Universidad de las Ciencias Informáticas

TÍTULO: Obtención de Certificados Digitales de Autorización

Trabajo de Diploma para optar por el Título de Ingeniero en Ciencias Informáticas

Autores: Liset Amador Coll
Mario Pereda Machín

Tutores: Lic. TC Teresa Pagés López
Lic. TC Pedro Luis Vázquez Columbié

Ciudad de la Habana, 08 de julio del 2008.
"Año 50 de la Revolución"

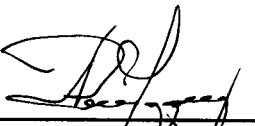
DECLARACIÓN DE AUTORÍA

Declaramos ser únicos autores de este trabajo y reconocemos a la Universidad de las Ciencias Informáticas a hacer uso del mismo en su beneficio.

Para que así conste firmamos la presente a los ____ días del mes de _____ del año _____.

Firma del Autor
(Liset Amador Coll)

Firma del Autor
(Mario Pereda Machín)



Firma del Tutor
(Lic. TC Teresa Pagés López)

Firma del Tutor
(Lic. TC Pedro L. Vázquez Columbié.)

DATOS DE CONTACTO

Lic. TC Teresa Pagés López: Investigadora Auxiliar. Graduada en el año 1985 en Licenciatura en Análisis Especiales de Sistemas de Comunicaciones en la Academia del MININT ¨Eliseo Reyes¨. Ha participado en varios proyectos de investigación y desarrollo. Ha presentado varios trabajos en eventos científicos tanto de autor como coautor de los mismos. Tiene siete años de experiencia en el tema.

Lic. TC Pedro L. Vázquez Columbié: Investigador Agregado. Graduado en Licenciatura en Análisis Especiales de Sistemas de Comunicaciones en la Academia del MININT ¨Eliseo Reyes¨ y es Licenciado en Cibernética Matemática en el año 1991 en la Universidad de La Habana. Ha participado en varios proyectos de investigación y desarrollo. Ha presentado varios trabajos en eventos científicos tanto de autor como coautor de los mismos. Tiene cuatro años de experiencia en el tema.

OPINIÓN DEL TUTOR

AGRADECIMIENTOS

A Concha por su preocupación sin límites, por cuidarnos y guiarnos durante estos cinco años. A Teresa y a Otto, por la ayuda brindada para el desarrollo de esta tesis, por su atención y preocupación. A Armando por brindarnos su apoyo incondicionalmente. Agradecemos muy especialmente a nuestro Comandante en Jefe por poner en nuestras manos los medios para convertirnos en hombres de ciencia; a esta hermosa obra que es la Revolución Cubana; a esta enorme casa, la UCI, por cada instante en ella, muchas gracias.

De Liset:

A mi mamá, a mami y a mi tía Yeins, por su amor, dedicación y apoyo incondicional. Por hacer de mí la persona que soy y por no dejar de exigirme para que sea mejor, por haber estado ahí hasta hoy y porque sé que estarán siempre. Porque las amo más que a nada en el mundo.

A papi, a Ramón y a mis primitos Ramoncito y Luis Carlos que más que primos son mis hermanos.

A mi tía Lily por su cariño y su confianza.

A mi novio Enrique por todo el amor que me ha dado, por su cariño y comprensión, por darme tantas veces el consuelo y el valor que necesité para seguir adelante, por ser parte de mi vida, porque lo amo.

A Mayeya y Kike por su preocupación y afecto.

A Jeney por dejarme saber que siempre puedo contar con ella, por ser mi amiga en todo momento.

A Mario, mi compañero de tesis por su dedicación y su paciencia.

A todos mis compañeros de la universidad, por los buenos y los malos momentos vividos, por la ayuda brindada, por los consejos dados, por compartir conmigo sus vidas durante estos cinco años.

A todas las personas que de alguna forma prestaron su valiosa colaboración para la realización de este sueño, de corazón, GRACIAS.

De Mario:

A mi mamá y mi papá por creer en mí, por todos los años de esfuerzo, sacrificio y dedicación para que yo fuese todo lo que soy hoy y por todo lo que he logrado, gracias por ser los mejores padres del mundo, todas las palabras maravillosas no serían suficientes para expresarles cuantos los amo y admiro, gracias por estar ahí, justo donde y cuando más los necesito. A mis abuelos por darme consejos y por siempre confiar en mí. A toda mi familia, por ser parte importante en mi vida y sentirse siempre orgullosos de mí. A mis hermanas, por marcar momentos felices en mi vida y brindarme todo su apoyo. A mis sobrinos Anel y Adiel por ser los sobrinos que más quiero. A Daniel y Adis por darme su apoyo incondicional, ayudarme a ser mejor profesional, por todo el cariño y la preocupación demostrados.

A todos mis compañeros del grupo 2105, que juntos pasamos hermosos momentos durante estos cinco años de la carrera, por las travesuras y los dolores de cabeza que vivimos juntos. A los que siempre han tenido una mano para ayudar y un rato para compartir. Esos que sin dudas son los mejores que he tenido, los que más he querido y los que extrañaré muchísimo: a Yadil, Osmany, Sergio, Lachy y a Johan Jiménez los de siempre. A mis amigos de bejucal. A la memoria de Willy Nicolás Ramos (Willito). A todas mis amigas, son muchas y cada una especial; a Alianny, por ser la más apegada a mi.

A mis profesores de todas las etapas de mi vida escolar, todos muy buenos y que tanto me han enseñado.

A esos que son la motivación a ser mejor cada día, y son el impulso para transmitir todo lo que de ellos he obtenido, por confiar en mí.

A mi compañera de tesis por su comprensión y su dedicación al trabajo, por ser mi amiga.

A Adila, por ser mi vida. Por ser mi amiga, mi compañera, mi confidente. La persona que me ha permitido quererle sin reservas y que me ha hecho completamente feliz. Mi t, mi tP.

DEDICATORIA

A Fidel y Raúl

por haber sabido dirigir

tan sabiamente la obra de la Revolución.

Al Ministerio del Interior.

A quienes corresponda

la continuación de esta obra.

RESUMEN

La Infraestructura de Llave Pública (PKI) es la tecnología que resuelve el problema de las llaves públicas asociadas a la identificación de un usuario a partir del uso del certificado digital. En la PKI que actualmente se diseña e implementa en Cuba por parte del Ministerio del Interior (MININT) estos certificados se emplean fundamentalmente para la autenticación ante aplicaciones y el aseguramiento del correo electrónico, pero teniendo en cuenta el alto nivel de seguridad requerido por todos los recursos informáticos pertenecientes a este ministerio, no es suficiente identificar a los usuarios, se hace necesario que estos certificados brinden la posibilidad de conocer el nivel de acceso de cada usuario sobre la aplicación ante la cual se autentica, es por ello que en el presente trabajo de diploma se ha concebido, sobre la base del estándar X.509 v3, un certificado digital de autorización que permitirá reflejar no sólo la información concerniente a la identidad de la entidad certificada sino también la incorporación de la información referente a las facultades con que cuenta dicha entidad sobre cada uno de los recursos a los que acceda, además se especifican el conjunto de acciones inmediatas que deben ser desarrolladas para comenzar a utilizar estos certificados. Finalmente se plantea el esbozo inicial de una propuesta para la implementación y puesta en funcionamiento en el país de una Infraestructura de Administración de Privilegios (PMI) orientada a integrarse con la PKI, pues los certificados de atributos gestionados por esta infraestructura vincularán uno o más atributos a una identidad. De esta forma intervendrán dos certificadores en la más precisa identificación del titular, el primero que certifica la identidad de las entidades por medio de un certificado de llave pública y el segundo que certifica las atribuciones y competencias de esas entidades para efectuar una determinada operación sobre un recurso.

Palabras Claves

PKI, certificado de llave pública, X.509, autorización, control de acceso.

ABSTRACT

Public Key Infrastructure (PKI) is the technology that solves the problem of public keys associated with the identification of a user by using the public key certificate. In Cuba, the PKI is currently designed and implemented by the Ministry of Interior (MININT) and the digital certificates are primarily used for authentication to applications and securing email, but taking into account the high level of security required by all computing resources belonging to this ministry, is not enough to identify users, but it is also necessary that those certificates provide the possibility to know the access level for each user on the application acceded, that is why in this thesis was conceived, based on standard X.509 v3, an authorization digital certificate allowing to reflect not only the information concerning to the identity of the certified entity, but also the incorporation of the information regarding the concessions over all resources it has access to. Besides, there are specified the set of immediate actions that should be developed to start using those certificates. Finally, it is raised the initial outline of a proposal for the implementation and operation in the country of a Privilege Management Infrastructure (PMI) oriented to be integrated with the PKI, because the attribute certificates managed by this infrastructure are going to link one or more attributes to an identity. This involved two certifiers in the more precise identification of the holder, the first to verify the identity of the entities through a public key certificate, and second that certifies the powers and prerogatives of these entities to perform a particular operation over a particular resource.

ÍNDICE

INTRODUCCIÓN

La utilización masiva de las computadoras y redes como medios para almacenar, transferir y procesar información se ha incrementado espectacularmente en los últimos años, al grado de convertirse en un elemento indispensable para el funcionamiento de la sociedad actual. Como consecuencia, la información en todas sus formas y estados se ha convertido en un activo de considerable valor, el cual se debe proteger y asegurar para garantizar su integridad, confidencialidad y disponibilidad, entre otros servicios de seguridad.

Actualmente se ha incrementado en Cuba el uso de aplicaciones electrónicas que abarcan: correo, comercio, transacciones, acceso seguro a bancos de información, comunicaciones seguras, entre otras. Por tal motivo, los requerimientos de seguridad son cada vez mayores, presentándose así un problema que la Seguridad Informática, haciendo uso fundamentalmente de técnicas criptográficas, trata de resolver implementando diversos servicios de seguridad.

Desafortunadamente los avances tecnológicos también han propiciado la proliferación de fraudes y robo de información vía electrónica, debido a esto es necesario contar con tecnologías que permitan asegurar la información. La solución más acertada hasta el momento la constituyen los certificados digitales, los cuales permiten la autenticación con un elevado grado de confiabilidad, pues se basan en dos características muy importantes: algo que el usuario sabe (una contraseña) y algo que el usuario posee (su llave privada).

La principal misión de los certificados no es otra que resolver de forma satisfactoria el problema de la autenticidad de las llaves empleadas en los sistemas de criptografía de llave pública. Como consecuencia, actualmente se utilizan los términos "certificado de llave pública" y "certificado digital" como sinónimos.

La PKI resuelve el problema de las llaves públicas asociadas a la identificación de un usuario a partir del uso del certificado digital. En la PKI que actualmente se diseña e implementa en Cuba, no está concebida la generación de certificados digitales de autorización, por lo que resulta conveniente, su diseño e implementación sobre el estándar de certificado digital X.509 v3, con el fin de resolver los problemas de autorización en las aplicaciones habilitadas por PKI en el MININT.

El interés creciente que ha suscitado este tipo de certificación en la comunidad científica viene marcado por las limitaciones que existían en los estándares X.509 a la hora de abordar las cuestiones relacionadas con la autorización. Se debe tener en cuenta que el principal objetivo de los certificados de llave pública ha sido el de proporcionar un mecanismo que permitiera establecer una relación entre el nombre y las llaves públicas de las entidades. (1) Sin embargo, el nombre no es más que un índice, un valor al cual habrá que asociar posteriormente una serie de atributos con el fin de determinar de qué privilegios dispone el usuario.

Partiendo de la situación problemática existente se ha definido el siguiente **problema científico**:

¿Cómo obtener un certificado digital de autorización?

A partir de este problema se estableció como **objeto de estudio** el proceso de obtención de certificados digitales.

El **objetivo** de este trabajo de diploma es concebir un certificado digital de autorización que permita resolver los problemas existentes en cuanto a la delimitación de niveles de acceso en las diferentes aplicaciones de la Infraestructura del MININT.

El **campo de acción** lo constituye la definición del campo de extensión de los certificados digitales X.509 v3.

Siendo la **hipótesis** que se plantea la siguiente: la obtención de Certificados Digitales de Autorización contribuirá a asegurar un correcto control de la autorización para el acceso y uso de los recursos informáticos en el MININT.

Para dar cumplimiento al objetivo planteado se llevaron a cabo un conjunto de **tareas**:

- Estudio detallado de las tendencias actuales de los certificados digitales en Cuba y el mundo.
- Investigación y análisis de la experiencia internacional en el uso de los certificados digitales con fines de autorización.
- Realización de un análisis detallado de las características del estándar para certificados de llave pública X.509 v3.
- Evaluación de la posibilidad de usar el estándar X.509 v3 como certificado digital de autorización.
- Definición de una extensión particular que permita incorporar la información referente a autorización en el certificado de llave pública X.509 v3.
- Puntualización de las principales ventajas que pueden derivarse de la integración de los certificados digitales de autorización en aplicaciones habilitadas por PKI en el MININT.
- Elaboración del esbozo inicial de una propuesta para la implementación de una PMI.

Métodos teóricos de la Investigación:

Histórico-Lógico: Permitió, a partir de la documentación consultada referente al origen y evolución de los Certificados Digitales determinar las tendencias actuales en el proceso de Obtención de Certificados Digitales de Autorización.

Analítico-Sintético: Este método se empleó fundamentalmente para el análisis de los diferentes campos que constituyen el certificado digital, teniendo en cuenta que el estudio exhaustivo de cada uno de ellos de forma relativamente independiente posibilitó una mejor comprensión de las relaciones e interacciones existentes entre estos elementos. Además este método permitió un mejor entendimiento del funcionamiento de la PKI, pues el análisis de cada uno de sus componentes de manera específica propició la comprensión de la influencia de los mismos en el correcto funcionamiento de la infraestructura, y mediante la síntesis se consiguió alcanzar un elevado conocimiento en cuanto a las relaciones existentes entre los diferentes componentes.

Hipotético-Deductivo: El empleo de este método desempeñó un papel esencial en el proceso de verificación de la hipótesis, permitiendo a partir de la misma inferir conclusiones en el transcurso de la investigación y establecer predicciones a partir del sistema de conocimientos ya poseído. Se aplicó en el análisis y construcción de las teorías científicas, posibilitando la sistematización del conocimiento científico adquirido durante el desarrollo de este trabajo de diploma.

Métodos empíricos de la Investigación:

Observación: Permitió percibir directamente el proceso de generación y emisión de un certificado digital, eliminando de esta forma las deformaciones que podrían presentarse con el uso de métodos indirectos, el registro visual de lo ocurrido permitió clasificar los acontecimientos de acuerdo con un esquema previsto, diferenciando los aspectos significativos de aquellos que no lo son.

El presente trabajo de diploma consta de Introducción, tres capítulos, Conclusiones y Recomendaciones.

En el Capítulo 1 se hace referencia a un conjunto de conceptos cuyo entendimiento es fundamental para la comprensión de los temas tratados, se analizan los antecedentes y tendencias actuales en Cuba y el mundo de los certificados digitales y del uso de los mismos con fines de autorización. Además se describe detalladamente el estándar para certificados digitales X.509 haciendo referencia a cada uno de los campos que componen el mismo.

En el Capítulo 2 como parte de la descripción de la solución se detalla la sintaxis ASN.1 de los certificados X.509, se explica en que consisten y que papel desempeñan dentro de la solución los OID. Lo fundamental de este capitulo es la definición de una extensión privada para los certificados X.509 v3 que permitirá incorporar en los mismos la información sobre autorización, también se plantean un conjunto de acciones que se deben llevar a cabo para comenzar a utilizar estos certificados.

