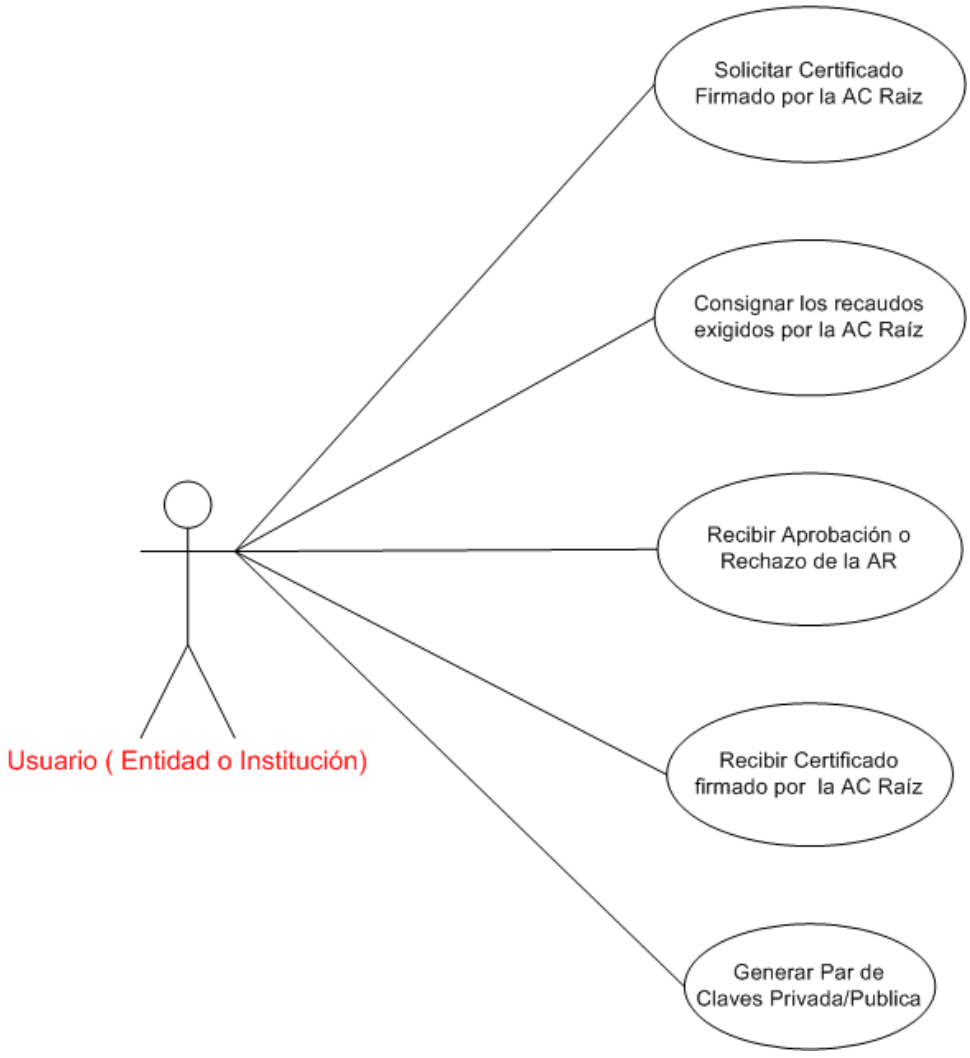

Figura 3.3: Caso de uso de un proveedor de servicios de certificación

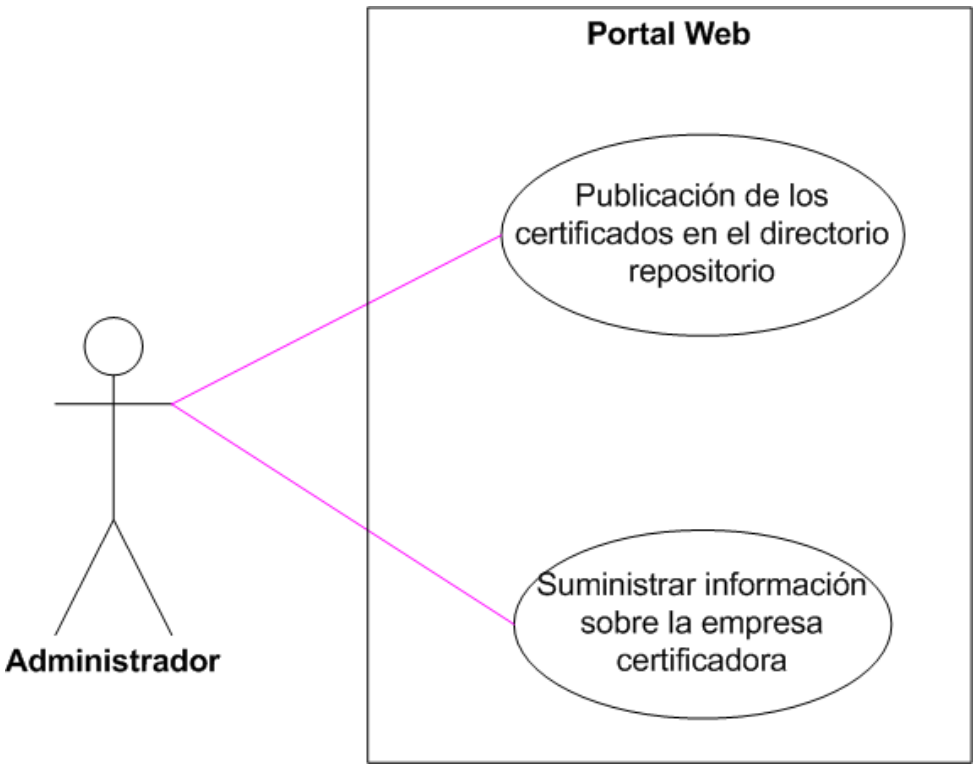

Figura 3.4: Caso de uso de un administrador PUB

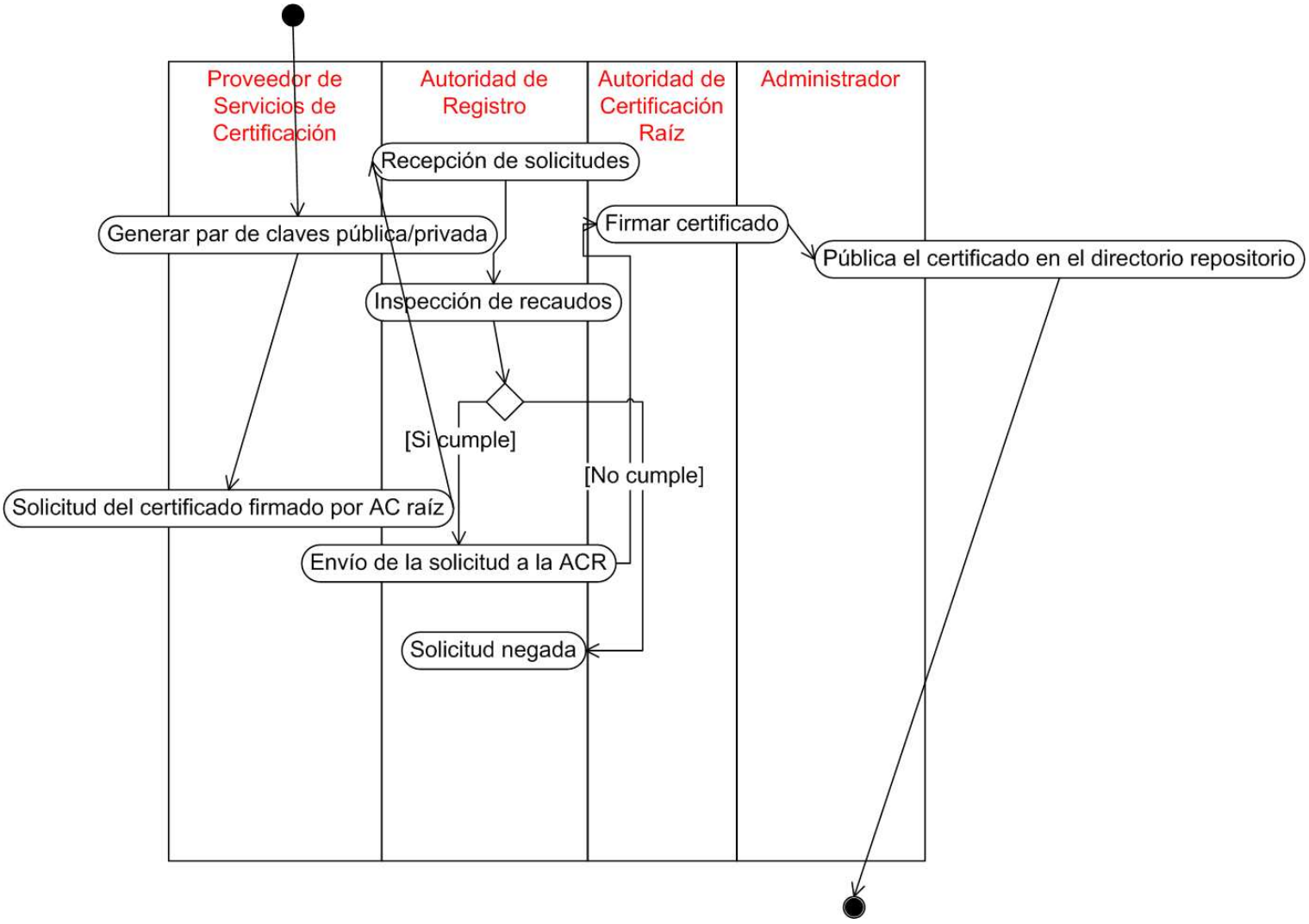

Figura 3.5: Diagrama de actividades

Capítulo 4

Requisitos de Software y Hardware

En este capítulo se describe los componentes de software y hardware necesarios para llevar a cabo la gestiones de una autoridad de certificación raíz. Esta lista comprenderá:

1. Software.
   1.1 Sistema operativo.
   1.2 Aplicaciones y bibliotecas.
2. Hardware.
   2.1 Hardware de seguridad.
   2.2 Hardware utilitario.

4.1. Sistema operativo

La alplicación utilizada para la gestion de una autoridad de certificación raíz está desarrollada en software libre, la distribución utilizada fue Debian Sarge versión estable. http://www.debian.org

4.2. Requisitos de software

Los requisitos de software se traducen en una lista de aplicaciones necesarias para instalar el software de gestión de una AC raíz bajo Linux, el software recibe el nombre de

ROOTVE (Autoridad de Certificación Raíz). La lista de aplicaciones es la siguiente:

- **OpenSC-Ceres**

  OpenSC es una aplicación estandarizada de gestión de acceso a dispositivos de tipo tarjeta inteligente. Funcionalidades básicas, como SELECT FILE, READ BINARY, etc deberían funcionar en cualquier tarjeta compatible con el estandard ISO-7816-4 para tarjetas inteligentes. Operaciones adicionales, como (des)cifrado, generación de claves, etc, son también soportadas en aquellas tarjetas compatibles con el protocolo PKCS#15.[12]

  Adicionalmente OpenSC proporciona las siguientes funcionalidades:

  - Soporte del estandard PKCS#11, lo que permite la integración con aplicaciones que utilicen funciones de criptografía, como pueden ser navegadores, sistemas de autenticación, sistemas de firma/cifrado electrónico, etc.
  - Diversas aplicaciones de test.
  - Entorno de desarrollo, para poder realizar programas basados en las bibliotecas proporcionadas por OpenSC.

  OpenSC funciona en plataformas Linux, MacOS y Windows.OpenSC es software libre: se distribuye bajo los términos y condiciones de la licencia GNU Lesser Public License (LGPL).

  OpenSC-Ceres es la adaptación del paquete OpenSC para su utilización con las Tarjetas Criptográficas Ceres, proporcionadas por la Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM). [13]

- **Repositorio no relacional** (Berkeley DB libdb versión 4.2)

Es una librería mediante la cual se pude crear bases de datos sin la necesidad de un servidor SQL. Tiene todo lo necesario para poder almacenar datos, borrarlos, navegar por ellos, duplicarlos, etc. [14]

- **Repositorio relacional** (Postgresql versión 7.4)