En el Capítulo 3 se explica como la solución planteada en el Capítulo 2 no es una solución definitiva para el problema de la autorización y el control de acceso y se plantea el esbozo inicial de una propuesta para la implementación de una PMI en el país.

CAPÍTULO 1: Fundamentación Teórica

1.1 Introducción

En este Capítulo se abordarán aquellos elementos teóricos que constituyen el sostén del problema científico que se ha planteado, para ello se hará referencia a los conceptos fundamentales que posibilitarán un mejor entendimiento de la investigación, se analizarán los antecedentes y tendencias actuales de los certificados digitales en diferentes países, incluido Cuba y se realizará una breve descripción de otra solución que da respuesta al problema planteado.

1.2 Conceptos asociados al dominio del problema

Criptografía:

Según el Diccionario de la Real Academia, la palabra Criptografía proviene del griego *"kryptos"* que significa oculto, y *"graphos"*, que significa escritura, y su definición es: "Arte de escribir con llave secreta o de un modo enigmático".

Desde un punto de vista técnico, se puede establecer que la criptografía es la ciencia que se encarga de la protección de datos mediante la transformación matemática de los mismos a un formato ilegible.(2)

La criptografía es la ciencia que estudia la escritura secreta, una cifra o criptosistema es un método secreto de escritura mediante el cual un texto en claro se transforma en texto cifrado o criptograma. Se le llama cifrado al proceso de transformar texto en claro en texto cifrado mediante llaves criptográficas. Esta ciencia se ocupa del análisis y diseño de algoritmos para cifrar y el criptoanálisis se encarga de romper esos algoritmos.

Criptografía asimétrica:

Método criptográfico en el que se utiliza un par combinado de llave pública y privada para el cifrado y el descifrado de mensajes.(3) Para enviar un mensaje cifrado, un usuario codifica un mensaje con la llave pública del receptor. Al recibirlo, se descifra con la llave privada del receptor. La utilización de diferentes llaves para las funciones de codificación y descifrado se conoce como la función de trampilla unidireccional, es decir, la llave pública se utiliza para codificar un mensaje pero no se puede utilizar para descifrarlo. Sin saber la llave privada, es prácticamente imposible invertir esta función gracias a las potentes funciones de codificación modernas.

Firma digital:

La firma electrónica o firma digital es una pieza de información que añadida a un mensaje, permite al receptor probar el origen y la integridad de los datos recibidos.(4)

La firma digital permite al destinatario de un mensaje verificar la autenticidad del origen de la información así como verificar que dicha información no ha sido modificada desde su generación. De este modo, la firma digital ofrece el soporte para la autenticación e integridad de los datos así como para el no repudio en origen, debida a que el originador de un mensaje firmado digitalmente no puede argumentar que no lo es.

Una firma digital está destinada al mismo propósito que una manuscrita. Sin embargo, una firma manuscrita es sencilla de falsificar mientras que la digital es imposible a menos que se posea la llave privada del firmante.

La firma digital se basa en la propiedad de que un mensaje cifrado utilizando la llave privada de un usuario sólo puede ser descifrado utilizando la llave pública asociada. De tal manera, se tiene la seguridad de que el mensaje que ha podido descifrarse utilizando la llave pública sólo pudo cifrarse utilizando la privada

Para evitar el principal inconveniente de los algoritmos de llave pública que viene dado por su lentitud, la cual crece con el tamaño del mensaje a cifrar, la firma digital hace uso de funciones resumen. Una **función resumen** es una operación que se realiza sobre un conjunto de datos de cualquier tamaño de forma tal que se obtiene como resultado otro conjunto de datos, de tamaño fijo independiente del tamaño original que, además, tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es prácticamente imposible encontrar dos mensajes distintos que tengan un resumen idéntico

Si la firma contiene la fecha y la hora de la transmisión, se obtiene protección contra la reactuación. Una firma digital es un medio para que los creadores de un mensaje, archivo u otra información codificada digitalmente vinculen su identidad a la información; es decir, proporcionen una firma.

Certificado Digital:

Loren Kohnfelder definió en 1978 (5) el término "certificado digital" como un documento firmado digitalmente que contiene tanto un nombre como una llave pública.

Los certificados son documentos digitales que aseguran que una llave pública corresponde a un usuario o entidad determinados, evitando así que alguien pueda utilizar una combinación de llaves pretendiendo ser otra persona. (6)

En el contexto de este trabajo de diploma, un certificado digital o certificado de llave pública constituye un documento electrónico intransferible y no modificable, generado y firmado digitalmente por una entidad de certificación, la cual vincula un par de llaves con una entidad determinada confirmando su identidad, constituye el equivalente digital del Carnet de Identidad en lo que a la autentificación de individuos se refiere, permitiendo que su propietario demuestre que es quien dice ser, es decir, que está en posesión de la llave secreta asociada a su certificado. Para los usuarios proporcionan además un mecanismo

para verificar la autenticidad de programas y documentos obtenidos a través de la red, el envío de correo encriptado y/o firmado digitalmente, etc.

Certificado Digital de Autorización:

Los Certificados de Autorización o potestad son aquellos que certifican otro tipo de atributos del usuario además de la identidad del mismo, como pueden ser, el pertenecer a una determinada asociación, disfrutar de una serie de privilegios, poseer un carnet de conducir, etc. (10)

Como parte de la realización de este trabajo de diploma se ha definido el **certificado digital de autorización** como un certificado digital en el que se refleja, además de la información sobre la identidad del usuario, aquella referente a los privilegios y/o permisos que le han sido conferidos a la entidad poseedora del certificado, esto se hará mediante la incorporación al certificado de una extensión privada definida con este fin, propiciando de esta forma el uso de los mismos en el control de acceso a recursos y aplicaciones.

Control de acceso:

Método que garantiza que solo tengan acceso a un sistema o a la información que éste contiene, aquellos debidamente autorizados para ello.(7) Los mecanismos de control de acceso se implementan utilizando técnicas de software y de hardware y por lo general incluyen: identificación y autenticación de usuarios; limitación de acceso a ficheros, monitorización de las acciones de los usuarios y un sistema de auditoría.

Confidencialidad:

Es el servicio básico de un sistema de seguridad. Proporciona la privacidad de los datos y protege contra el análisis y manipulación de los mismos. El mecanismo principal para este servicio es el cifrado de datos. A veces se emplea también tráfico de relleno para evitar el análisis de tráfico por un intruso.(8)

De acuerdo con lo planteado en (9) la confidencialidad es la condición que asegura que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados.

En otras palabras para poder afirmar que una información es confidencial se tiene que asegurar que la misma sólo puede ser accedida por el destinatario previsto.

Integridad:

Proporciona la seguridad de que los datos no han sido alterados durante la comunicación o almacenamiento. Protege contra la manipulación de los datos.(10)

Es la condición que garantiza que la información sólo puede ser modificada, incluyendo su creación y borrado, por el personal autorizado. (9) De acuerdo con el criterio de los autores y teniendo en cuenta las características de este trabajo de diploma se plantea que el concepto de integridad significa que el sistema no debe modificar o corromper la información que almacene, o permitir que alguien no autorizado lo haga.

Autenticación:

Asegura que un usuario, al momento de utilizar el sistema, es el que se anuncia como tal. Este mecanismo protege contra la suplantación de usuarios y puede implementarse mediante el intercambio de nombre y contraseña entre emisor y receptor, o la firma digital.(8)

Según se establece en (9) la autenticación es el método empleado para comprobar la identificación de un usuario o proceso. Una vez identificado al usuario, es necesario que este demuestre de algún modo la veracidad de su identidad. Actualmente la autenticación biométrica y la autenticación por llave secreta son los modelos de autenticación más fuertes.

No repudio:

Asegura la integridad y la identidad del emisor de los datos, de modo que el mensaje recibido constituya una prueba de ambas cosas. Protege contra el repudio.(8)

El mecanismo más utilizado para lograr el no repudio es la firma digital, puesto que la cadena que se firma con la llave privada del usuario, se obtiene del mensaje enviado, a partir de una función resumen determinada, es por ello que confiere la capacidad de evitar que un usuario niegue más adelante haber efectuado una acción.

Infraestructura de Llave Pública (PKI):

Es una combinación de productos de hardware y software, políticas y procedimientos que posibilitan el uso y administración de certificados y criptografía de llave pública, en sistemas de computación distribuidos. (11) Ofrece la seguridad básica requerida para llevar a cabo aplicaciones electrónicas de forma tal que los usuarios, aunque no se conozcan o estén alejados entre sí, puedan comunicarse con seguridad a través de una cadena de confianza.

Una PKI es el conjunto de elementos de hardware y software, así como de procedimientos y políticas, que permiten llevar a cabo la gestión y el control de vida de certificados digitales.(12)

Autoridad de Certificación:

Entidad encargada de generar los certificados a partir de las solicitudes, firmarlos y almacenarlos en un repositorio de acceso público.(13)

La Autoridad de Certificación es la responsable de emitir, renovar, revocar y publicar los certificados. Además, debe permitir la implementación de políticas de certificación, garantizar el almacenamiento seguro de llaves privadas, crear y mantener actualizadas las listas de revocación y conservar los certificados y llaves privadas que han sido revocados.

Entidad de Registro:

Básicamente, una Autoridad de Certificación puede delegar en una o varias Entidades de Registro distintas funciones. (6) Se utilizan normalmente para distribuir funcionalidad a través de la red en organizaciones de considerable tamaño.

Esta es la entidad encargada de registrar y verificar los datos de quienes solicitan un certificado digital, generar la solicitud de certificación y enviarla a la Autoridad de Certificación.

Lista de Revocación de Certificados Digitales (CRL):

Lista en la que se reflejan los certificados revocados, está firmada por una Autoridad de Certificación u otra autoridad opcional a la que se haya delegado la responsabilidad de la publicación de dicha lista en un repositorio en el que pueda ser libremente accedida. Cada certificado revocado es identificado en una CRL por su número de serie.(14)

Una CRL contiene todos aquellos certificados que por algún motivo han perdido su validez antes de su fecha de expiración, para garantizar la integridad de la información contenida en la CRL la misma es firmada por la Autoridad de Certificación que la emite, esta autoridad debe publicar las CRL periódicamente de forma que la información en ella contenida se mantenga actualizada.

Repositorio:

Sistema o colección de sistemas distribuidos donde se almacenan los certificados y las CRL y que sirve como medio de distribución tanto de las listas como de los certificados para los usuarios. (14)

De acuerdo con otros autores también es definido como un sitio público de fácil acceso donde cada certificado es ubicado luego de ser firmado digitalmente por la autoridad que lo emite y donde se disponen las CRL correspondientes.(10)

Un Repositorio debe contar con gran capacidad de almacenamiento así como permitir numerosas conexiones simultáneas de forma que se garantice y facilite el acceso de los usuarios, permitiendo que las CRL y los certificados sean consultados y/o descargados.

Identificador de Objeto (OID)

Un OID es un árbol de nodos, en el que cada nodo es simplemente una secuencia de dígitos. Las normas establecen que una vez que a una entidad se le asigna un nodo en el árbol de OID tiene la facultad de subdelegar los sub-árboles a partir de ese nodo. (15)

Básicamente, un OID es una secuencia de números que se asignan jerárquicamente y que permite identificar cualquier tipo de objetos en la red, siendo usados con gran cantidad de protocolos. Los niveles superiores de una jerarquía de identificadores de objeto se gestionan mediante una autoridad encargada de la asignación y registro de los mismos y se delegan a entidades que pueden a partir del OID asignado crear sus propias definiciones de esquema.

1.3 Certificados Digitales, antecedentes y tendencias actuales

Uno de los problemas fundamentales que surge en Internet es el de la identificación de las personas o entidades, por ejemplo, cómo asegurarse de que una llave pública que se encuentra en la red pertenece realmente a quién dice pertenecer.

Una solución factible es la utilización de un certificado digital, pues al ser un documento electrónico intransferible y no modificable, generado y firmado digitalmente por una Autoridad de Certificación la cual vincula un par de llaves con una persona determinada confirmando su identidad, constituye el equivalente digital del Carnet de Identidad en lo que a la

autentificación de individuos se refiere, permitiendo que un individuo demuestre que es quien dice ser, es decir, que está en posesión de la llave secreta asociada a su certificado. Para los usuarios proporcionan además un mecanismo para verificar la autenticidad de programas y documentos obtenidos a través de la red, el envío de correo encriptado y/o firmado digitalmente, el control de acceso a recursos, etc.

Los formatos más aceptados para los certificados digitales son los definidos en el estándar X.509. Este estándar define formatos de datos y procedimientos específicos para la distribución de llaves públicas a través de certificados firmados digitalmente por Autoridades de Certificación. (16)

La primera versión del estándar X.509 apareció en 1988 y fue publicada como el formato X.509 v1, siendo la propuesta más antigua para una PKI a nivel mundial. Esto, junto con su origen ISO/ITU (International Standards Organization/International Telecommunication Union) han hecho del X.509 el estándar para PKI más ampliamente utilizado. Más adelante, en 1993 la definición del estándar fue ampliada surgiendo el X.509 v2, se adicionaron únicamente dos campos que permitirían identificar de forma única al emisor y al usuario del certificado. Estos campos brindan la posibilidad de reutilizar los nombres del sujeto y/o el emisor, sin embargo, la mayoría de los documentos sobre certificación recomiendan que los nombres no sean reutilizados. Por esta razón, estos certificados son poco usados. (10)

El X.509 v3 amplía aún más la funcionalidad del estándar X.509, y fue publicado en 1996. Los campos básicos del certificado X.509 v3 son los mismos que en el X.509 v2 y los nuevos campos que se añaden se denominan "de extensión" y pueden ser definidos y registrados por cualquier organización o grupo.

Las extensiones del estándar X.509 permiten incluir atributos adicionales en los certificados para gestionar la estructura jerárquica de las Autoridades de Certificación y la construcción y

distribución de las CRL, también permiten a las organizaciones emisoras definir extensiones privadas en los certificados para transportar informaciones particulares y propias de esos grupos.(14) Las extensiones que se definen en el X.509 v3 están en relación con las políticas de seguridad y llaves utilizadas, con los atributos del titular y del emisor del certificado, etc.

Como se puede apreciar la versión tres del X.509 introduce cambios significativos en el estándar. La diferencia fundamental es el hacer el formato de los certificados extensible. Ahora los que implementen X.509 pueden definir el contenido de los certificados como les resulte conveniente.

Las Autoridades de Certificación por lo general pueden emitir diferentes tipos de certificados; básicamente son:

- Certificados de Llave Pública.
- Certificados de Potestad.
- Certificados Transaccionales (actas y resguardos).
- Certificados de Tiempo (estampillado o registro temporal).

Los Certificados de Llave Pública son los más utilizados actualmente dentro de los criptosistemas de llave pública y ligan una identidad personal (usuario) o digital (equipo, software, etc.) a una llave pública.

Los Certificados de Potestad son aquellos que certifican otro tipo de atributos del usuario distintos a la identidad, como pueden ser, el pertenecer a una determinada asociación, disfrutar de una serie de privilegios, poseer un carnet de conducir, etc.

Los Certificados Transaccionales son aquellos que atestiguan que algún hecho o formalidad acaeció o fue presenciado por un tercero.

Los Certificados de Tiempo o de Estampillado Digital de tiempo permiten dar fe de que un documento existía en un instante determinado de tiempo, por lo que constituyen un elemento fundamental de todos los servicios de registro documental y de protección de la propiedad intelectual o industrial.

En la actualidad las aplicaciones principales de los certificados digitales están dirigidas fundamentalmente al Comercio Electrónico (para la identificación personal del propietario en una transacción a través de Internet o dentro de una organización), al aseguramiento de Redes Privadas Virtuales, correo electrónico, comunicación entre servidores y buscadores de Internet, intercambio electrónico de datos, autenticación de aplicaciones y firma de software.

1.3.1 Experiencia internacional en el uso de los Certificados Digitales

Crear una infraestructura tecnológica implica lograr un alto nivel de automatización y desarrollo en los espacios distribuidos, relacionado fundamentalmente con la conectividad y la velocidad de transmisión. Esto concederá el más amplio y seguro acceso a las aplicaciones, sobre todo a aquellas que precisan conexión a la red, por ejemplo: correo y comercio electrónico, acceso a servidores, autenticación de aplicaciones, etc. y además proveerá la eficiencia que exige la sociedad actual.

Independientemente de que aún no exista una normativa internacional para el despliegue de una PKI, cada país debe adoptar un conjunto de regulaciones para que los usuarios de los certificados digitales puedan tener un respaldo legal en las transacciones, validez de los contratos y seguridad en las operaciones comerciales, así como una determinada garantía en cuanto a la seguridad que ofrece el uso de esta tecnología.

Realizar transacciones de cualquier índole a través de la red exige disponer de sistemas de comunicación seguros, capaces de adaptarse a las necesidades de estos servicios; por esa razón, es de gran importancia garantizar todas las normas y procedimientos para lograr una verdadera seguridad informática. A nivel internacional se ha generalizado el uso de los certificados digitales como el medio más apropiado para alcanzar altos niveles de seguridad en cuanto a la autenticación de la identidad de los usuarios.

Colombia

En **Colombia** existe la entidad de certificación digital llamada Certicamara, creada por las Cámaras de Comercio del país, para brindar seguridad y garantía a las transacciones y comunicaciones electrónicas, mediante certificados digitales que cuentan con el respaldo jurídico en las leyes nacionales. Los certificados digitales que emite Certicamara tienen validez nacional debido a que la legislación que se aplica en Colombia para el comercio electrónico no es igual a la de otros países y por lo tanto los certificados digitales emitidos por esta entidad no tendrían valor jurídico fuera del territorio colombiano.(17)

Certicamara brinda dos servicios fundamentales:

Expedición de Certificados Digitales Personales: Estos pueden usarse para brindar seguridad al correo electrónico, control de acceso a usuarios de Internet, Intranet y Extranet ó para todo tipo de transacciones de información como servicios de suscripción on-line.

Expedición de Certificados Digitales para servidores: Estos certificados garantizan la identidad del servidor y posibilitan las comunicaciones seguras y privadas con clientes, socios, proveedores y otras personas u organizaciones. Los Certificados de servidor seguro permitirán mostrar el símbolo de confianza de VeriSign y son ideales para Sitios Web comerciales y servidores de Intranets que por el tipo de información almacenada requieren

comunicaciones seguras; por lo tanto la información crítica (como datos de tarjetas de créditos o datos personales) podrá intercambiarse de una forma totalmente segura y confidencial.

Brasil

En **Brasil**, con fecha 30 de noviembre de 2001, se desarrolló el primer par de llaves criptográficas y el correspondiente certificado digital de la Autoridad Certificadora Raíz de la ICP-Brasil (Infraestructura de Llaves Públicas Brasilera). A partir de esa fecha se pueden emitir certificados a las Autoridades Certificadoras que deseen formar parte de la ICP-Brasil.(18)

Si bien el Gobierno no prohíbe a ninguna empresa o Autoridad Certificadora operar fuera del ICP-Brasil, mantiene, al menos por el momento, la postura de reconocer jurídicamente sólo los certificados emitidos por aquellas empresas que se encuentren reconocidas en el ICP-Brasil.

Esto significa que algunas de las empresas o entidades certificadoras que más posibilidades tenían de explotar este mercado, como Unicert, Serasa o Certisign (de la americana VeriSign), deberán someterse a estas normativas si quieren que sus certificados digitales sean garantizados por el Gobierno. En la práctica, las llaves no avaladas por el ICP-Brasil seguirán teniendo validez aunque sólo en una relación de confianza entre las partes, pero no tendrán validez jurídica, ni la tutela o el aval del Estado como un documento legalmente reconocido.

Argentina

Hace ya varios años que se vienen implementando en el Sector Público Argentino iniciativas relativas a la digitalización de sus circuitos administrativos y a la utilización de la firma digital

para dotar de seguridad a las comunicaciones internas. A partir de la promulgación, en diciembre de 2001, de la Ley N° 25.506 de Firma Digital, este proceso se ha consolidado. (7) La legislación mencionada estableció como obligación del Estado Nacional la utilización de esta tecnología en su ámbito interno fijando un plazo máximo de cinco años para que la misma fuera aplicada a la totalidad de las leyes, decretos, decisiones administrativas, resoluciones y sentencias emanadas del Sector Público Nacional.

A fin de fortalecer y apoyar a los organismos del Sector Público Nacional, la Oficina Nacional de Tecnologías de Información (ONTI) participa activamente en las iniciativas de informatización, proveyendo certificados digitales a agentes y funcionarios públicos actuando como Autoridad Certificante. Estos certificados digitales son administrados de manera centralizada por la ONTI, la cual delega en las jurisdicciones respectivas las funciones de Autoridad de Registro. De este modo se logra mayor eficiencia en el proceso de emisión y administración de los certificados pues el procedimiento de validación de identidad de los suscriptores se realiza directamente en cada organismo, evitando desplazamientos y demoras.

Esta función ha sido asignada a la ONTI por el Decreto Nº 1028/03, el cual establece como una de sus responsabilidades primarias "Asistir al Subsecretario de la Gestión Pública.... actuando como Autoridad Certificante en los organismos del Sector Público Nacional" y dentro de sus acciones "Entender, asistir y supervisar en los aspectos relativos a la seguridad y la privacidad de la información digitalizada y electrónica del Sector Público Nacional".(7)

Con el fin de lograr un mayor nivel de seguridad se ha establecido en Argentina una estructura de certificación de únicamente dos niveles, donde el primer nivel es el de la Autoridad Certificante Raíz, operada por el ente licenciante, y el segundo nivel es el de las

Autoridades Certificantes operadas por los certificadores licenciados. No habrá Autoridades Certificantes subordinadas a estas últimas.

Para que sea reconocido un certificado extranjero, un certificador de la República Argentina debe garantizar la validez y vigencia de ese certificado a través del licenciamiento de una política de certificación apropiada. Los solicitantes de licencias deben ser personas jurídicas, admitiéndose tanto las personas de derecho privado como las de derecho público.(19) Deben hacerlo a través de representantes legales en el caso de personas jurídicas privadas y a través de sus máximas autoridades de la jurisdicción u organismo en el caso de personas jurídicas públicas.

La solicitud se dirige al ente licenciante y debe ser presentada conjuntamente con toda la documentación requerida en la Mesa de Entradas de la Subsecretaría de la Gestión Pública de la Ciudad de Buenos Aires.(19) La infraestructura tecnológica que soporta los servicios de un certificador licenciado deberá estar situada en territorio argentino, bajo su control y afectada exclusivamente a las tareas de certificación. Un certificador licenciado puede emitir certificados a favor de una persona física, una persona jurídica o una aplicación informática, según lo que especifique la política de certificación bajo la cual se emite el certificado.

España

En España el mercado de PKI ha ido creciendo gradualmente en los últimos años. Para 2002, los analistas cifraron en alrededor de 54 millones de euros el volumen del mercado español de servicios de certificación, con las administraciones públicas y el sector financiero, seguidos del sector de las telecomunicaciones, los colegios profesionales y algunas empresas de servicios como sus principales clientes. Evidentemente, su expansión aparece estrechamente ligada al grado de penetración de Internet y al desarrollo del comercio electrónico. (20).

Safelayer Secure Communications S.A. es una empresa española fundada en mayo de 1999, fabricante de soluciones de software de seguridad para gestión de identidad digital, firma electrónica y protección de datos. En enero del año 2004 la Fábrica Nacional de Moneda y Timbre (FNMT) seleccionó la tecnología de Safelayer Secure Communications para renovar el sistema de certificación electrónica CERES (Certificación Española). En su momento Safelayer explicó que el objetivo de este proyecto, era ampliar la gama de productos y servicios basados en la utilización del certificado y la firma digital.(21) Actualmente, la tecnología de Safelayer sustenta los dos mayores proyectos de certificación e identificación digital de España, que son la FNMT y el DNI (Documento Nacional de Identidad) Digital.

De acuerdo a Safelayer, empresa líder del mercado PKI en España, la puesta en marcha del DNI Digital supondrá un efecto multiplicador en cuanto a la extensión de la firma digital en la sociedad. Según prevé esta empresa, aunque el sector empresarial será el primero en extender este uso, no se debe perder de vista su extensión en el usuario personal, tanto profesionales liberales como usuarios particulares.(10)

También se prevé que la PKI que ha desarrollado Safelayer, soportará hasta 60 millones de usuarios con al menos dos certificados por cada uno de ellos. En estos 60 millones de usuarios, se integran los 33 millones de usuarios actuales que contarán con el nuevo DNI electrónico, más el crecimiento vegetativo calculado para los próximos años, que según estima el Ministerio del Interior español, será de un millón de usuarios nuevos por año.(22)

1.3.2 Experiencia cubana

En el año 1997 la Resolución Económica del V Congreso del Partido Comunista de Cuba reflejó orientaciones precisas destinadas a impulsar el uso y desarrollo de las Tecnologías de la Información y las Comunicaciones (TIC) en el país y el Gobierno aprueba por primera vez, los Lineamientos Generales para la Informatización de la Sociedad y la forma de implementarlos, pues se concibe el proceso de Informatización de la Sociedad como una de

las tareas más importantes que adopta el Estado Cubano y que demanda del esfuerzo mancomunado de los ministerios y empresas dirigidos por la Oficina de Informatización de la Sociedad, adjunta al Ministerio de Informática y Comunicaciones (MIC), para propiciar todo el desarrollo científico y tecnológico necesario para la implementación de una PKI en el país.

En Cuba el MININT es el máximo responsable del desarrollo y aplicación de la criptografía, es por ello que dentro de la PKI, funge como la Autoridad de Certificación, teniendo la responsabilidad del diseño o evaluación de los algoritmos criptográficos a aplicar y la generación de las llaves tanto simétricas como asimétricas.

La realización de este proyecto se inició con una profunda investigación en la temática de Criptografía Asimétrica, lo que coadyuvó al desarrollo de la estrategia que permitió el diseño, análisis e implementación del Módulo Criptográfico como parte medular de la PKI que actualmente se diseña e implementa en el país.

Esta infraestructura es la encargada de garantizar el ciclo de vida completo del certificado de llave pública, desde el registro del solicitante hasta la entrega de la llave privada y la publicación del certificado digital en el sitio web correspondiente. Estos certificados desempeñan un rol fundamental en la seguridad de las aplicaciones telemáticas, como son la identificación y autenticación y una vez puesto en práctica el resultado de este trabajo de diploma se espera poder usarlos además con fines de autorización. La infraestructura es también la responsable de la creación y actualización de las CRL y de la seguridad y protección de las llaves privadas.

A partir del año 2000 comienza el diseño e implementación en Cuba, por parte del MININT, de una PKI que actualmente se encuentra en período de prueba, esta infraestructura posibilita la obtención, emisión y revocación de certificados digitales que permiten la identificación y autenticación de los usuarios. Su uso fundamental, en estos momentos, está

encaminado a lograr una mayor seguridad en el servicio de correo electrónico. Una vez que esta infraestructura se encuentre funcionando plenamente, está previsto extenderla de forma paulatina a las diferentes esferas de la sociedad cubana y ampliar su uso a sectores como el comercio electrónico, cuyo desarrollo actual se ve frenado por las limitantes de no contar con esta tecnología.

El primer paso de avance importante del MININT como órgano rector de la criptografía en el país fue establecer las regulaciones para el desarrollo de una metodología que permitió evaluar con rigor las tecnologías y módulos criptográficos que se desarrollan en el mundo. Definió el uso de los estándares con desarrollos propios, adecuándolos a las estructuras y condiciones de la sociedad cubana. Así mismo se procedió a la elaboración de los procedimientos, declaraciones de práctica de certificados y las políticas de certificación para la PKI, y actualmente se trabaja en los proyectos de ley para la firma digital y para la implementación de la PKI. (23)

En estos momentos existe un Centro Productor de Llaves Criptográficas para Algoritmos Asimétricos y Emisor de Certificados de Llave Pública, que trabaja con un sistema de protección criptográfica y de gestión de certificados que son desarrollos propios y están sustentados sobre los estándares internacionales: RSA con X 509 v3 y PKCS 12, poniendo en manos de los operadores una tecnología amigable que permite una interacción mínima y segura con el sistema y al mismo tiempo imposibilita el acceso a la información relacionada con las llaves privadas de los usuarios.

Este Centro Productor fue sometido recientemente a la primera prueba real sobre la Red Interna del MININT (RIM) con el fin de comprobar la correcta publicación de los certificados en un sitio de la propia red, el cual permitirá a los usuarios el acceso a los certificados y su uso posterior para los fines con que fueron emitidos, esta prueba también tuvo como objetivo corroborar el flujo productivo en la obtención de las llaves privadas. Como resultado de esta

prueba se detectaron un conjunto de deficiencias relacionadas fundamentalmente con la interacción de los operadores con la aplicación y actualmente se trabaja en la solución de las mismas para la realización de una segunda prueba, a realizarse probablemente en el presente año.

1.4 Certificado X.509

El certificado de llave pública en PKI es definido de acuerdo al estándar X.509. El mismo ha evolucionado para ser más flexible y poderoso y puede ser usado para portar una gran variedad de información, mucha de la cual es opcional. El certificado de llave pública X.509 está protegido por la firma digital del emisor. Los usuarios del certificado saben que el contenido no ha sido corrompido mediante la verificación del mismo. Los certificados contienen un conjunto de campos comunes, y también pueden incluir opcionalmente una variedad de extensiones. A partir del surgimiento del X.509 v3 existen diez campos comunes en los certificados, seis de los cuales son obligatorios y cuatro opcionales. Los campos obligatorios son: número serial, identificador de algoritmo de la firma, nombre del emisor del certificado, período de validez, llave pública, y el nombre del sujeto. Los cuatro campos opcionales son: número de versión, identificadores únicos tanto de emisor como de sujeto, y las extensiones. Los campos opcionales aparecen únicamente en los certificados X.509 v2 y X.509 v3.

1.4.1 Campos básicos del certificado X.509

A continuación se explica de forma detallada la función de cada uno de los campos que componen un certificado digital X.509. (14)

Versión: Identifica la versión del certificado según el estándar X.509. Existen tres versiones de certificados. Cuando el campo de versión es omitido, el certificado está codificado en la versión 1. La versión 1 no incluye identificadores ni extensiones. La versión 2 incluye

identificadores pero no extensiones. En la versión 3 se incluyen las extensiones y es la versión más utilizada en la actualidad.

Número de serie: El número de serie es un número entero asignado por el emisor del certificado. Este número debe de ser único para cada certificado generado por una misma Autoridad de Certificación. La combinación del número de serie y el nombre del emisor identifica únicamente a cualquier certificado.