  PostgreSQL es un motor de base de datos, es servidor de base de datos relacional libre, liberado bajo la licencia BSD. Es una alternativa a otros sistemas de bases de datos de código abierto (como MySQL, Firebird y MaxDB), así como sistemas propietarios como Oracle o DB2. [15]

- **Algoritmos criptográficos** (Crypto++ versión 5.2.1)

  - Librería de clases de primitivas criptográficas.
  - Criptografía de clave pública RSA.
  - Códigos de autenticación de mensajes: MD5-MAC, HMAC, XOR-MAC, CBC-MAC, DMAC.
  - Cifradores basados en funciones hash.
  - Esquemas de secretos compartidos de Shamir y Rabin. [16]

- **Algoritmos estándar criptográficos** (OpenSSL versión 0.9.8)

  El software OpenSSL es un proyecto de software desarrollado con todos los principios de software libre, se ha convertido en un estándar para el desarrollo de aplicaciones de seguridad. Es un robusto juego de herramientas que le ayudan a su sistema a implementar el Secure Sockets Layer (SSL), así como otros protocolos relacionados con la seguridad , tales como el Transport Layer Security (TLS). También incluye una librería de criptografía. Este paquete de software es importante para cualquiera que esté planeando usar cierto nivel de seguridad en su máquina Linux. [17]

- **Qanava libqanava versión 0.0.3**

  Es una librería gráfica para mostrar la jerarquía de la ICP, esta librería premite mostrar el modelo e confianza jerárquico que establece una organización.

- **Interfaz GUI y utilitarios** (Qt3 versión 3.3)

  Es una librería destinada a la construcción de aplicaciones con interfaz gráfica de usuario. Está escrita en lenguaje C++, es totalmente orientada a objetos y facilita a los programadores una serie de clases muy útiles, gracias a las cuales la creación de aplicaciones que funcionen en entornos gráficos es muy simple. [18]

- **ROOTVE** (Raíz Venezolana)

  Es una aplicación desarrollada para crear y administrar certificados X.509 y claves RSA en una Autoridad de Certificación Raíz [8]. Ver apéndice A

- **Servidor HTTP Apache**

  Un servidor web, este término podría referirse a la máquina que almacena y maneja los sitios web. Básicamente, un servidor web sirve contenido estático a un navegador, carga un archivo y lo sirve a través de la red al navegador de un usuario. Este intercambio es mediado por el navegador y el servidor que hablan el uno con el otro mediante HTTP. Se pueden utilizar varias tecnologías en el servidor para aumentar su potencia más allá de su capacidad de entregar páginas HTML; éstas incluyen scripts CGI, seguridad SSL. [19]

4.3. Requisitos de Hardware

4.3.1. Hardware utilitario

- El sotware se instala en una computadora de escritorio que tiene las siguientes especificaciones:

  - Doble núcleo mayor a 2 Ghz.
  - Memoria mayor o igual a 512MB de DDR.
  - Disco duro mayor de 80GB.
  - tarjeta de red.
  - Unidad de CD-RW.
  - Unidad de DVD-ROM.
  - Puertos USB, lector de soportes digital.