Firma: El campo de firma indica cual fue el algoritmo de firma digital que fue utilizado para proteger el certificado. Un ejemplo es el tipo de firma utilizado en la infraestructura implementada por el MININT, RSA-con-SHA1. La primera parte identifica al criptosistema de llave pública utilizado mientras que la segunda parte identifica al algoritmo usado para obtener la función resumen del certificado.

Emisor: Este campo contiene el nombre de la entidad que expidió el certificado digital. Este nombre es proporcionado de acuerdo al estándar X.500.

Validez: El campo de validez indica la fecha a partir de la cual el certificado comienza a ser válido y la fecha en la cual el certificado expira.

Sujeto: El campo del sujeto contiene el nombre que identifica al propietario de la llave privada que corresponde con la llave pública que se encuentra en el certificado. El sujeto puede ser cualquier entidad (usuario final, dispositivos de hardware, compañías, aplicaciones, etc.).

Información de llave pública: Este campo contiene la llave pública del sujeto, parámetros opcionales y el identificador del algoritmo.

Identificador único del emisor y del sujeto: Estos campos contienen identificadores, y aparecen únicamente en las versiones 2 ó 3. Los identificadores del sujeto y del emisor son utilizados para la reutilización del nombre del emisor y el nombre del sujeto. Sin embargo, se ha probado que este mecanismo no es una solución satisfactoria.

Extensiones: Este es un campo opcional que permite la adición de nuevos campos a la estructura sin modificar la definición ASN.1; es una secuencia de una o más extensiones de certificados agregadas de acuerdo a las especificaciones del estándar; este campo sólo puede estar presente en certificados X.509 v3. Una extensión está constituida por un identificador de extensión, una bandera de criticidad y un valor específico para la extensión identificada.

1.5 Certificados Digitales SPKI/SDSI

La especificación SPKI/SDSI es el resultado de la unión de dos propuestas surgidas de forma independiente a mediados de la década de los noventa. Tanto el sistema SDSI (*Simple Distributed Security Infrastructure*) como la especificación SPKI (*Simple Public Key Infrastructure*) supusieron en su momento una ruptura drástica respecto a la filosofía del modelo X.509 (1), principalmente en lo que se refería tanto al esquema de asignación de identidades como a la posibilidad de emplear los certificados también con fines de autorización.

SPKI/SDSI se caracteriza por definir tres tipos de certificados diferentes, los cuales contienen al menos un emisor y una entidad receptora (*subject*), y pueden especificar períodos de validez, información de autorización e información de delegación. Dentro de estos están los certificados digitales de autorización, el cual puede hacer referencia a un usuario. Los certificados de autorización se emplean para asignar privilegios directamente a llaves, mientras que los certificados de atributo son útiles para asignar privilegios a grupos de entidades.

1.5.1 Gestión del ciclo de vida de los certificados SPKI/SDSI

La gestión de los certificados digitales, es decir, la forma en la que los usuarios solicitan los certificados, el medio por el cual se distribuyen, o la política de autorización seguida para tal efecto suele ser dependiente del sistema y está implementada de forma demasiado limitada y no distribuida.

Aunque este enfoque puede funcionar correctamente en determinados escenarios, entornos más complejos pueden sacar a relucir ciertas carencias en materia de escalabilidad o interoperabilidad. Conscientes de este hecho, se llevó a cabo el desarrollo de un sistema para la gestión distribuida de certificados SPKI/SDSI denominado DCMS (*Distributed Credential Management System*). DCMS define cómo deben expresarse las solicitudes de certificación, proporciona mecanismos para satisfacer las distintas políticas de seguridad, identifica las entidades involucradas en un escenario de certificación y cómo dichas entidades pueden intercambiar información relativa a autorización. (1)

DCMS constituye una aportación muy valiosa a la definición de sistemas capaces de proporcionar servicios de autorización a la mayoría de escenarios basados en delegación y roles, independientemente del entorno de aplicación en el cual se encuentren éstos ubicados.

Con el fin de ilustrar cuáles han sido los criterios de diseño a la hora de construir DCMS, se mostrará a continuación un entorno de control de acceso basado en delegación, roles y certificados SPKI. El objetivo del estudio de dicho entorno es la extracción de las características comunes a cualquier escenario de control de acceso basado en estos elementos, lo cual justifica la estructura de DCMS.(1)

En estos entornos, los controladores delegan gran parte de su gestión del control de acceso en terceras partes confiables denominadas de forma genérica autoridades de autorización.

De esta forma, la determinación de qué usuarios, o grupos de usuarios, están autorizados a acceder a los recursos se realiza de forma distribuida por parte de cada una de dichas autoridades, las cuales actuarán según lo especificado en su política de autorización. Es decir, se considera que una autoridad de autorización puede ser cualquier entidad final del sistema a la cual se le hayan conferido los privilegios de gestión de un conjunto de recursos por parte del controlador de los mismos.

Una vez que las autoridades de autorización han obtenido la responsabilidad de gestionar un conjunto de los recursos del sistema, deberán proceder con la asignación de tales privilegios al conjunto de entidades correspondientes. Dicho conjunto, dependiente totalmente de la autoridad en cuestión, forma parte de lo que se conoce como la política de autorización de dicha autoridad. La política contiene tanto el conjunto de entidades que pueden recibir los privilegios como qué parte de los mismos y durante qué intervalo de tiempo serán asignados. Es decir, la política de autorización puede verse como una sentencia que especifica cuáles son los certificados que la autoridad estará dispuesta a emitir cuando le sean solicitados.

Es importante recalcar que aunque la autoridad pueda conocer de antemano los certificados que generará en un futuro, no los emite hasta que las entidades involucradas así lo soliciten. Esto evita que, sobre todo en entornos con gran cantidad de usuarios o recursos que proteger, se produzca una generación desmesurada de certificados que conlleve a la emisión y distribución de un porcentaje de autorización es muy superior al que se va a hacer efectivo frente a los controladores. Como consecuencia, la especificación y el cumplimiento de las políticas de autorización es otro de los mecanismos incluidos en el sistema DCMS. Es posible identificar dos tipos de entidades receptoras de los privilegios administrados por una autoridad de autorización. En primer lugar, los privilegios pueden ser asignados a un nombre previamente definido. Este nombre puede hacer referencia a un grupo de usuarios (rol) o bien a un único usuario al cual se le ha asignado un identificador dentro del sistema.

1.6 Modelos de Control de Acceso

Un factor fundamental para determinar el funcionamiento de todo entorno de autorización es la definición del modelo de control de acceso que se va a establecer. Los mecanismos utilizados para restringir el acceso a los recursos son generalmente de una (o muchas veces la combinación) de dos formas:

Control de Acceso Discrecional (DAC): Le deja las decisiones de control de acceso al propietario del recurso, de manera que es él/ella quien decide qué sujetos pueden realizar determinadas acciones sobre los recursos poseídos. (10) Así, un sujeto con permisos de acceso puede otorgarlos (quizás indirectamente) a otro sujeto.

Control de Acceso Obligatorio (MAC): Este control de acceso se basa en las reglas establecidas por una autoridad central. MAC restringe el acceso a los objetos basándose en la sensibilidad de la información que estos contienen (representada por una etiqueta) y en la autorización formal de los sujetos para acceder a dicha información (10). Los objetos son considerados como entidades pasivas que almacenan información, mientras que los sujetos son entidades activas que realizan peticiones de acceso a los objetos.

Existen diversos modelos de control de acceso de tipo DAC y/o MAC. Los más usados se listan a continuación, argumentando en cada caso la factibilidad de su uso:

Control de Acceso Basado en Identidad (IBAC): En este caso, los permisos de acceso a un recurso se asocian directamente al identificador del sujeto (es decir, el nombre del usuario). Por tanto, se garantiza el acceso al recurso sólo cuando existe dicha asociación.

Con IBAC no se asocian etiquetas de seguridad a los usuarios, por lo que éste es primordialmente un mecanismo de control de acceso discrecional. Un ejemplo de IBAC son las Listas de Control de Acceso (ACL) (24), encontradas comúnmente en sistemas

operativos y servicios de seguridad en red. Una ACL contiene los identificadores de los usuarios junto con sus derechos de acceso a un recurso determinado, como leer, escribir, ejecutar, etc. Esta estructura básica de autorización únicamente extiende el concepto de autenticación, pues si el usuario no puede autenticarse correctamente ante el guardián del recurso, su solicitud de acceso es denegada.

Como se puede inferir en la medida en que se incremente el número de usuarios que soliciten el acceso a un recurso, más identificadores contendrá la ACL, lo que dificulta enormemente el manejo de estas listas y las hace una alternativa poco escalable. Por otra parte, la decisión de control de acceso no depende de alguna función o característica de la organización a la que pertenece el usuario sino solamente de los identificadores, es por ello que el uso de IBAC resultaría inapropiado e ineficiente en los entornos de seguridad en los que esta enfocado el presente trabajo.

Control de Acceso Basado en Roles (RBAC): Restringe el acceso a los recursos basándose en la función o rol que desempeña el sujeto dentro de la organización. Los permisos para acceder a un recurso son asignados a cada rol, en lugar de asociarlos directamente al identificador del sujeto.

Este modelo de control de acceso es altamente recomendado considerando que se asigna un conjunto de privilegios a cada rol, y uno o varios roles a cada usuario. De esta forma se desvinculan los privilegios del usuario de su identidad local, lo que permite un control de acceso más flexible y dinámico. Además es importante tener en cuenta que el RBAC es escalable y reduce significativamente la cantidad de información de administración necesaria, pues los permisos no son asignados constante e individualmente a los usuarios. RBAC es primordialmente un mecanismo de control de acceso discrecional.

Control de Acceso Basado en Atributos (ABAC): En ABAC, los privilegios son establecidos en base a la colección de atributos que posee el usuario y una política que los determina. ABAC es la convergencia natural de los modelos de control de acceso IBAC y RBAC. La representación de las políticas en ABAC es semánticamente más rica y expresiva. Además, posee una mayor granularidad pues puede basarse en cualquier combinación de atributos de sujeto, de recursos y de entorno. De esta forma para conceder el acceso a un recurso es indispensable que la aplicación o sistema accedido verifique y compruebe en la política de control de acceso correspondiente si el usuario tiene los privilegios suficientes para acceder al recurso solicitado.

1.7 Conclusiones

El desarrollo de la Infraestructura de Llave Pública es un camino acertado para alcanzar la seguridad indispensable de una Sociedad Informatizada, la inserción en la actual globalización de la información es ya una realidad, que requiere crear las condiciones de una tecnología con una base científica y adecuadamente sustentada en políticas de seguridad.

La certificación de autorización ofrece una nueva gama de servicios orientados a complementar las funciones básicas de las infraestructuras de llave pública. En este sentido, cobra especial importancia aportar soluciones tanto en el campo de la gestión de este tipo de certificados como en el de su integración en escenarios de aplicación reales.

CAPÍTULO 2: Descripción de la Solución Propuesta

2.1 Introducción

La autenticación permite comprobar la identidad de los usuarios. La autorización (o control de acceso) establece con qué facultades cuenta el usuario sobre el recurso ante el cual se autentica. Estos dos conceptos, que a menudo se mezclan de manera difusa, son completamente independientes. Sin embargo, especialmente cuando se accede a un recurso de información a través de la red, sin protección física, estas dos actividades irán siempre ligadas. Los certificados digitales de autorización descritos en este capítulo, propiciarán que en el momento en que una entidad acceda a un recurso, pueda verificarse no solo la identidad de dicha entidad sino también los privilegios o permisos que le han sido conferidos.

2.2 ASN.1 (Abstract Syntax Notation One)

El propósito de esta sección es brindar una breve introducción a la Notación de Sintaxis Abstracta Uno (ASN.1) para así poder entender de una mejor forma la generación de los certificados digitales X.509.

ASN.1 es una notación usada para describir formalmente la semántica de datos transmitidos a través de una red. (3) Las diferentes entidades que se comunican en un sistema distribuido pueden tener diferentes representaciones de sus respectivos tipos de datos; por ejemplo, el número de bits requeridos para representar un número flotante. Debido a esto, es importante tener una forma de describir datos de una manera que sea independiente de la representación particular de cada sistema.

Entre las principales cualidades de ASN.1 se encuentran las siguientes:(25)

- Es un estándar internacional, independiente de plataformas, de vendedores, y de notaciones de lenguaje.

- Es soportado por reglas, las cuales determinan los patrones de bits exactos para representar los valores de las estructuras de datos cuando estas tienen que ser transferidas sobre una red de computadoras.
- Es soportado por herramientas disponibles para muchas plataformas (Unix, Linux, Win32, etc.) y varios lenguajes de alto nivel mapean la notación ASN.1, a través de un compilador, en estructuras de datos definidas en el lenguaje de programación de elección; por ejemplo, C++, Java, Pascal, etc.
- ASN.1 proporciona una gama de estructuras de datos que generalmente resulta mucho más abarcadora que la de los lenguajes de programación genéricos, tales como tamaño de enteros, asignación de nombre a estructuras, tipos de caracteres y tipos de cadenas.

Para poder explicar de una forma intuitiva el lenguaje ASN.1 se considera el siguiente ejemplo:

```
Rectangulo ::= SEQUENCE {
    alto INTEGER,
    ancho INTEGER
}
```

La especificación ASN.1 anterior, describe un tipo de dato construido denominado *Rectangulo*, el cual contiene dos campos enteros. Esta especificación es una clase de estructura de dato que cualquier entidad puede enviar o recibir dentro de un sistema distribuido. Por ejemplo, *Rectangulo* puede ser codificado y enviado a un destino utilizando el protocolo TCP (*Transmission Control Protocol*,). Para que la especificación de *Rectangulo*

sea procesada por un compilador ASN.1 y se genere el código fuente en el lenguaje de programación deseado, se debe insertar en un módulo de la siguiente forma:

```
EjemploModulo1
{ iso org(3) dod(6) internet(1) private(4)
enterprise(1) spelio(9363) software(1)
asn1c(5) docs(2) usage(1) 1 }

DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

-- Este es un comentario
Rectangulo ::= SEQUENCE {
alto INTEGER,
ancho INTEGER
}

END
```

El módulo consiste en un encabezado, el cual es su propio nombre (EjemploModulo1), el OID definido entre llaves y que es explicado en la siguiente sección de este capítulo; DEFINITIONS que es una palabra reservada de ASN.1 al igual que AUTOMATIC TAGS. La sentencia ::= BEGIN, indica el inicio del las definiciones ASN.1, mientras que la sentencia END finaliza el módulo.

A continuación se explican brevemente los tipos de datos ASN.1 más utilizados en la generación de certificados X.509.(25)

2.2.1 Tipos de datos básicos en ASN.1

2.2.1.1 Tipo BOOLEAN

El tipo BOOLEAN es utilizado para la representación de valores binarios (CIERTO/FALSO, ENCENDIDO/APAGADO, SI/NO, etc.). En este trabajo de diploma se utiliza este tipo de dato para especificar el valor de la bandera de criticidad de la extensión particular definida para el certificado digital X.509 v3.

2.2.1.2 Tipo INTEGER

El tipo INTEGER es usado para representar números enteros sin restricción en su tamaño. Los siguientes son ejemplos de las diferentes formas de definir un entero en ASN.1:

```
EnteroSimple ::= INTEGER -- entero sin restricciones
EnteroPositivo ::= INTEGER (0..127) -- entero con longitud limitada
EnteroNegativo ::= INTEGER (MIN..0) -- entero negativo
```

El tipo INTEGER es utilizado en la generación del certificado X.509 para especificar el número de serie del certificado expedido por la Autoridad de Certificación.