  Para poder utilizar la aplicación es necesario e indispensable la utilización de algunos de los dispositivos físicos, estos dispositivos indispensables son: teclado, ratón, monitor y el computador con todos sus requisitos tecnológicos. A nivel de usuario se necesita los mismos componentes físicos con la excepción de que el computador no tiene la necesidad de tener instalados todos los paquetes tecnológicos, basta con solo tener el sistema operativo.

4.3.2. Hardware de seguridad

Una de las principales funcionalidades de la aplicación ROOTVE es el uso de dispositivos criptográficos para el soporte de las operaciones. El uso de estos dispositivos es una práctica común en las aplicaciones de infraestructuras de claves públicas. ROOTVE utiliza 2 tipos de hardware crtiptográfico: HSM módulos de seguridad en hardware y tarjetas inteligentes.

1. **HSM**

   Siglas de "*Hardware Security Module*"(Módulo de Seguridad Hardware).

   El HSM se utiliza para la generación y almacenamiento seguro del par de claves pública/privada de la autoridad de certificación raíz, la firma y revocación de certificados digitales y la generación de listas de revocación de certificados.

   La funcionalidad de un periférico HSM es la generación de datos seguros (asegurados mediante criptografía de clave pública o PKI) para su acceso a lo largo del tiempo pudiendo aportar adicionalmente seguridad física. Los datos custodiados por un HSM suelen ser las claves privadas usadas en PKI, y en algunas ocasiones también permiten la protección de claves simétricas.

   Como se ha mencionado el objetivo de un HSM es el almacenado seguro de certificados PKI, que son los datos sensibles de esta tecnología.

   - La seguridad que proporcionan dichos dispositivos es muy elevada si se siguen ciertas políticas de seguridad.
   - Las claves protegidas por los HSM sólo están "completamente protegidas por hardware"si fueron generadas dentro del propio hardware. (si se generan fuera y se importan, las copias de dichas claves fuera del dispositivo -obviamente- no podrán ser protegidas por el dispositivo HSM).

   HSM nShield especializado para mejorar la seguridad de todo tipo de aplicaciones, desde emisión de certificados PKI y encriptación de bases de datos a sistemas que emplean firmas digitales y comunicaciones por SSL, nShield protege las claves y operaciones criptográficas mediante hardware resistente a las manipulaciones

Figura 4.1: HSM nShield (Hardware criptográfico de la empresa nCipher)

2. **Tarjeta inteligente**

   La tarjeta inteligente tiene métodos de autenticación del usuario, como pueden ser un PIN de usuario o una huella digital según las características de la tarjeta. Todo sin salir la información relativa a la autenticación de la tarjeta, dado que es esta la que recibe esta información e indica si es correcta o no.

   La seguridad de las tarjetas inteligentes se fundamenta en los elementos de seguridad físicos del chip y, los mecanismos del sistema operativo utilizados para cada aplicación concreta, como, las memorias resistentes a campos magnéticos y electromagnéticos, borrado de la memoria por radiación ultravioleta si se intenta abrir un módulo para explorarlo, utilización de bits centinelas que permitirían detectar un uso ilegal, distribución no lineal de la memoria para evitar la exploración de su contenido, consumo aleatorio de corriente independiente de la operación que se esté realizando y del número de bits escritos, etc.

   Uso de una una Tarjeta Inteligente en entornos ICP

   a) Una tarjeta inteligente se puede usar como elemento seguro para almacenar los certificados digitales generados por una AC y sus claves asimétricas asociadas.

b) El uso de este dispositivo permite generar el par de claves RSA , almacenar el certificado digital, generar firmas digitales, y/o el cifrado de datos dentro de la tarjeta inteligente protegiendo el acceso a las operaciones sensibles (por ejemplo que hagan uso de la clave privada) mediante métodos de autenticación, incrementando la seguridad al realizar estos dentro de un dispositivo seguro.

c) El uso de tarjeta inteligente también garantiza la portabilidad de esta información al estar almacenado en esta.

Las tarjetas inteligentes se utilizan como dispositivo que le permite a los usuarios de ROOTVE autenticarse pues en ellas se generan y almacenan pares de claves públicas/privadas.

En la figura 4.2 se muestra un kit básico de sistema de cifrado e identificación digital con tarjeta CERES-FNMT de la Fábrica Nacional de Moneda y Timbre.

Figura 4.2: CryptoKit de la empresa C3po

Características de seguridad

- Autenticación interna Tarjeta-Terminal. Autenticación externa de usuario y de

aplicación.

- Validación de PIN de usuario.
- Servicios de integridad mediante la generación y verificación de firmas digitales RSA.
- Generación de claves RSA en tarjeta.
- Mecanismos de confidencialidad para el intercambio seguro de claves de cifrado.

Operaciones Criptográficas

- Permite el almacenamiento y uso de claves de 1024 bits o 2048 bits.
- Generación y verificación de firmas digitales RSA.
- Cifrado y descifrado RSA.
- Generación de claves RSA.
- Cifrado hash SHA-1, SHA-256, MD5.

Seguridad

- Cifrado dinámico de memoria/buses con diferentes claves.
- Sensores para control de tensión y frecuencia.
- Generador real de números aleatorios.
- Módulo de cálculo de CRCs.

3. 4.3.3. Token USB

Los token criptográficos tienen las siguientes características:

- Las claves no circulan por la red.

- Es necesario robar el token para llevar acabo las acciones para las que ha sido diseñado.
- Llaveros USB que alojan un certificado.
- Se desbloquean de modo análogo.
- PKCS11 u otro standard de acceso a dispositivos criptográficos para su acceso.
- No necesitan lectores, solo un conector USB y un software determinado.

Figura 4.3: Token criptográfico de la empresa C3po

Capítulo 5

Configuración de una AC raíz

Uno de los objetivos de este trabajo es seleccionar el software, entre la lista de software libre que gestionan certificados se encontró:

- **OpenCA:** es una herramienta que proporciona un interface Web para poder administrar una infraestructura de clave pública, diseñada para PSC.
- **PYCA:** presenta caracteríticas limitadas.
- **ROOTVE:** diseñado para la AC raíz, cumple con los principios de software libre y además tiene soporte local.

En este capítulo se muestra como configurar el prototipo de Autoridad de Certificación Ráiz usando el software ROOTVE, cada experimento hará referencia a los casos de uso descritos en el capítulo 3, además se mostrará mediante un diagrama de despliegue los nodos que representan los componentes de una infraestructura de clave pública.

5.1. Diagrama de despliegue

Los diagramas de despliegue muestran la disposición física de los distintos nodos que componen un sistema y el reparto de los componentes sobre dichos nodos. La vista de

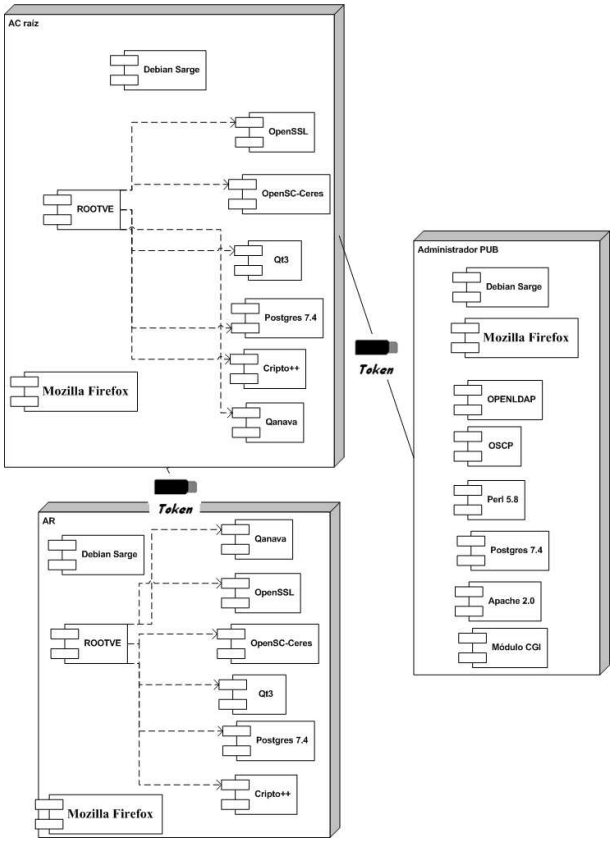

Figura 5.1: Diagrama de despliegue

despliegue representa la disposición de las instancias de componentes de ejecución en instacias de nodos conectados por enlaces de comunicación. Un nodo es un recurso de ejecución tal como un computador, un dispositivo o memoria. El diagrama de despliegue que se ve a continuación, sitúa el software(aplicaciones y sistema operativo) en el hardware que lo contiene. Ver figura 5.1

5.2. Configuración y uso de ROOTVE

Esta aplicación muestra cada uno de los módulos a la cual puede acceder la Autoridad de Certificación Raíz. El nombre de la aplicación es ROOTVE, dicha aplicación tiene

soporte local. http://www.funmrd.gov.ve

Se inicia ejecutando el software, la aplicación permite autenticación de nivel 1 (por contraseña y nivel 2 (por tarjeta inteligente), en ste caso la autenticación se hizo por contraseña

Figura 5.2: Ventana cuentas de usuario ROOTVE

Una vez que se está dentro de la aplicación, se puede comenzar a generar algunos de los casos de uso descritos en el capítulo 3.

5.2.1. Autoridad de certificación raíz

Toda autoridad de certificación raíz debe pertenecer a una organización, en este caso se tomó como ejemplo de organización a la Universidad de los Andes ULA. Ver figura 5.3

Se introducen los datos pertenecientes a la organización y pasamos a almacenar los datos de la autoridad de certificación raíz, recordemos que la gestión de organización y autoridad (AC) se encuentran dentro del módulo AC. Ver figura 5.4

También se guardan los datos de la autoridad de certificación raíz, el software como medida de seguridad le pedirá al usuario que firme digitalmente las acciones que él esta realizando. La acción de que el usuario tenga que firmar es lo que llamabamos en el

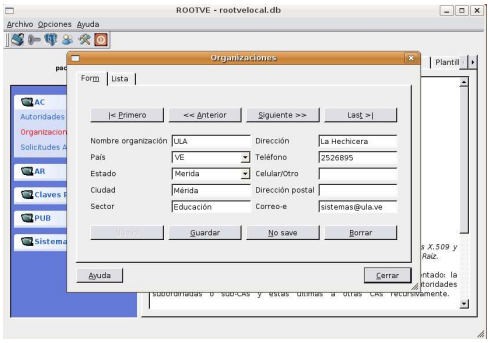

Figura 5.3: Organizaciones

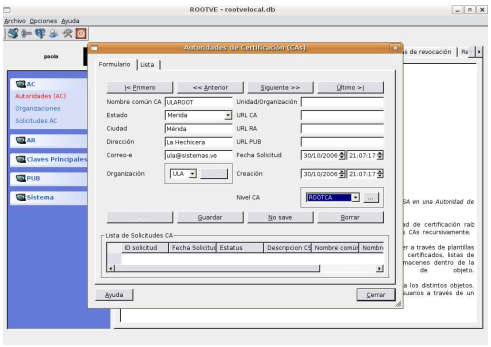

Figura 5.4: Autoridad de certificaciones

capítulo 2 **no repudio**, por lo tanto cada una de las operaciones que el usuario realice van a estar registradas. Ver figura 5.5

Ya se tienen los datos correspondientes a la AC raíz, ahora se pasa a generar el par de claves pública/privada y su certificado autofirmado, la aplicación admite generación de claves en hardware (la clave puede ser generada en el HSM) o en software (generada por ROOTVE). Ver figura 5.6

Listo el par de claves, pasamos a realizar la solicitud de firma de certificado. Ver figura 5.7 y figura 5.8

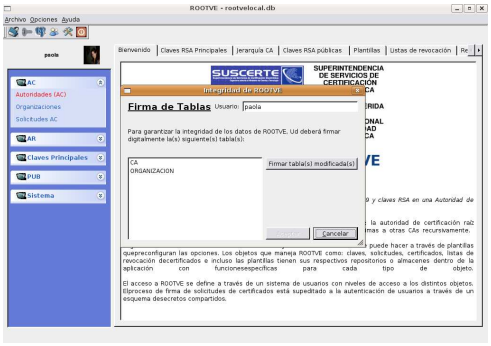

Figura 5.5: Integridad de ROOTVE

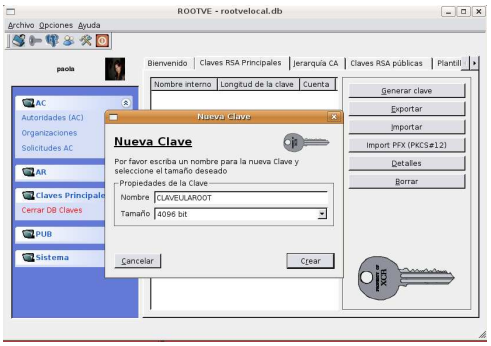

Figura 5.6: Clave nueva

La autoridad de certificación puede observar la solicitud y el estado de la mísma. Ver figura 5.9

Después de que la solicitud esta hecha, generamos el certificado autofirmado. Esta acción corresponde con el caso de uso emitir certificado de una Ac raíz de la figura 3.1. Ver figura 5.10-.13

Características de una Autoridad de Certificación Raíz:

1. Debe poseer un par de clave pública/privada, recordemos que la clave privada de

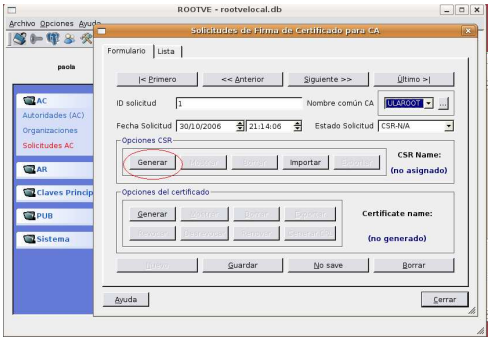

Figura 5.7: Solicitud de firma de certificados

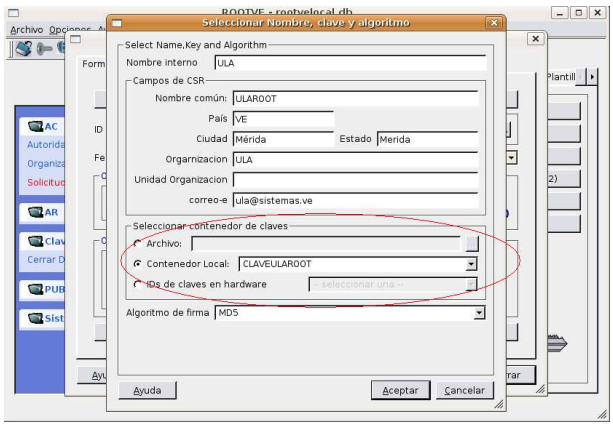

Figura 5.8: Generación de la CSR

la autoridad debe estar almacenada en el HSM, la clave privada no es conocida por otra persona.