2.2.1.3 Tipo ENUMERATED

Este tipo es el equivalente semántico al tipo INTEGER pero con valores enteros explícitamente nombrados. Ejemplo:

```
TipoDeCertificadoX509 ::= ENUMERATED {
Version1, -- adquiere el valor 0
Version2, -- adquiere el valor 1
Version3 -- adquiere el valor 2 }
```

2.2.1.4 Tipo OCTET STRING

Este tipo de dato permite representar secuencias de bytes, las cuales pueden ser utilizadas para transmitir datos serializados a través de un sistema distribuido; por ejemplo, archivos de video, imágenes, voz, etc.

2.2.1.5 Tipo BIT STRING

Este tipo de dato permite la representación de cadenas de bits y es principalmente utilizado para aplicaciones de seguridad. En este caso particular, se utiliza el tipo BIT STRING para la representación de las firmas digitales generadas por el algoritmo RSA.

2.2.1.6 Tipo IA5String

Este tipo de cadena está compuesto por caracteres ASCII. Cada carácter utiliza los siete bits menos significativos de un byte; por lo cual, existen 128 caracteres diferentes. En el certificado X.509 se utiliza este tipo para las direcciones de correo electrónico tanto de la entidad final como la entidad emisora.

2.2.1.7 Tipo PrintableString

Este es un tipo de cadena que cuenta únicamente con un alfabeto imprimible. Este alfabeto está compuesto por los siguientes caracteres: "'", "(", ") ", "+ ", ", ", "- ", ". ", "/ ", dígitos ("0 "... "9 "), ": ", "= ", "? ", letras mayúsculas y minúsculas ("A "... "Z"y "a "... "Z").

El tipo de dato PrintableString es utilizado para especificar el nombre de la entidad final y la entidad emisora.

2.2.1.8 Tipo UTCTime

Este tipo de dato permite la manipulación de la fecha y hora. Los valores que puede tomar este tipo de dato son cadenas de caracteres del siguiente tipo:

yymmddhhmmZ
yymmddhhmmssZ
yymmddhhmm+hhmm
yymmddhhmm-hhmm
yymmddhhmmss+hhmm
yymmddhhmmss-hhmm

"yymmdd" representa el año (00 ... 99), mes (01 ... 12), día (01 ... 31), y "hhmmss" son horas (00 ... 23), minutos (00 ... 59), segundos (00 ... 59).
La "Z"es usada comúnmente como sufijo que indica que los valores fueron tomados de acuerdo al GMT (Greenwich Mean Time). Si está presente el "+hhmm" o el "-hhmm" entonces el tipo de dato expresa un valor de tiempo local y está referenciado al GMT.

2.2.1.9 Tipo OID (OBJECT IDENTIFIER)

El OID es usado para representar un identificador único de cualquier objeto. Es quizás el más usado de los tipos de datos básicos de ASN.1. Por ejemplo, el OID que identifica el algoritmo de firma digital con RSA y SHA-1 es el siguiente:

sha-1WithRSAEncryption OBJECT IDENTIFIER ::=

{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}

2.2.2 Estructura de datos construidos

Existe una gran variedad de datos construidos pero en esta sección sólo se mencionan los que son utilizados en la generación de certificados digitales X.509.

2.2.2.1 Tipo SEQUENCE

Este tipo representa una colección ordenada de otros tipos de datos diferentes ya sean simples (INTEGER, BOOLEAN, PrintabeString, etc.) o construidos. El tipo de dato construido SEQUENCE es muy similar a la sentencia *struct* del lenguaje C.

2.2.2.2 Tipo SEQUENCE OF

Es una lista ordenada de tipos de datos iguales. Es similar al tipo SEQUENCE, la diferencia consiste en que todos los datos tienen que ser del mismo tipo. Por ejemplo:
MuchosRectangulos ::= SEQUENCE OF Rectangulo

2.2.2.3 Tipo SET

Al igual que el tipo SEQUENCE, este es una colección de tipos simples o complejos con la particularidad que el orden no es importante.

2.2.2.4 Tipo CHOICE

Este tipo permite la elección entre varios subtipos especificados. El siguiente ejemplo define un tipo de código de respuesta, el cual puede ser un entero o un valor binario.

```
CodigoDeRespuesta ::= CHOICE {
codigoEntero INTEGER,
codigoBoleano BOOLEAN
}
```

2.2.3 Descripción de la sintaxis ASN.1 de un certificado X.509 v3

Un certificado X.509 v3 es definido mediante ASN.1 de la siguiente forma:

```
Certificate ::= SEQUENCE {
    tbsCertificate          TBSCertificate,
```

```
    signatureAlgorithm    AlgorithmIdentifier,
    signatureValue        BIT STRING
}
```

Para el cálculo de la firma digital, los datos firmados deben de estar codificados usando ASN.1 DER (*Distinguished Encoding Rules*). La codificación ASN.1 DER está basada en etiquetas, longitud de campos y codificación de valores para cada elemento.

2.2.3.1 Tipo tbsCertificate

El campo tbsCertificate contiene los nombres de la entidad final y el emisor, la llave pública asociada a la entidad final, un período de validez, extensiones, versión, número serial, entre otros campos. A continuación se muestra la sintaxis para este tipo de dato compuesto.

```
TBSCertificate ::= SEQUENCE {
    version                 [0]  EXPLICIT Version DEFAULT v1,
    serialNumber                 CertificateSerialNumber,
    signature                    AlgorithmIdentifier,
    issuer                       Name,
    validity                     Validity,
    subject                      Name,
    subjectPublicKeyInfo         SubjectPublicKeyInfo,
    issuerUniqueID          [1]  IMPLICIT UniqueIdentifier OPTIONAL,
                                 -- si está presente la versión DEBE ser v2 o v3
    subjectUniqueID         [2]  IMPLICIT UniqueIdentifier OPTIONAL,
                                 -- si está presente la versión DEBE ser v2 o v3
    extensions              [3]  EXPLICIT Extensions OPTIONAL
                                 -- si está presente la versión DEBE ser v3
    }
```

Como se puede observar el tipo de dato tbsCertificate está compuesto a su vez, por más tipos de datos compuestos. A continuación se listan algunos de estos campos.

```
Version ::= INTEGER { v1(0), v2(1), v3(2) }
CertificateSerialNumber ::= INTEGER

Validity ::= SEQUENCE {
    notBefore      Time,
    notAfter       Time }

Time ::= CHOICE {
    utcTime        UTCTime,
    generalTime    GeneralizedTime }
UniqueIdentifier ::= BIT STRING

SubjectPublicKeyInfo ::= SEQUENCE {
    algorithm            AlgorithmIdentifier,
    subjectPublicKey     BIT STRING }

Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension
Extension ::= SEQUENCE {
    extnID       OBJECT IDENTIFIER,
    critical     BOOLEAN DEFAULT FALSE,
    extnValue    OCTET STRING }
```

2.2.3.2 Tipo signatureAlgorithm

El campo *signatureAlgorithm* contiene el identificador para el algoritmo criptográfico usado por la autoridad certificadora para firmar el certificado. El RFC-3279 lista los algoritmos soportados. La sintaxis ASN.1 es la siguiente:

```
AlgorithmIdentifier ::= SEQUENCE {
    algorithm           OBJECT IDENTIFIER,
    parameters          ANY DEFINED BY algorithm OPTIONAL }
```

El identificador de algoritmo es usado para identificar el algoritmo criptográfico. El componente OBJECT IDENTIFIER identifica el algoritmo (como RSA con SHA-1). El contenido del campo optativo de parámetros diferirá según el algoritmo identificado. El identificador de algoritmo contenido en este campo debe ser el mismo que el contenido en el campo *signature* en la secuencia *tbsCertificate*.

2.2.3.3 Tipo signatureValue

El campo *signatureValue* contiene la firma digital del *tbsCertificate*. La codificación ASN.1 DER del *tbsCertificate* es usada como entrada para la función de firma de la Autoridad de Certificación. El valor resultante es codificado como BIT STRING e incluido en el campo de firma del certificado X.509.

Generando esta firma, la Autoridad de Certificación certifica la validez de la información contenida en el campo *tbsCertificate*. En particular, la Autoridad de Certificación certifica la unión entre el la llave pública y el sujeto del certificado.

2.3 OID

Los identificadores de objeto se utilizan fundamentalmente para identificar objetos en Internet como políticas de certificación, extensiones de certificados digitales, algoritmos de cifrado, clases de objeto, tipos de atributos, aplicaciones, recursos, entre otros. De esa manera se pueden ser usados posteriormente para referenciar los objetos identificados ya sea en protocolos o en otras especificaciones que una organización crea conveniente dar a conocer.

La distribución de los OID se define como una estructura de árbol que asegura que cada objeto está representado como un nodo, los nodos que conforman el árbol están dispuestos en forma jerárquica. Cada nodo es representado con un número entero y tiene sólo un nodo superior pero puede tener tantos nodos subordinados como resulte necesario. El OID de un objeto es la concatenación de los números enteros (a modo de ejemplo, una secuencia del tipo 2.16.192.1) a través de la ruta desde la raíz del árbol (que es el nodo del que parte la secuencia numérica) hasta el nodo del objeto en cuestión. Una vez que una organización dispone de una rama, dicha organización puede establecer su propia jerarquía de asignaciones según sus intereses concretos.

Los Identificadores de Objeto se utilizan en gran variedad de protocolos, aunque es importante señalar que actualmente los usos más comunes son los siguientes:

- Objetos y atributos que se gestionan vía SNMP (*Simple Network Management Protocol*).
- Identificación de objetos en la red.
- Árboles de indexación en CIP (Common Indexing Protocol)
- Elementos dentro de una PKI: Identificación unívoca de Autoridades de Certificación, Políticas de Certificación y Declaraciones de Práctica de Certificados, atributos, nuevas extensiones, etc.

En este caso serán usados con dos fines específicos el primero vinculado a la identificación de elementos dentro de una PKI, pues se definirá una extensión privada que precisa la asignación de un OID para el valor del identificador de la extensión y el segundo relacionado con la identificación de objetos en la red.

2.3.1 Identificadores de Objeto existentes

La raíz del árbol contiene los tres "arcos" siguientes:

0: ITU-T

1: ISO

2: joint-iso-itu-t

El arco correspondiente a la joint-iso-itu-t cuyo nodo raíz es (2) tiene la identificación de cada país a partir de la rama 2.16 (*Country assignments*), a partir de ella han sido asignados un conjunto de nodos de los cuales cada uno corresponde a un país o estado independiente y pueden ser usados para asignar identificadores dentro de estos territorios. Es decisión del país en cuestión la asignación de la responsabilidad del registro de los OID a una autoridad capaz de desempeñar esta función.

Una vez que se dispone de un OID asignado por alguna de las agencias registradoras existentes, se tiene el derecho de asignar libremente esa rama de la jerarquía según los intereses concretos de la organización en cuestión.

Actualmente en Cuba no existe ninguna autoridad o entidad encargada de la asignación y registro de los arcos subsiguientes al 2.16.192 que es el que le corresponde al país de acuerdo con la estructura "joint ISO-ITU/T" siendo el 192 el nodo que identifica a Cuba. Tanto ISO como ITU-T brindan otras estructuras de OID distintas a la que se propone sea utilizada por Cuba, a través de sus nodos raíces (0) y (1), respectivamente.

Por resultar necesario para el desarrollo de este trabajo de diploma se asumirá una jerarquía en la que se definirán solamente aquellos arcos que sean imprescindibles para la descripción y correcto entendimiento de la solución planteada (Ver Fig. 2.1), no obstante, se recomienda que por el beneficio que se deriva del uso de este tipo de identificadores se establezca cuanto antes una autoridad encargada de la gestión y control de los mismos en el país. Esta autoridad sólo tendría que asignar las ramas inmediatas a la 2.16.192, es decir, aquellas cuya estructura sería 2.16.192.X, una vez hecho esto las organizaciones, ministerios o entidades que formen parte de este nivel de jerarquía son las encargadas y únicas responsables de la distribución de los niveles inferiores, no obstante cada OID que sea asignado debe ser registrado con la autoridad encargada de estas gestiones, la cual debe garantizar la unicidad de cada OID. Como parte de la jerarquía de OID definida se ha asignado el 2.16.192.3 para la identificación de los ministerios y a partir de este el 2.16.192.3.2 le corresponde al MININT y el 2.16.192.3.2.5 y el 2.16.192.3.2.50 se han asignado al DICC y a la PKI respectivamente.

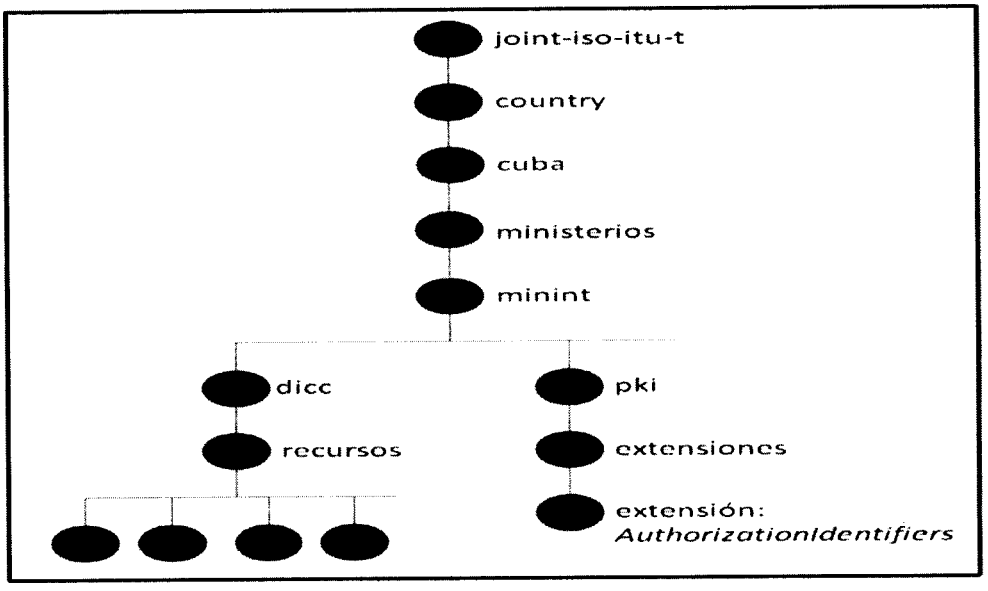


Fig. 2.1 Estructura propuesta para la asignación de los OID en Cuba.

La jerarquía descrita no es obligatoria sino que puede ser modificada para responder a las necesidades específicas ya sea del país, del MININT o de las unidades organizativas de este ministerio involucradas en esta distribución.

Se asumirá una política de asignación de OID para el MININT dentro su rango privado de numeración, de esta forma el OID correspondiente a la PKI sería el 2.16.192.3.2.50 es de por la cual el OID de cualquier extensión particular definida para los certificados digitales comenzará con el prefijo 2.16.192.3.2.50.2 por ser esta la primera extensión que se define será identificada con el OID 2.16.192.5.50.2.1 y la representación del mismo según la notación ASN.1 seria la siguiente:

{ joint-iso-itu-t(2) country(16) cu(192) min(3) minint(2) pki(50) extPriv(2)
authorizationIdentifiers(1) }

Para la identificación de los recursos se debe asignar un OID a cada uno de los mismos, independientemente de su naturaleza, y una vez asignado el identificador al recurso se debe asociar un identificador a cada uno de los niveles de acceso con que cuente el recurso en cuestión, en cada recurso se pueden definir tantos niveles de acceso como se considere necesario, de esta forma siguiendo la jerarquía que se había planteado anteriormente se adjudica la rama 2.16.192.3.2.5 al DICC y de esta se deriva la 2.16.192.3.2.5.10 a partir de la cual serán identificados los recursos de este departamento cuyo control de acceso se realizará mediante el uso de certificados digitales de autorización, las ramas subsiguientes serán asignadas a cada recurso específico de manera que siendo 2.16.192.3.2.5.10.6 el OID del recurso "X" entonces 2.16.192.3.2.5.10.6.0 sería el OID del máximo nivel de acceso al recurso "X".