2. Debe ser parte de una Organización.

3. Cada acción que se ejecute debe se firmada digitalmente, con su clave privada.

4. Una autoridad de certificación raíz es la única que puede autofirmar certificados.

5. La autoridad de certificación raíz solo certifica a proveedores de servicios de certificación.

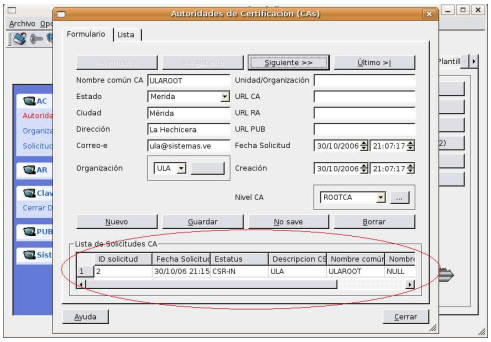

Figura 5.9: Estado de solicitud de la firma

6. Una Autoridad de certificación raíz, es el principal ancla de confianza dentro de una infraestructura de clave pública.

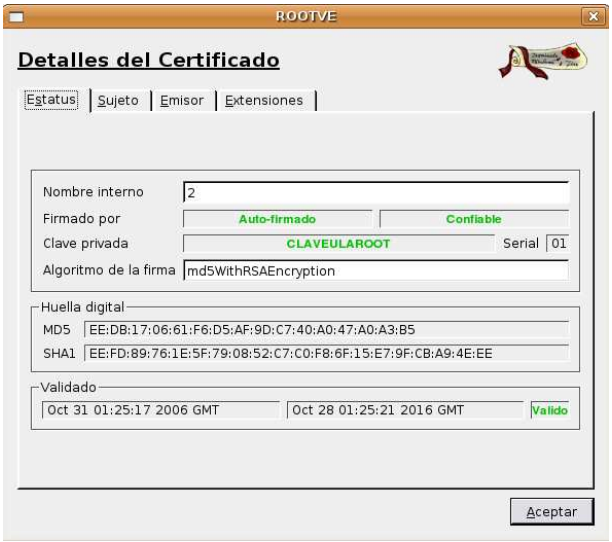

Figura 5.10: Estado del certificado

Emitir certificados

Una autoridad de certificación raíz puede emitir certificados a PSC provenientes de su misma organización o de organizaciones externas, en el ejemplo se genera un certificado para un PSC externo. Ver figuras 5.16-19

Figura 5.11: Certificado de un PSC

Características de un certificado para PSC:

1. No son certificados autofirmados.

2. Debe incluir los datos de la autoridad que lo certifica.

3. Debe poseer los datos del proveedor de servicios de certificación.

4. Tiene un periodo de válidez.

5. Se encuentran almacenados en un directorio repositorio.

Revocar certificados

Revocar certificados es parte de los casos de uso de una autoridad de certificación raíz.

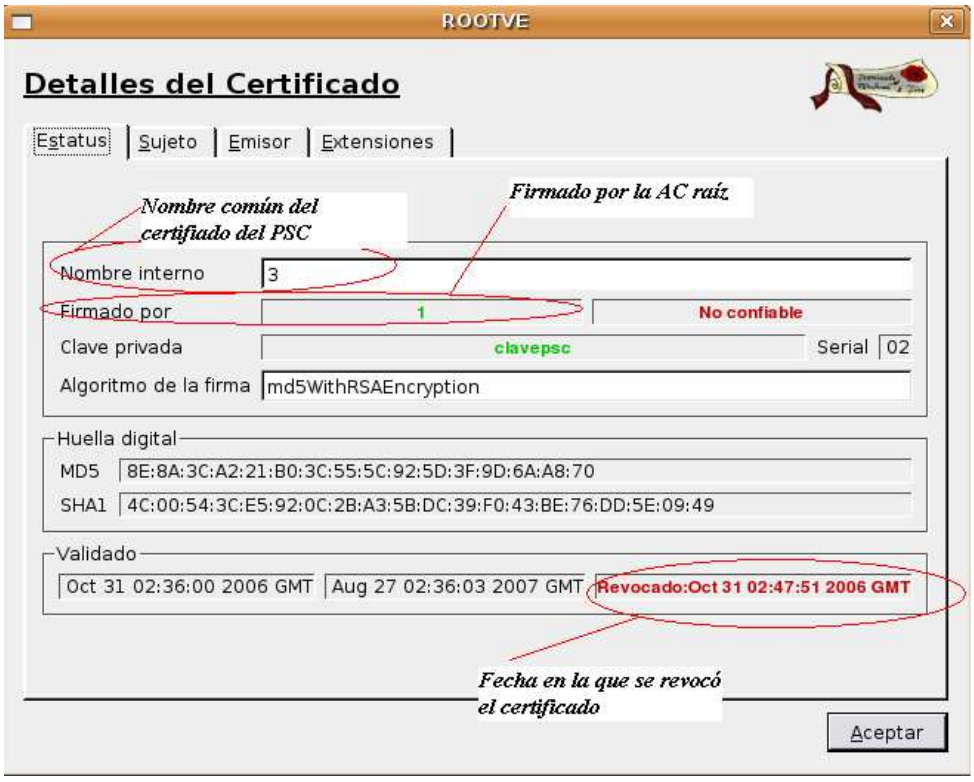

Figura 5.12: Certificado del PSC revocado

Características de un certificado revocado:

1. La Lista de Certificados Revocados (CRL) contiene el número de serie de todos los certificados emitidos por una Autoridad de Certificación y que, por algún motivo

han dejado de ser válidos de manera previa a la expiración de su periodo de validez original.

2. Para saber si un certificado es de confianza debe comprobar si el número de serie del mismo está incluido en la CRL publicada por la Autoridad de Certificación emisora. Si es así, el certificado ha sido revocado y no es de confianza.

5.2.2. Administrador PUB

Aqui el usuario encuentra la lista de autoridades de certificación raíz y de proveedores de servicios de certificación. Se puede observar el estado de los certificados (certificados válidos y no válidos). Esto satisface el caso de uso correspondiente publicación de certificados de la figura 3.4