2.4 Definición de una Extensión Privada

La solución que se plantea en el presente trabajo de diploma para resolver el problema de la incorporación de información referente a autorización en el certificado digital está basada en el aprovechamiento de la más significativa utilidad del estándar X.509 v3, la cual está dada por su eficiente campo de extensiones, definido únicamente para esta versión de los certificados, y que da la posibilidad de que el contenido de los mismos pueda ser adaptado fácilmente para responder a las necesidades específicas de la PKI implementada por el MININT, puesto que dicho campo permite añadir información adicional al certificado a través del conjunto de extensiones estándar definidas con este fin, así como también permite a las comunidades definir extensiones privadas para reflejar información única para las mismas.

De acuerdo con lo establecido en la RFC-3280 (14) el campo de extensión esta constituido por una o más extensiones y cada extensión a su vez está compuesta por un identificador de extensión (*extnID*), una bandera de criticidad (*critical*) y una codificación de un valor de datos (*extnValue*) asociado con la extensión identificada. La definición estándar del campo de extensiones del certificado digital X.509 v3 es la siguiente:

```
Extensions  ::=  SEQUENCE SIZE (1..MAX) OF Extension
  Extension  ::=  SEQUENCE  {
      extnID        OBJECT IDENTIFIER,
      critical      BOOLEAN DEFAULT FALSE,
      extnValue     OCTET STRING
}
```

A partir de los argumentos anteriores se determinó que la solución más apropiada la constituye la incorporación de una extensión privada, que se incluirá en aquellos certificados que serán emitidos por la Autoridad de Certificación, conteniendo información sobre las facultades de su propietario y que posteriormente serán usados con fines en los que se

precise no sólo identificar al propietario del certificado, sino también determinar si el mismo cuenta con las potestades necesarias para acceder a una determinada aplicación, servidor o cualquier otro tipo de recurso, cuya seguridad esté basada en el uso de los certificados digitales de autorización para determinar si los privilegios de acceso con que cuenta el usuario sobre el recurso accedido son suficientes para ejecutar las acciones que solicite el usuario.

La extensión privada en la que se incorporará la información referente a los niveles de acceso del usuario del certificado digital de autorización denominada *AuthorizationIdentifiers* tendrá una estructura similar a la definida en el estándar X.509, la diferencia fundamental radicará en que el campo correspondiente al valor de la extensión no contendrá un valor de tipo OCTET STRING sino que estará definido como una secuencia de OID, en la que cada OID representa un permiso o privilegio del poseedor del certificado.

Siguiendo la notación ASN.1 la extensión *AuthorizationIdentifiers* queda definida de la manera siguiente:

id-cu-min-minint-pki-extPriv-authorizationIdentifiers OBJECT IDENTIFIER ::=
{ id-cu-min-minint-pki-extPriv 1 }

AuthorizationIdentifiers ::= SET SIZE(1..MAX) OF AuthorizationIdentifier
AuthorizationIdentifier ::= OBJECT IDENTIFIER

El valor del identificador de extensión permite identificar de forma única la extensión en cuestión es por ello que un certificado no debe incluir más de una instancia de una misma extensión, por ejemplo un certificado puede contener sólo una extensión de tipo *AuthorizationIdentifiers.*

Por su parte el valor de la bandera de criticidad desempeña un papel fundamental en la validación de un certificado puesto que cuando una aplicación está procesando un certificado y no reconoce una extensión, si la bandera de criticidad es FALSO, la extensión puede ser ignorada y el certificado considerado válido, sin embargo si la bandera de criticidad esta marcada como VERDADERO, extensiones no reconocidas harán que la estructura se considere no válida, es decir, en un certificado, una extensión crítica no reconocida provocará el fracaso de la validación del certificado en cuestión. Ahora bien, cuando una aplicación que intenta procesar un certificado reconoce y es capaz de comprender una extensión, la procesará independientemente del valor de la bandera de criticidad.

En el caso particular de la extensión *AuthorizationIdentifiers* se establece que la misma sea marcada como no crítica pues independientemente de que su valor influirá de forma definitiva en la determinación de la concesión o no del acceso al propietario del certificado digital de autorización y sobre todo en qué medida le será conferido el acceso, se define de esta forma tomando en consideración que todas aquellas aplicaciones, procesos, sistemas y/o recursos que precisen el uso de este tipo de certificados para su correcto funcionamiento contarán con las funcionalidades requeridas para la comprensión y el procesamiento de esta nueva extensión. Además de esta forma se evita que aquellos sistemas que no sean capaces de procesar la extensión rechacen el certificado, es decir, que si bien este certificado digital de autorización sólo cumplirá su objetivo, en cuanto a autorización se refiere, cuando sea empleado en las aplicaciones del MININT, por otra parte puede ser usado por su propietario para autenticarse ante cualquier aplicación que utilice esta tecnología para la autenticación de los usuarios. De marcarse esta extensión como crítica, se estaría limitando el conjunto de aplicaciones que serían capaces de procesar un certificado digital de autorización pues cuando un sistema que no forme parte de la infraestructura del MININT intente validar el certificado lo rechazará inmediatamente al no reconocer una extensión marcada como crítica e impediría la autenticación del usuario.

El valor de la extensión *AuthorizationIdentifiers* estará definido por una secuencia de OID, cada uno de los cuales representará un privilegio o permiso de la entidad poseedora del certificado. Estos OID deben ser definidos teniendo en cuenta las especificaciones planteadas en la sección anterior.

2.4.1 Pasos para la obtención de un Certificado Digital de Autorización

Para que un usuario obtenga un Certificado Digital de Autorización, debe seguir esencialmente los siguientes pasos: el usuario se presenta personalmente ante la entidad de registro con la documentación necesaria para la creación del certificado, el usuario debe presentar un documento firmado por una persona con la facultad requerida para conceder los permisos en cuestión. Este documento será el que confirme que se le pueden asignar al usuario los privilegios que solicita, es responsabilidad de la Entidad de Registro comprobar la veracidad de los datos que presenta el usuario.

Después que la Entidad de Registro confirma la legitimidad de la documentación presentada, solicita a la Autoridad de Certificación que emita el certificado. La Autoridad de Certificación, es el órgano responsable de la emisión de los certificados una vez realizada la verificación por parte de la Entidad de Registro por los métodos que considere en sus Políticas de Certificación, el Centro Productor de Llaves para Algoritmos Asimétricos y Certificados Digitales es el proveedor de la tecnología criptográfica para la creación de las llaves y el encargado de publicar los certificados emitidos a favor de entidades pertenecientes a este ministerio, cuya publicación se realizaría en un sitio web de la RIM.

Una vez concluida la generación y emisión del certificado el usuario debe personarse en la entidad de registro para recoger su llave privada, la cual le es entregada en un dispositivo de almacenamiento, en estos momentos el sistema con el que se cuenta para realizar la entrega está preparado para grabar la llave en cualquier tipo de dispositivo, por ejemplo una memoria flash, un disco de 3½, un disco compacto, etc.

En caso de que el certificado digital de autorización que se solicite no sea para una persona física sino para otro tipo de usuario, entiéndase un servidor, una aplicación o cualquier otro recurso, la solicitud para la obtención del certificado debe ser realizada o autorizada por el máximo responsable de las facultades a asignar, la Entidad de Registro debe validar esta información y se deben extremar las medidas de seguridad para la entrega de llave privada.

La Autoridad de Certificación es la encargada de verificar constantemente la validez y autenticidad de los certificados que distribuye.

2.4.2 Validación y Revocación del Certificado Digital de Autorización

En el caso de los certificados digitales de autorización la validación es un proceso que cobra especial importancia pues los permisos conferidos al propietario del certificado pueden expirar o cambiar con una frecuencia mayor que la información sobre la identidad de su poseedor. La validación puede ser realizada de dos formas "en línea" o "fuera de línea" en dependencia de si se establece o no una conexión directa con la Autoridad de Certificación en el momento de realizar este proceso. Estrechamente vinculado al proceso de validación está el de revocación del certificado, que es la forma que tiene la entidad que intenta comprobar la validez del mismo de conocer si dicho certificado ya no es válido y por lo tanto no puede ser utilizado.

La PKI implementada por el MININT, en estos momentos, realiza la validación fuera de línea mediante el uso de las CRL, y tiene en desarrollo el uso del protocolo OCSP (*Online Certificate Status Protocol*), que permitirá la validación en línea de los certificados, lo cual resulta imprescindible para la extensión del uso de los certificados digitales a aplicaciones de comercio electrónico y para la transferencia bancaria. Es importante señalar que si bien los certificados digitales de autorización pueden ser empleados a pesar de realizarse la validación fuera de línea lo más recomendable es la realización de este proceso en línea.

Para realizar la validación fuera de línea de un certificado digital de autorización el verificador debe descargar una CRL actualizada desde el repositorio de la Autoridad de Certificación que emitió el certificado digital de autorización en cuestión. A continuación comprueba la autenticidad de la lista haciendo uso de la firma digital de la Autoridad de Certificación. Después debe comprobar si el número de serie del certificado cuestionado está en la lista. En caso afirmativo, no se debe aceptar el certificado como válido. Estrictamente hablando, no es necesario descargar una CRL cada vez que se verifica un certificado. Solamente es necesario cuando la lista de la que se dispone tiene una cierta antigüedad que aconseja su renovación o si se conoce de la publicación de una lista actualizada.

Si bien las CRL tienen a su favor el hecho de que se pueden consultar sin necesidad de una conexión de datos permanente con la Autoridad de Certificación, pues basta establecer dicha conexión con cierta periodicidad para descargar la CRL actualizada, el empleo de las mismas implica una serie de riesgos que desaconsejan su uso, especialmente para la validación de los certificados digitales de autorización cuyo estado puede variar periódicamente debido a que los permisos y privilegios de los usuarios pueden ser modificados con cierta frecuencia, algunos de estos inconvenientes se relacionan a continuación:

- Existe el peligro de que un certificado haya sido revocado, pero no aparezca en la CRL del tercero que comprueba su validez. Esto se debe a que la CRL utilizada podría no estar actualizada.

- Durante el tiempo que media entre la revocación de un certificado y la actualización y publicación de la CRL correspondiente el propietario podría hacer uso del mismo, independientemente del cese de sus facultades, esto acarrearía significativas brechas en la seguridad de las aplicaciones y servicios que hagan uso de estos certificados ya sea para controlar el acceso a los recursos o para tomar cualquier otro tipo de decisión que implique la validación del certificado digital de autorización.

- De existir responsabilidad legal por el uso de un certificado revocado, no hay forma de demostrar quién es el culpable: el tercero por no comprobar la validez, o la Autoridad de Certificación por no incluirlo en la CRL a tiempo.
- El tamaño de la CRL solamente tiende a crecer, resultando ineficientes para su tratamiento directo.

Teniendo en cuenta estos argumentos se recomienda la validación en línea de los certificados digitales de autorización, de forma que se pueda conocer en tiempo real el estado de los mismos. No obstante este procedimiento presenta la dificultad de que se requiere de conexión con la Autoridad de Certificación cada vez que se precise comprobar la validez de un certificado de atributos, pero si bien la CRL está disponible sin conexión, mientras más tiempo esté sin actualizarse, se hace menos confiable la información que brinde, porque pueden haber sido revocados otros certificados desde que se produjo la actualización de la lista.

Son varias las razones por las que se recomienda el uso de la validación en línea sobre el uso de las CRL, algunas de ellas se listan seguidamente. La validación en línea:

- Puede proporcionar información más adecuada y reciente del estado de revocación de un certificado digital de autorización.
- Elimina la necesidad de que quien necesite comprobar la validez de un certificado tenga que obtener y procesar la CRL, ahorrando de este modo tráfico de red y procesado por parte del verificador.
- Una consulta sobre el estado de un certificado sobre una CRL, debe recorrerla completa secuencialmente para determinar si es válido o no, esto resulta extremadamente costoso en tiempo de ejecución y se manifiesta aún más cuando el tamaño de la CRL es muy grande.

Actualmente el protocolo más extendido para la realización de la validación en línea es el OCSP, el cual fue propuesto por el IETF (*Internet Engineering Task Force*) en 1999 y se describe en el RFC-2560. Los mensajes OCSP se basan en mecanismos de solicitud/respuesta, se codifican en ASN.1 y habitualmente se transmiten sobre el protocolo HTTP (*HyperText Transfer Protocol*). La naturaleza de las peticiones y respuestas de OCSP hace que a los servidores OCSP se les conozca como "*responder* OCSP". Para conocer el estado de revocación de uno o más certificados, el verificador envía su solicitud al responder OCSP este puede devolver una respuesta firmada que contiene el estado de revocación de los certificados, junto con sus respectivos identificadores y el intervalo de validez de dicha respuesta. Esta respuesta va firmada digitalmente por el responder OCSP. El estado *good* significa que el certificado no ha sido revocado, pero puede no haber sido expedido todavía o que la respuesta se expidió fuera de su período de validez. El estado *revoked* significa que el certificado se ha revocado y el estado *unknown* significa que el responder no tiene información sobre el certificado requerido. También puede devolver un código de error, en cuyo caso la respuesta no tendría que estar firmada.

En sentido general la validación de un certificado digital de autorización involucra esencialmente los siguientes pasos:

Verificación de la Validez del Certificado: Constituye el paso básico para la validación del certificado, consiste en confirmar si el certificado ha expirado o ha sido revocado. La expiración se comprueba con el período de validez del certificado, y la verificación del estado de revocación depende del mecanismo de revocación utilizado.

Verificación de Firma Digital: Consiste en comprobar la firma digital del certificado recuperado. La Autoridad de Certificación tiene la responsabilidad de firmar digitalmente cada uno de los certificados que expide. Así, para validar la firma de un certificado, el

verificador debe conocer la llave pública de la autoridad que emitió dicho certificado y llevar a cabo los siguientes pasos:

1. Descifrar, con la llave pública de la Autoridad de Certificación correspondiente, la parte firmada del certificado.

2. Aplicar una función resumen sobre el contenido del certificado.

3. Comparar los resultados obtenidos en 1 y 2. Si coinciden, la firma es válida y el verificador puede confiar en el contenido del certificado.

De existir varias Autoridades de Certificación, lo cual podría resultar necesario y conveniente a largo plazo si se produce un incremento considerable de la cantidad de usuarios que hacen uso de los servicios de la PKI, el proceso de validación de los certificados digitales de autorización requeriría además los pasos siguientes:

Construcción del Camino de Certificación: Consiste en el establecimiento de un camino confiable entre el verificador y la entidad objetivo, a través de las Autoridades de Certificación de la PKI, basándose en la relación de confianza que existe entre ellas. Puesto que el modelo de la PKI implementada en Cuba es jerárquico esto implica que cada entidad poseerá un certificado expedido por su Autoridad de Certificación superior, y sólo existe un camino entre dos autoridades, esta constituye la vía más apropiada para la construcción del camino de certificación.

Recuperación de los Certificados: Consiste en recuperar los certificados que forman parte del camino de certificación de los repositorios donde se encuentran almacenados.

2.5 Conclusiones

Garantizar el máximo nivel de seguridad posible de todos los recursos informáticos del MININT contribuye de forma significativa a garantizar la seguridad de la nación cubana. Es por ello que resulta tan importante controlar no solo quién accede a cada recurso sino también las acciones que tiene permitidas efectuar sobre el recurso en cuestión. El uso de los certificados de llave pública constituye hasta el momento la vía óptima para la identificación de cualquier entidad ante una aplicación en la que el proceso de autenticación esté implementado sobre la base del uso de este tipo de certificado, pero los certificados digitales de autorización posibilitarán que una vez que esas aplicaciones cuenten con las funcionalidades requeridas para procesarlos la validación del certificado permita además de comprobar la identidad del usuario que accede conocer y verificar las facultades que le han sido otorgadas, es decir determinar el nivel de acceso del usuario sobre el recurso accedido.

CAPÍTULO 3: Propuesta inicial para la implementación de una PMI

3.1 Introducción

La continua aparición de aplicaciones que precisan la utilización, no sólo de servicios de autenticación, sino también de autorización, ha provocado la creación de un nuevo marco de trabajo por parte de la ITU, con el fin de cubrir las necesidades presentadas por las PKI para integrar los servicios de autorización.

En el presente capítulo se esboza una propuesta para la implementación de este marco de trabajo por parte del DICC del MININT teniendo en cuenta que la solución planteada en el capítulo anterior para resolver el problema de la autorización resulta conveniente para su aplicación a corto plazo, pero una vez que se incremente el número de usuarios que hacen uso de la PKI comenzarán presentarse serias dificultades, fundamentalmente en cuanto a la escalabilidad y funcionamiento óptimo de la infraestructura. Se describen además los componentes fundamentales de la PMI así como el papel que desempeña cada uno de ellos en el desarrollo de la misma.

3.2 El CDA como propuesta inmediata pero no como solución permanente

3.2.1 El CDA como propuesta inmediata. Ventajas de su utilización en el MININT

Los certificados digitales de autorización presuponen la posibilidad de lograr un mecanismo de autenticación de aplicaciones que esté muy ligado con la autorización de acceso, teniendo en cuenta no sólo la identidad sino también la especificación de los roles y funciones de quienes se autentiquen con un certificado digital de autorización.

Es importante señalar que las acciones necesarias para comenzar a utilizar los certificados digitales de autorización no son de gran complejidad ni precisan la asignación de importantes recursos, es por ello que requieren de un corto período de tiempo para su ejecución, esto

resulta muy beneficioso pues estos certificados permitirán ampliar la seguridad de las aplicaciones telemáticas que hoy se desarrollan en el MININT, y se constituirán como un criterio para fortalecer los elementos de seguridad inherentes a los certificados digitales de las infraestructuras de llave pública pues posibilitarán el establecimiento de un mecanismo de control de acceso a los recursos informáticos correspondientes a cada una de las líneas del trabajo operativo a partir de los privilegios y facultades asignados a cada usuario, en dependencia de su jerarquía y los roles que desempeñe en su puesto de trabajo.

3.2.2 ¿Por qué no como solución permanente?

La PKI no es en realidad la herramienta más apropiada para satisfacer todos los requerimientos de seguridad de las aplicaciones que necesitan de servicios de autorización. La principal razón de esta afirmación es que los elementos básicos de la PKI son los certificados digitales y la razón de ser de los mismos no es dar cobertura a los problemas de autorización.

En la especificación de la ITU de 1997, se proporciona, dentro del estándar X.509 v3, una alternativa al uso de los certificados de atributos, que consiste en la inclusión de los atributos del usuario dentro del certificado digital, a través de una extensión. La solución descrita en el capítulo anterior se basa en este argumento, sin embargo este procedimiento, aunque puede ser válido para dar cobertura a algunos problemas, resulta insuficiente ante un sistema con un uso intensivo del servicio de autorización por lo que una vez que la PKI desarrollada por el MININT esté funcionando plenamente y se comience a extender su uso a todas la esferas tanto dentro como fuera de este ministerio se comenzarán a observar de forma paulatina las dificultades que se derivan del uso de los certificados digitales con fines de autorización.

Una de las principales dificultades que se presentará será el considerable crecimiento de las CRL, la razón fundamental es que los certificados digitales están concebidos para un período

de vigencia relativamente largo en comparación con los derechos de acceso y los privilegios del usuario, los cuales poseen un dinamismo mayor, relativo al cambio de estado. Esto produce una inevitable avalancha de revocaciones incrementando el número de certificados que deben ser incorporados a la CRL y que permanecerán reflejados en la misma hasta su fecha de expiración, ocasionando en el sistema una reducción de la funcionalidad, disminuyendo la calidad del servicio prestado.

Como parte de esta nueva idea el concepto de certificado X.509 se ha diversificado, obteniéndose además de los certificados de llave pública, los certificados de atributos y con ellos un nuevo tipo de infraestructura, la Infraestructura de Administración de Privilegios (PMI, por sus siglas en inglés). Los certificados de atributos son el elemento necesario para vincular los privilegios a los usuarios y posibilitan especificar una relación con los certificados de identidad los cuales proporcionan, en la mayoría de las ocasiones, la solución más adecuada para dotar del servicio de autenticación a la totalidad de las aplicaciones. Sin embargo, en entornos donde no es suficiente con probar quién se es, sino que además es necesario proporcionar un mecanismo que detalle qué se tiene permitido hacer, se hace necesario contar con un servicio de autorización y la vía más apropiada para alcanzarlo es la implantación de una PMI que resuelva los problemas de escalabilidad que presentan las soluciones desarrolladas hasta el momento.

3.3 Introducción a un nuevo tipo de infraestructuras: las PMI y sus components

3.3.1 ¿Qué es PMI?

El surgimiento de nuevos estándares internacionales en relación al uso de los certificados digitales, ha dado respuesta a una preocupación constante en cuanto a separar los ámbitos relativos a la identidad y las facultades de las entidades y ha contribuido en gran medida a solucionar inconvenientes derivados de un intercambio comercial y de información, a través

de medios electrónicos, cada vez más ágil y que implica constantes cambios. De este modo, los problemas que surgen de la modificación de permisos y privilegios en relación a una entidad que puede autenticarse electrónicamente en el momento de realizar una acción, se ven mitigados en gran medida con la implantación y puesta en funcionamiento de una PMI.

PMI es una infraestructura construida de acuerdo a normas internacionales, como la RFC-3281, un nuevo estándar internacional para la administración de facultades y atributos, orientada a integrarse con las soluciones de certificados de llave pública, pues los certificados de atributos gestionados por esta infraestructura vinculan uno o más atributos a una identidad. Es decir, PMI es el conjunto de hardware, software, recursos humanos, políticas y procedimientos necesarios para crear, manejar, almacenar, distribuir y revocar certificados de atributos.(10)

El principio básico que se encuentra presente en esta solución, es que el certificado de atributos es un documento electrónico suscrito por el emisor y en virtud del cual se da certeza de las cualidades o poderes que tiene una entidad en un momento determinado. Para lograr el objetivo se vincula el certificado de identidad del suscriptor del documento electrónico con el certificado de atributos manteniéndolos asociados de manera segura. Así intervienen dos certificadores en la más precisa identificación del titular, el primero que certifica la identidad de las entidades por medio de un certificado de llave pública, y el segundo que certifica las atribuciones y competencias de esas entidades para efectuar una determinada operación sobre un recurso.

3.3.2 Componentes fundamentales de la PMI

A continuación se definen los componentes principales de una PMI así como el papel que desempeña cada uno de ellos en el funcionamiento de la misma, se describe además cómo deben interactuar dichos componentes de forma tal que se realice una correcta gestión de los atributos y facultades de los usuarios.

Certificado de Atributos: Es el componente fundamental de la PMI, establece un vínculo sólido y seguro entre su propietario y los atributos plasmados en el mismo. Es un documento electrónico suscrito por el emisor y en virtud del cual se da certeza de las cualidades o poderes que tiene una entidad en un momento determinado

Autoridad de Certificación de Atributos (ACA): Es la máxima responsable del control de todo el ciclo de vida de los certificados de atributos, incluyendo la emisión, almacenamiento y revocación de los mismos. La ACA posee la facultad de asignar privilegios a otras entidades que pueden ser Autoridades de Delegación de Atributos o Propietarios.

Usuario o Propietario: Puede ser cualquier cliente de los servicios brindados por la PMI, por lo general será el acreedor de uno o más privilegios, puede ser un dispositivo, un proceso, una aplicación, un servidor, una persona física o cualquier cosa identificada como el propietario de un certificado de atributos. No tiene la facultad de conceder a otra entidad los atributos que le han sido asignados.

Autoridad de Delegación de Atributos (ADA): Es una entidad que tiene permitido asignar a otras entidades (ya sea a ADA o propietarios) los privilegios que le han sido conferidos por la ACA, es responsable de realizar toda la verificación necesaria antes de efectuar la solicitud de emisión o revocación de un certificado de atributos.

Repositorio: Es el medio de almacenamiento y recuperación de certificados de atributos y ACRL. Constituye el medio de distribución de los certificados y ACRL a los usuarios. Su funcionamiento es muy similar al de los repositorios de la PKI.

Una ACRL es una lista, firmada digitalmente por la ACA, que contiene los números seriales de los certificados de atributos revocados junto con su fecha y razón de revocación. Esta lista

debe ser actualizada periódicamente y publicada en un repositorio confiable destinado a este fin, para facilitar el acceso a la misma por parte de los usuarios.

De acuerdo con esta propuesta la ACA será responsabilidad del MININT, este ministerio debe disponer de los recursos humanos y tecnológicos necesarios para la implementación y puesta en funcionamiento de la misma. Se debe poder contar con tantas ADA como sean necesarias puesto que de esta forma se simplifica el proceso de verificación de los privilegios a asignar, así para la emisión de un certificado de atributos por parte de la ACA bastaría con la solicitud de la ADA que tiene la potestad de asignar los atributos contenidos en la solicitud en cuestión, antes de realizar la solicitud la ADA debe haber verificado la identidad de la entidad a la que le serán otorgados los privilegios a través del certificado de llave pública correspondiente a esa entidad, el cual es requisito indispensable para la obtención del certificado de atributos. Es decir que una entidad que no posea un certificado de llave pública no puede ser propietario de un certificado de atributos, por otra parte una entidad puede ser el propietario de tantos certificados de atributos como sea necesario. Para la revocación de un certificado de atributos es requisito suficiente y necesario la solicitud por parte de la ADA que requirió la emisión del mismo.

La ACA debe contar con un certificado de llave pública emitido por la Autoridad de Certificación del MININT, todos los certificados que emita deben estar firmados con su llave privada de forma que se pueda comprobar la validez de los mismos, cada ADA debe poseer también un certificado de llave pública que le permita firmar las solicitudes que realice a la ACA. De ser revocado el certificado de llave pública de una ADA es responsabilidad de la ACA determinar, según las causas que hayan motivado la revocación, si los certificados de atributos emitidos a solicitud de esta mantienen o no su validez, ahora bien, si es revocado certificado de llave pública de un propietario quedan sin efecto (son revocados) todos los certificados de atributos con los que contaba el propietario en cuestión.

3.3.3 Certificados de Atributos

En su revisión del año 2000 del X.509, la ITU-T dio un paso significativo hacia la solución de la problemática existente en cuanto a la vinculación de los usuarios con las facultades que les eran conferidas, esta revisión definió formalmente el marco de trabajo para los certificados de atributos, e incluyó la especificación de los objetos de datos utilizados para representar este tipo de certificados.

La sintaxis del certificado de atributos guarda cierta similitud con la de los certificados de identidad, pues contiene los campos habituales de versión (*version*), número de serie (*serialNumber*), firma (*signature*), emisor (*issuer*), período de validez (*attrCertValidityPeriod*), e incluso los campos opcionales identificador único de emisor (*issuerUniqueID*) y extensiones (*extensions*). Existen, sin embargo, campos nuevos como son el del titular o propietario del certificado (*subject/holder*) y el de atributos (*attributes*), que contendrá la información sobre los privilegios o permisos conferidos al titular, este campo podrá reflejar además otro conjunto de características como pertenencia a grupos, identificación de cargos, valores límite de transacciones, etc.

Es conveniente resaltar que, a diferencia de lo que ocurre en el certificado de llave pública, es posible no dejar explícita la identificación del usuario en el certificado de atributos, sino que se utiliza el campo propietario para enlazar este certificado con el correspondiente certificado digital del usuario, mediante la inserción en el mismo del número de serie del certificado de llave pública de la entidad sobre la que se expresan los atributos o privilegios. De esta forma, la PKI autentica a aquellos usuarios de quien la PMI emite certificados de atributos, reflejándose así la estrecha relación existente entre estas infraestructuras. No obstante, ésta no es la única solución, como alternativa, el campo propietario puede contener el valor resumen de la llave pública del usuario, o bien el del certificado de identidad completo. De no existir vínculo con una PKI, el cual no es el caso, este campo podrá contener el identificador del usuario. Nótese que en ningún caso el certificado de atributos

contendrá una llave pública y por consiguiente su propietario no tendrá una llave privada asociada específicamente a este certificado, es por ello que una entidad puede poseer tantos certificados de atributos como sea necesario sin el inconveniente de tener que recordar cual es la llave privada que le corresponde a cada uno de ellos.

3.3.3.1 Descripción de la sintaxis ASN.1 del Certificado de Atributos X509 v2

Un Certificado de Atributos X.509 v2 es definido mediante ASN.1 de la siguiente forma: (26)

```
AttributeCertificate ::= SEQUENCE {
        acinfo              AttributeCertificateInfo,
        signatureAlgorithm  AlgorithmIdentifier,
        signatureValue      BIT STRING
    }

    AttributeCertificateInfo ::= SEQUENCE {
        version             AttCertVersion – la versión es v2,
        holder              Holder,
        issuer              AttCertIssuer,
        signature           AlgorithmIdentifier,
        serialNumber        CertificateSerialNumber,
        attrCertValidityPeriod  AttCertValidityPeriod,
        attributes          SEQUENCE OF Attribute,
        issuerUniqueID      UniqueIdentifier OPTIONAL,
        extensions          Extensions OPTIONAL
    }

    AttCertVersion ::= INTEGER { v2(1) }
    Holder ::= SEQUENCE {
```

```
    baseCertificateID   [0] IssuerSerial OPTIONAL,
          -- emisor y número de serie del certificado
          -- de llave pública del propietario

    entityName          [1] GeneralNames OPTIONAL,
    objectDigestInfo    [2] ObjectDigestInfo OPTIONAL
          -- se usa si se desea autenticar directamente al propietario
          -- no se recomienda su uso
}

AttCertIssuer ::= CHOICE {
   v1Form   GeneralNames,  -- NO será usado
   v2Form   [0] V2Form        -- recomendado
}

V2Form ::= SEQUENCE {
    issuerName          GeneralNames  OPTIONAL,
    baseCertificateID    [0] IssuerSerial  OPTIONAL,
    objectDigestInfo     [1] ObjectDigestInfo  OPTIONAL
     -- issuerName DEBE estar presente
     -- baseCertificateID y objectDigestInfo NO DEBEN estar presentes
}

IssuerSerial  ::=  SEQUENCE {
    issuer        GeneralNames,
    serial        CertificateSerialNumber,
    issuerUID     UniqueIdentifier OPTIONAL
}
```

```
AttCertValidityPeriod  ::= SEQUENCE {
    notBeforeTime  GeneralizedTime,
    notAfterTime   GeneralizedTime
}
Attribute ::= SEQUENCE {
     type     AttributeType,
     values   SET OF AttributeValue
       -- se requiere al menos un valor
}

AttributeType ::= OBJECT IDENTIFIER

AttributeValue ::= ANY DEFINED BY AttributeType
```

Algunos de los campos presentes en este tipo de certificados coinciden con los detallados en el Capítulo 2, es por ello que sólo se puntualizarán aquellos que son nuevos o que difieren en su definición con respecto a los descritos anteriormente.