Figura 5.13: Portal web del PUB

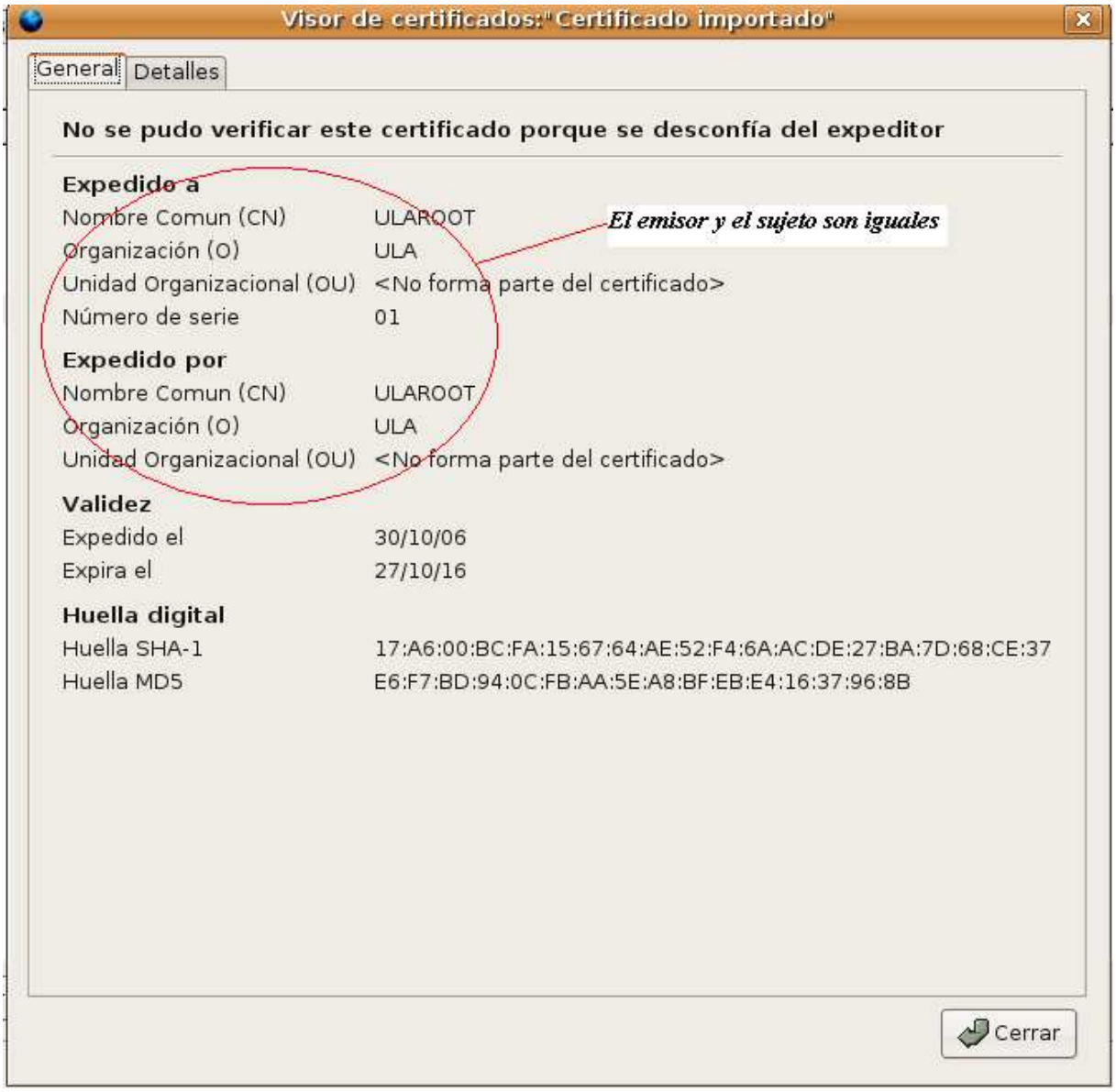

Figura 5.14: Certificado raíz

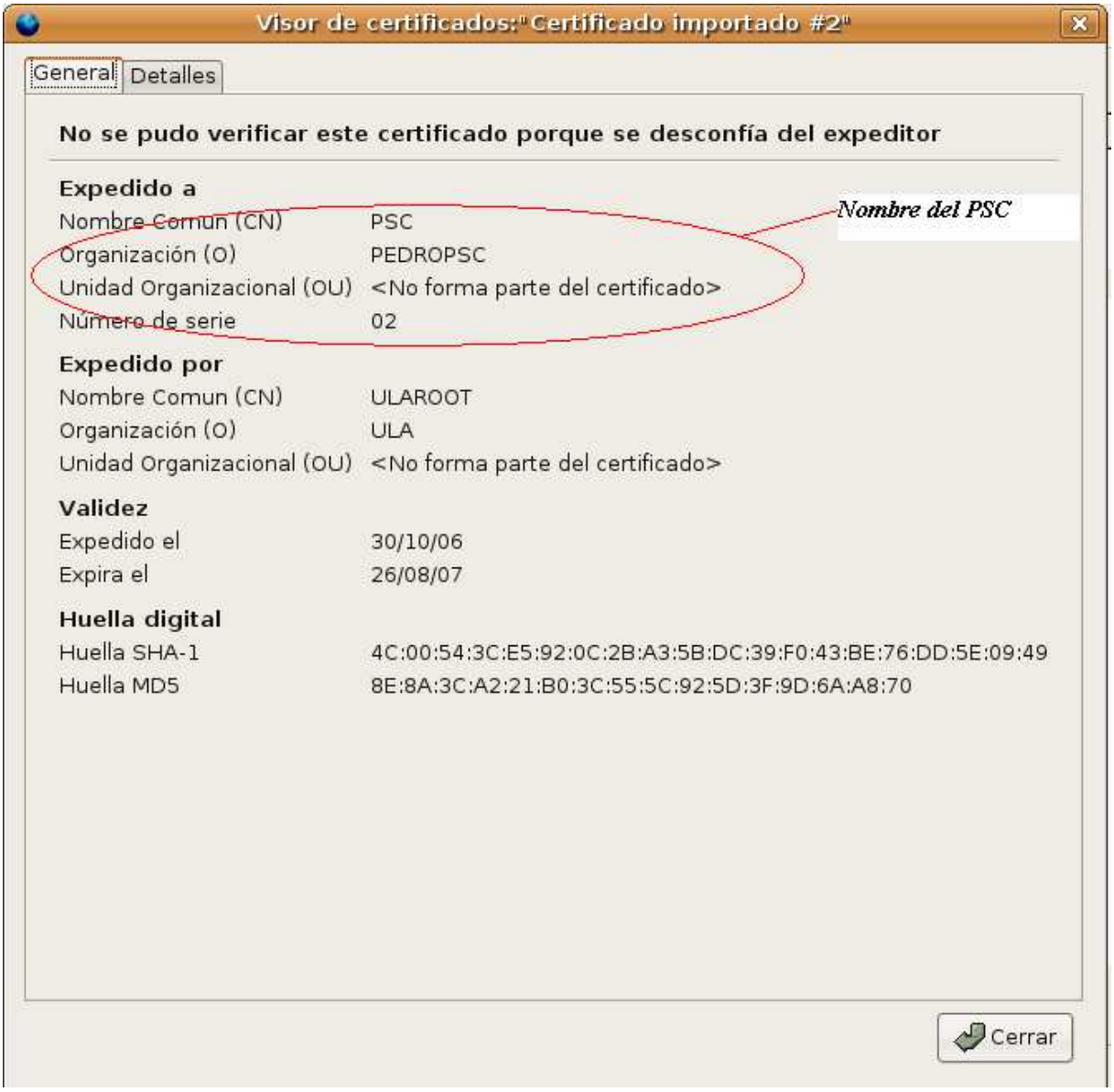

Figura 5.15: Certificado

Capítulo 6

Conclusiones

6.1. Conclusiones

La infraestructura de clave pública es una solucion válida para prestar servicios de seguridad (autenticación, integridad, confidencialidad y no repudio) por medio de certificados digitales; este trabajo incluye un marco teórico para facilitar la comprensión de aspectos como seguridad informática, herramientas criptográficas, infraestructura de clave pública entre otras cosas.

Se seleccionó un modelo de confianza jerárquico para una infraestructura de clave pública, en este modelo se encontraron las siguientes ventajas y desventajas:

- Es muy fácil incorporar una nueva comunidad de usuarios, estableciendo una relación entre la AC de la comunidad y la AC Raíz u cualquier otra. La posición de la nueva AC puede estar determinada por las políticas de la organización.
- La búsqueda de la cadena de certificados es muy simple porque existe una sola dirección de confianza.
- Si la AC raíz es comprometida, se compromete toda la ICP y no existe una forma directa de recuperarse.

Una vez definido el modelo, se realizó una configuración de software para la gestion de una AC raíz, probando que la mayoría de los casos de uso expuestos en el capítulo 3 se satisfacen. El software utilizado fue ROOTVE debido a que cumple con las gestiones de los componentes de una ICP, es software libre y tiene soporte local.

6.2. Recomendaciones

- Establecer un conjunto de políticas de prácticas de certificación en coherencia con las leyes del estado.
- Buscar y seleccionar otras aplicaciones y bibliotecas basadas en software libre que satisfagan nuevas gestiones dentro de una ICP.

Bibliografía

.1. Bibliografía

[1] Schmuller, J. *Aprendiendo uml en 24 horas* (P. hall, Ed.).

[2] Booch, G. (1999). *Uml lenguaje unificado de modelado* (A. Wesley, Ed.).

[3] CNSI. (2005). *Rootve.*URL:http://cnsi.funmrd.gov.ve/web-rootve/.

[4] Nash, A. (2002). *Pki infraestructura de claves publicas (la mejor tecnología para implementar y administrar la seguridad electrónica de su negocio)* (McGRAW-HILL, Ed.).

[5] Larman Craig. *UML y PATRONES. Una Introducción al Análisis y Diseño Orientado a Objetos y al Proceso Unificado.* Segunda Edición. Prentice Hall Madrid 2003.

[6] Pierre-Muller Alain *Modelado de Objetos con UML.* Eyrolles Barcelona 1997.

.2. Referencias Web

[7] http://www.rsasecurity.com

[8] http://cnsi.funmrd.gov.ve/web-rootve/

[9] http://www.suscerte.gob.ve/

[11] Díaz J. *Usando Infraestructura PKI para implementar firma digital.* http://www.linti.unlp.edu.ar

[12] https://software-libre.org

[13] http://www.C3po.es

[14] http://www.spleepycat.com

[15] http://www.postgresql.org

[16] http://www.eskimo.com

[17] http://www.openssl.org

[18] http://www.trolltech.com

[19] http://httpd.apache.org/

[20] http://es.wikipedia.org/wiki/HSM

[21] http://www.gemplus.com

[22] http://www.gpul.org

[23] http://es.wikipedia.org/wiki/X.509

Apéndice A

Descripción de ROOTVE

A.1. ROOTVE

ROOTVE es una aplicación desarrollada para crear y administrar certificados X.509 y claves RSA en una Autoridad de Certificación Raíz. Todo lo necesario para una autoridad de certificación se ha implementado: la autoridad de certificación raíz puede firmar certificados para autoridades subordinadas o sub-CAs y éstas últimas a otras CAs recursivamente. La generación de solicitudes de firma de certificados y los certificados mismos se puede hacer a través de plantillas que preconfiguran las opciones. Los objetos que maneja ROOTVE como: claves, solicitudes, certificados, listas de revocación de certificados e incluso las plantillas tienen sus respectivos repositorios o almacenes dentro de la aplicación con funciones específicas para cada tipo de objeto. El acceso a ROOTVE se define a través de un sistema de usuarios con niveles de acceso a los distintos objetos. El proceso de firma de solicitudes de certificados está supeditado a la autenticación de usuarios a través de un esquema de secretos compartidos. http://cnsi.funmrd.gov.ve/web-rootve/

Esta aplicación está pensada como una herramienta para gestionar una autoridad de certificación raíz. Se almacenan claves públicas/privadas y se gestionan solicitudes de certificados, certificados y listas de revocación de certificados. ROOTVE tiene como base

el software XCA (http://www.hohnstaedt.de/xca.html) desarrollado por Christian Hohnstaedt (christian@hohnstaedt.de) que gestiona claves RSA y certificados digitales.

ROOTVE es una aplicación desarrollada utilizando herramientas basadas en software libre y se distribuye bajo la licencia GPL.

A.1.1. Características de la aplicación

A continuación se describen algunas características de la aplicación ROOTVE:

- Punto inicial de confianza de una Infraestructura de Claves Públicas.
- Software para gestión de Autoridad de Certificación Raíz.
- Generación y almacenamiento seguro de claves privadas.
- Generación de certificados digitales bajo el estándar X509v3.
- Cumplimiento de estándares aceptados para aplicaciones de autoridades de certificación.
- Mecanismo de respaldo y manejo del ciclo de vida de claves.
- Uso de herramientas basadas en software libre para el desarrollo de la aplicación.

A.1.2. Funcionalidades de la aplicación

A continuación se describen funcionalidades de la aplicación ROOTVE:

- Generación de pares de claves RSA (pública/privada), solicitudes de firma de certificados (CSR), certificados digitales de AC, certificados digitales de entidades finales (usuarios de la aplicación), listas de revocación de certificados (CRL).
- Almacenamiento de datos persistentes en BD. Para el almacenamiento de datos persistentes, ROOTVE utiliza una base de datos Postgres (http://www.postgresql.org) con un esquema que guarda información de usuarios, organizaciones, solicitudes de

certificados, certificados, autoridad de certificación, listas de revocación de certificados, entre otras.

- Gestión de usuarios con sistema de permisos y perfiles de usuarios.
- Esquema umbral limite (k,n) de Shamir para acceso al repositorio de claves privadas tanto en software como en dispositivos criptográficos.
- Módulo de registro de acciones dentro de la aplicación para auditoría.
- Rollback de transacciones dentro de la aplicación.
- Integridad de la información de la aplicación a través de la firma digital del contenido de tablas de la base de datos.
- Utilización de hardware criptográfico dentro del ROOTVE.

A.1.3. Arquitectura modular de la aplicación

La aplicación ROOTVE se ha desarrollado pensando en módulos con funciones específicas.

- **Módulo AC:** se realizan las funciones pertinentes de una autoridad de certificación. Generación y revocación de certificados, generación de listas de revocación de certificados entre otras.
- **Módulo AR:** se realizan las funciones pertinentes al registro de información. Se almacena información de: usuarios de la aplicación, organizaciones que gestionan autoridad de certificación, solicitudes de firma de certificados, información de autoridades de certificación, entre otras.
- **Módulo PUB:** se realizan funciones pertinentes a la publicación de certificados digitales. La aplicación permite importar y exportar solicitudes de firma de certificados, certificados digitales, en formatos comunes para intercambiar información con otras aplicaciones de infraestructuras de claves públicas.

A.1.4. Formatos de archivos

Todas las estructuras de datos (claves, solicitudes de firma de certificados, certificados y plantillas) pueden ser importadas y exportadas en diversos formatos como DER o PEM. El proceso de importar significa leer un archivo desde el sistema de archivos y almacenar la estructura de datos en el archivo de base de datos, mientras que el proceso de exportar significa escribir la estructura de datos desde el archivo de base de datos al sistema de archivos, por ejemplo para ser importados en otras aplicaciones.

A.2. Usuarios

Esta sección muestra la forma en que se administran los usuarios dentro de ROOTVE. Los usuarios de ROOTVE se administran a través de un sistema de usuarios que define un login o identificador, una contraseña o PIN (autenticación con tarjetas inteligentes) y niveles de acceso. Al realizar la instalación de ROOTVE se crea una cuenta de usuario cuyo login es root y su password es root. El usuario root sólo tiene privilegios dentro de la aplicación para crear otros usuarios.

A partir de esta cuenta, se puede ejecutar la aplicación:

A.2.1. Creación de usuarios

Para crear cuentas de usuario es necesario acceder al módulo Sistema y hacer click sobre la opción Usuarios.

Se abre el diálogo Gestión de usuarios que permite la creación de nuevos usuarios, la actualización de datos de usuarios existentes, la eliminación de usuarios así como también visualizar los registros asociados a todas las cuentas de usuario existentes en la aplicación.

Para crear un usuario es necesario hacer click en el botón Insertar del diálogo. Este limpia los campos del diálogo. Es necesario introducir la siguiente información:

- Cédula: número de cédula de identidad del usuario, especificando si es venezolano (V) o extranjero (E).
- Cuenta: identificador de la cuenta del usuario.
- Autenticación: el tipo de autenticación que va a utilizar el usuario. Los mecanismos disponibles son los siguientes:
    - Autenticación: el tipo de autenticación que va a utilizar el usuario. Los mecanismos disponibles son los siguientes:
    - Tarjeta: utiliza una tarjeta inteligente como mecanismo de autenticación. Para cada usuario nuevo que tenga este mecanismo se le crea dentro de la tarjeta un par de claves RSA pública/privada. La clave pública del par se extrae de la tarjeta y se guarda en la base de datos Postgres. La clave privada no se puede extraer de la tarjeta.

      Cuando un usuario intenta entrar a ROOTVE y tiene la autenticación utilizando tarjetas ocurren los siguientes pasos:

        - Se generan unos datos aleatorios dentro de la tarjeta inteligente.
        - Se firman digitalmente los datos aleatorios dentro de la tarjeta inteligente y se envian a la aplicación.
        - La aplicación busca la clave pública del usuario que se está autenticando.
        - Se verifica la firma digital de los datos aleatorios recibidos con la clave pública. Si la firma es verificada el usuario es quien dice ser; por lo tanto se deja entrar a la aplicación. En caso de fallar la autenticación se genera un mensaje de error y el usuario deberá probar nuevamente. Después de 3 intentos fallido por medidas de seguridad la tarjeta inteligente se bloquea. Para desbloquear la tarjeta debe recurrir al administrador de la aplicación.

- Nivel de acceso: para establecer los permisos que el usuario tendrá sobre los objetos dentro de ROOTVE. Aquí se especifica el perfil de usuario que tendrá el usuario y sus respectivos permisos. Se muestra un diálogo para seleccionar el perfil de usuario y si se desea se pueden agregar o modificar permisos del perfil.
- Nombre comun: nombre completo del usuario.
- País: por defecto se asigna VE (Venezuela).
- Estado: estado en el que reside el usuario (Venezuela).
- Ciudad: ciudad donde reside el usuario.
- Creación: fecha de creación del usuario.
- Organización: a la cual pertenece el usuario. La organización se escoge de un grupo de organizaciones.

A.3. Módulos

A.3.1. Módulo AC (Autoridad de Certificación)

El módulo AC de ROOTVE permite administrar toda la información relevante de a las autoridades de certificación a quienes se les emiten certificados, las organizaciones que gestionan las autoridades y las solicitudes y certificados.

Desde este modulo se pueden manejar:

- **Autoridades (AC):** se muestra el diálogo Autoridades de Certificación que permite introducir, modificar, eliminar y navegar a través de la información una autoridad de certificación que solicita un certificado generado por ROOTVE.
  Para crear una Autoridad de Certificación es necesario hacer click en el botón Insertar del diálogo. Se limpian los campos del diálogo y se introducen los siguientes datos:

- Nombre común CA: identificador de la autoridad de certificación dentro de ROOTVE.
- Estado: estado en el que se encuentra la sede de la autoridad de certificación.
- Dirección: ubicación de la autoridad de certificación.
- Correo-e: un correo electrónico asociado a la autoridad de certificación.
- Organización: organización que administra la autoridad de certificación (lista desplegable de organizaciones).
- Unidad/organanización: unidad de la organización que administra la autoridad de certificación.
- URL CA: url asociada a la autoridad de certificación.
- URL RA: url asociada a la autoridad de registro.
- URL PUB: url asociada al sitio de publicación de certificados e información de la autoridad.
- Fecha solicitud: fecha y hora de la solicitud.
- Creación: fecha y hora de la creación de la autoridad de certificación.
- Nivel CA: establece el nivel de la autoridad de certificación: puede ser ROOT-CA (raíz), Sub-CA (autoridad subordinada) o Proveedor-CA (proveedor de servicios de certificación).

▪ **Organizaciones:** se muestra el diálogo Organizaciones que permite crear, modificar, eliminar y navegar a través de la información una organización definida dentro de ROOTVE. Una organización será una entidad que se encarga de administrar una autoridad de certificación. Inclusive un usuario puede pertenecer a una organización.

Para crear una organización es necesario hacer click en el botón Insertar del diálogo. Se limpian los campos del diálogo y se introducen los siguientes datos:

- Nombre organización: identificador de la organización dentro de ROOTVE.

- País: por defecto VE.
- Estado: estado en el que se encuentra la organización.
- Ciudad: ciudad donde se encuentra la organización.
- Sector: sector al que pertence la organización.
- Dirección: ubicación de la organización.
- Telefono: teléfono de la organización.
- Celular/Otro: otro teléfono de la organización.
- Dirección postal: dirección de correspondencia de la organización.
- Correo-e: correo electrónico de contacto de la organización.

Para obtener un listado de las organizaciones dentro de ROOTVE se debe abrir el diálogo Organizaciones y hacer click en la pestaña Lista del diálogo.

- **Solicitudes AC:** se muestra el diálogo Solicitudes de firma de certificados para CA que permite crear, modificar, eliminar y navegar a través de la información de las solicitudes de firma de certificados de autoridades de certificación.

Apéndice B

Glosario

AC una Autoridad de certificación (en ocasiones se conoce como autoridad de certificado o autoridad que certifica). Una organización o compañía de confianza que expide certificados digitales y parejas de claves pública/privada.

Autenticación la acción de verificar información, como identidad, propiedad o autorización. Los métodos de autenticación incluyen contraseñas, hardware de identificadores de prenda, software de identificadores de prenda, tarjetas inteligentes, software de tarjetas inteligentes y dispositivos biométricos.

AR una entidad que es responsable de la identificación y autenticación de los suscriptores antes de la emisión del certificado, pero no firma ni emite el certificado.

certificado digital una estructura de datos que usa un sistema de clave pública para unir a un individuo en particular y autenticado con una clave pública en particular.

Certificado X.509 información digital firmada por una autoridad de certificado; un certificado X.509 contiene información relacionada con el sujeto que enlaza a un usuario específico con su clave pública.

Cifrado la transformación de texto claro en una forma aparentemente menos legible

(llamada texto cifrado), a través de un proceso matemático. El texto cifrado lo puede leer cualquiera que tenga la clave que lo descifra (deshace el cifrado).

Cifrado asimétrico un método criptográfico que usa una clave para cifrar un mensaje, y una clave diferente para descifrarlo. Es el fundamento de la Infraestructura de claves públicas.

Cifrado simétrico un método que usa la misma clave para cifrar y descifrar información.

clave privada en el cifrado asimétrico o ICP, la clave de cifrado confidencial que mantiene en privado el usuario. La clave privada se puede usar para cifrar un mensaje cuando se descifra con la clave pública correspondiente; debido a que la clave privada se puede usar para descifrar un mensaje, protege la privacidad de la comunicación que envían otros, quienes usan la clave pública para descifrar mensajes.

clave pública la clave de cifrado que se presenta públicamente para comunicarse con seguridad con el poseedor de una clave privada. La clave pública se puede usar para descifrar un mensaje creado por la clave privada del usuario, la cual brinda una prueba de la creación de un mensaje auténtico.

Confianza en tecnología de seguridad, la definición de la relación entre dos partes o computadoras, a través de la cual se conceden ciertos derechos o privilegios a la parte en que se confía.

Confidencialidad limitar la comunicación del contenido privado a las partes autorizadas y conocidas.

CSR solicitud de firma de certificado.

Entidad cualquier elemento autónomo dentro del PKI. Puede ser un CA, RA o una Entidad Final.

Directorio una tabla de búsqueda de nombres de usuario y claves públicas, basada en estándares como X.509.

Firma digital técnica para comprobar que no se ha adulterado un mensaje, usando el cifrado de clave pública.

Función hash fórmula matemática que cambia un bloque de textoen un bloque único de texto cifrado de longitud fija.

ICP (Infraestructura de claves públicas) un sistemaque usa cifrado asimétrico para ofrecer pruebas de la identidad, privacidad de datos, aceptación e integridad de datos.

LDAP (Protocolo lightweight de acceso a directorios) permite a los usuarios acceder y buscar directorios dispares en Internet.

LCR lista de certificados revocados de la autoridad de certificado.

MD5 función hash desarrollada por laboratorios RSA.

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.

RSA uno de los primeros criptosistemas de clave pública, patentado en 1983.

SSL (Nivel de conexiones seguras) es un protocolo para cifrar el tráfico de transacciones en una red.

X.509 el estándar que define el certificado digital.