***Holder* / Propietario**

El campo Propietario es una secuencia que permite para su definición el uso de tres sintaxis diferentes: *baseCertificateID, entityName and objectDigestInfo*. Es importante señalar que el uso de más de una de estas opciones por parte de una misma ACA podría acarrear confusiones, es por ello que se recomienda usar sólo una, en este caso se sugiere el uso de *baseCertificateID*, teniendo en cuenta que la PMI que se propone coexistirá con una PKI y por consiguiente la autenticación de los usuarios o entidades se realizará mediante el uso de Certificados de Identidad X.509. Con esta opción la información contenida en los campos

issuer y serialNumber del certificado de llave pública del propietario tiene que ser idéntica a la del campo *holder* del Certificado de Atributos.

***serialNumber* / Número de Serie**

En los certificados de atributos emitidos por la ACA el par *issuer/serialNumber* debe ser una combinación única, incluso si el período de vigencia del certificado es muy breve se debe generar un nuevo número de serie para cada certificado que se emita, la ACA debe establecer que los números de serie de los certificados sean siempre enteros positivos.

Considerando lo antes expuesto, es de esperar que los números de serie estén constituidos por enteros de gran tamaño, por tal motivo es sumamente significativo que las aplicaciones que vayan a hacer uso de estos certificados sean capaces de operar valores de números de serie mayores de cuatro octetos, aunque es importante destacar que estos valores no deben exceder nunca los 20 octetos.

No existe ninguna restricción en cuanto al orden que deben seguir estos valores, lo primordial es garantizar que cada certificado que se emita por parte de una ACA contenga un número de serie único.

***Attributes* / Atributos**

El campo de atributos brinda información sobre el propietario del certificado de atributos, cuando el certificado es usado para la autorización este campo usualmente contendrá una serie de privilegios, estos privilegios pueden y se recomienda que sean especificados mediante el uso de los OID definidos como parte de la solución descrita en el capitulo anterior.

El campo de atributos generalmente contiene una secuencia de uno o más atributos, el OID de cada atributo de la secuencia debe ser único, es decir que un certificado de atributo puede

aparecer sólo una instancia de cada atributo, no obstante es posible que cada instancia contenga más de un valor, esto significa que cada atributo puede contener un conjunto de valores y cualquier aplicación o sistema que vaya a hacer uso de los certificados de atributos debe ser capaz de manipular múltiples valores para todos los tipos de atributos.

3.3.3.2 Validación y Revocación de Certificados de Atributos

La validación es parte fundamental de la PMI, porque permite corroborar la validez y el origen de los certificados de atributos. La verificación de la firma de un certificado permite corroborar la integridad y autenticidad de su contenido. Para ello, el verificador necesita conocer la llave pública de la autoridad que expidió dicho certificado. Para poder confiar en la llave obtenida, el usuario debe verificar la firma y el estado de validez del certificado. Por su parte la revocación es, en esencia, anular el vínculo existente entre un atributo o un conjunto de atributos y una entidad, antes de la expiración del certificado de atributos que establece dicho vínculo. Se prevé que la causa fundamental que conllevará a la revocación de los certificados de atributos será la modificación o suspensión de los derechos de acceso, privilegios o atributos del propietario.

El proceso de validación de los certificados de atributos, al igual que el de los certificados de llave pública y los certificados digitales de autorización puede realizarse esencialmente de dos formas: en línea o fuera de línea y en ambos casos estos procesos se realizan siguiendo los mismos procedimientos descritos en el Capítulo 2 de este trabajo de diploma, la diferencia fundamental radica en que en el caso de los certificados de atributos es totalmente desaconsejable la validación fuera de línea pues las dificultades presentadas por este mecanismo, que también fueron descritas en el Capítulo 2, se hacen especialmente latentes cuando se trata de este tipo de certificación.

Los certificados de atributos deben ser revocados cuando los permisos especificados dejen de ser válidos. Lo que diferencia a este tipo de revocación de la realizada con certificados de

llave pública, es que se debe distinguir entre dos tipos: la revocación sencilla de un propietario, y la revocación más compleja de una ADA que ha propagado ciertos privilegios a otras entidades porque estaba autorizada a ello. Para el primer caso basta aplicar cualquiera de las técnicas clásicas de revocación de certificados que se han mostrado efectivas. Sin embargo, en el caso del segundo debemos tener en cuenta que la revocación de los privilegios de dicha entidad puede conllevar también una revocación propagada, es decir, la anulación de todos o parte de los privilegios emitidos por dicha entidad. Será necesaria la realización de una revocación propagada sólo en el caso en el que se haya demostrado una actitud inapropiada por parte de la ADA cuyo certificado de atributos se ha revocado, en otro caso se podría decidir mantener los privilegios propagados.

Tanto los certificados como la información de revocación deben estar disponibles para los usuarios en algún sitio. En este caso se propone su publicación en un sitio de la RIM, en el que se debe garantizar su disponibilidad y fácil acceso. Además de que esta información debe estar almacenada en un repositorio destinado para este fin, el cual debe contar con las medidas de seguridad apropiadas para garantizar la protección de estos datos.

3.3.3.3 Requerimientos básicos para el empleo de los certificados de atributos

El empleo de los certificados de atributos precisa del cumplimiento de una serie de requerimientos mínimos de los que depende en gran medida su correcta utilización y funcionamiento:

Requerimientos de Período de Validez:

- Deben soportar períodos de validez tanto cortos como largos, los períodos cortos típicamente se miden en horas, contrario a los Certificados de Identidad en los que este tiempo suele expresarse en meses. Los periodos de validez cortos posibilitan que

los certificados de atributos sean útiles sin la necesidad de un uso excesivo del mecanismo de revocación.

Requerimientos de Tipos de Atributos:

- La ACA debe ser capaz de definir Tipos de Atributos propios, que permitan satisfacer de forma más eficiente las necesidades específicas de los usuarios.
- Independientemente de los atributos propios determinados por la AA es recomendable que al menos algunos de los atributos estándar de los Certificados de Atributos estén definidos, por ejemplo "*access identity*," "*group*," "*role*," "*clearance*," "*audit identity*," y "*charging identity*."
- Los atributos estándar deben ser definidos de forma tal que permitan distinguir los distintos usos de un mismo atributo en diferentes dominios.

Requerimientos para la Solicitud

- Para solicitar un certificado de atributos es requisito indispensable que el usuario o entidad posea un certificado de llave pública emitido por la Autoridad de Certificación del MININT.
- Se debe presentar la documentación, ya sea en copia dura o digital, que acredite la asignación del privilegio invocado.
- En caso de que el certificado de atributos no sea para una persona física sino para otro tipo de entidad, entiéndase servidor, aplicación, etc., la persona que sea la máxima responsable de la entidad en cuestión es la encargada de realizar los trámites para la solicitud del certificado de atributos requerido.

3.3.4 Modelos de PMI

Se pueden usar varios modelos en función de la aplicación que consideremos. Así, hay un modelo general y sobre éste se definen tres modelos específicos: modelo de control, de roles

y de delegación. Es importante señalar que estos modelos no son excluyentes, sino que la aplicación combinada de todos es lo que define realmente el modelo de la PMI.

El modelo general consta de tres entidades: objeto, tenedor del privilegio y verificador del privilegio. El objeto es el recurso que se pretende proteger. Sobre el objeto se definen ciertos métodos, que identifican formas de uso del mismo (como ejemplos básicos, leer, escribir, ejecutar, borrar, etc.). El propietario del privilegio es la entidad a la que se le ha asignado el privilegio, mientras que el verificador del privilegio es la entidad que determina si los privilegios asignados al propietario son suficientes para realizar una determinada operación sobre el objeto. La decisión sobre si el verificador permite o no al propietario realizar la operación solicitada se basa en tres factores: privilegios del propietario, política de privilegios y variables de entorno.

El modelo de control, o de control de accesos, muestra cómo el verificador controla el acceso al método del objeto, por parte del propietario, según la política establecida. El verificador de privilegios combina las distintas entradas y determina si el acceso se permite o no. Es decir, el verificador controla el acceso al método del objeto por parte del propietario de acuerdo con la política de privilegios y las variables de entorno.
El modelo de roles se basa en el uso de roles para asignar privilegios a usuarios, pero de forma indirecta. Es decir, a cada usuario se le asignan uno o varios roles, y entonces a cada rol se le asignan una serie de privilegios. En este modelo existen dos tipos de certificados: el certificado de asignación de rol, que enlaza al usuario con el rol, y el certificado de especificación de rol, que enlaza el rol con los privilegios específicos.

El modelo de delegación se utiliza en aquellos escenarios en que no sólo es necesario asignar privilegios, sino también proporcionar mecanismos para que las entidades puedan delegar esos privilegios que les han sido otorgados. La ACA es la responsable de la asignación inicial de privilegios, y autoriza al propietario a actuar como una ADA. Ésta puede

a su vez delegar en otra ADA todos o parte de esos privilegios que posee, o bien delegar directamente en las entidades finales. Con ello se forma un camino de delegación que consta de una serie de certificados de atributos que están enlazados por los nombres de los emisores y los propietarios.

3.3.5 Requerimientos para la implementación y puesta en funcionamiento de la PMI

La implementación de una PMI puede resultar una tarea compleja, es por ello que requiere la ejecución de un conjunto de tareas de las que depende de forma substancial su óptimo funcionamiento. A continuación se hace referencia a algunas de estas tareas que si bien no abarcan todas las acciones a desarrollar brindan una idea de las cuestiones fundamentales a tener en cuenta para la puesta en marcha de esta infraestructura:

- Personal calificado, especialmente administradores de redes bien preparados.
- Infraestructura de seguridad con mecanismos adecuados, como pueden ser un sistema de bitácora de seguridad, sistemas de detección de vulnerabilidades y sistemas de detección de intrusos.
- Procedimientos y políticas que permitan la explotación de la tecnología, la emisión, renovación y revocación de certificados, partiendo de un nivel de seguridad confiable. Las políticas deben ser implementadas no por regulaciones, sino a partir de la configuración de los programas adoptados para la PMI, de forma tal que ellos sean los que no permitan realizar las acciones que las políticas prohíben. En el caso de que aparezcan vulnerabilidades en estos programas, los mismos deben ser cambiados o mejorados, la detección temprana de estas vulnerabilidades sólo se logra si se mantiene un control sistemático.
- Definir y adoptar protocolos de comunicación eficientes y seguros.

- La ACA debe establecer las políticas de seguridad para definir las reglas según las cuales debe realizarse todo el proceso de gestión de los certificados de atributos, así como también los procedimientos para instrumentar la generación, distribución, revocación y empleo de estos certificados.
- Crear Sistema de Distribución de Certificados.
- Implantar el control de acceso basado en tarjetas inteligentes, envío de mensajes autentificados y módulos de seguridad de hardware.
- Los sistemas de ACA y ADA deben contar con un nivel de seguridad elevado con este fin se propone el empleo de hardware a prueba de manipulaciones, módulos de autoridad de certificación y otros elementos que proporcionen una integración armónica con otros sistemas de seguridad.
- Determinar la jerarquía en cada una de las estructuras de manera que se establezcan las conexiones funcionales de carácter interno y externo.
- Establecer los niveles de seguridad de acuerdo a la jerarquía de cada entidad.

3.4 Conclusiones

En este capítulo se han analizado ampliamente las características esenciales con que debe contar una PMI para la correcta gestión de la autorización mediante el uso de los certificados de atributos. Además, se hace énfasis en las características de los componentes que la constituyen y la forma en que deben relacionarse estos componentes para lograr el correcto funcionamiento de la infraestructura. Se describen detalles específicos del proceso de validación de los certificados de atributos y se plantean un conjunto de tareas que resultan imprescindibles para la implementación de la PMI.

CONCLUSIONES

El certificado digital de autorización se concibe luego de analizar las tendencias actuales en el uso de los certificados de llave pública con fines de autorización, considerar las particularidades y necesidades del MININT en cuanto al control de acceso y comprender cuan significativa resulta la concepción y utilización de estos certificados en el aseguramiento de los recursos informáticos de este ministerio. Se concluye que:

- La propuesta se ha elaborado sobre la base del estándar X.509 v3.
- La nueva extensión definida permite que en el momento de la autenticación de una entidad ante cualquier recurso o aplicación, mediante el uso de un certificado digital de autorización, puedan ser considerados los privilegios o facultades con que cuenta la entidad sobre el recurso ante el que se autentica, definiéndose de esta forma su nivel de acceso sobre el mismo.
- La integración de la certificación de autorización a los servicios proporcionados por la PKI constituye un avance significativo en cuanto al aseguramiento y control de los recursos informáticos del MININT.

RECOMENDACIONES

Para comenzar a utilizar los certificados digitales de autorización es necesario llevar a cabo un conjunto de acciones previas:

- Realizar las modificaciones pertinentes al proceso de solicitud de forma que se puedan registrar los datos sobre los privilegios del usuario ya sea incorporándole nuevos campos al formulario de solicitud empleado para los certificados de llave pública o definiendo un nuevo formulario para los certificados digitales de autorización.

- Implementar con la mayor brevedad posible las funcionalidades requeridas por aplicaciones que emplearán este tipo de certificados para el control de accesos de forma que puedan comprender y procesar la nueva extensión.

- Establecer una estructura definitiva para la asignación de los OID dentro del MININT y una vez hecho esto definir y asignar de forma paulatina el OID correspondiente a cada recurso, priorizando aquellos recursos de mayor importancia y precisando el identificador proporcionado a cada nivel de acceso en dicho recurso.

- Realizar las adecuaciones necesarias a la Declaración de Prácticas de Certificación de forma tal que indique claramente las políticas y procedimientos relativos a la seguridad y mantenimiento de los certificados digitales de autorización, las responsabilidades de la Autoridad de Certificación respecto a los sistemas que emplean estos certificados y las obligaciones de los subscriptores respecto a la misma. Esto debe reflejarse en una nueva versión de la Declaración de Prácticas de Certificación.

REFERENCIAS BIBLIOGRÁFICAS

1. REVERTE, Ó. C. y SKARMETA, A. G. Gestión y uso de certificados de autorización SPKI/SDSI. *Ágora SIC*, 04/2003 2003, vol. 34.

2. *Fundamentos de criptografía y de PKI* [Científico]. 2002, [Consultado el: 02/03/2008]. Disponible en: http://www.idg.es/iworld/impart.asp?id=131016.

3. SILVA, G. M. *Diseño e Implementación de una Autoridad Certificadora en Plataformas Móviles.* INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY, 2005, [Consultado el: 10/04/2008].

4. CASAS, G. y ARTURO, J. M. Introducción a la Criptología. *Universidad Nacional Autónoma de México.*

5. KOHNFELDER, L. *Towards a Practical Public-key Cryptosystem.* Tutor: Len Adleman, Profesor Asistente. Massachusetts Institute of Technology, 1978.

6. GIROLAMO, C. D. *Implementación y uso de PKI (Public key infrastructure – Infraestructura de llave pública).* 2006.

7. *Decisión Administrativa 6/2007 Jefatura de Gabinete de Ministros. Firma Digital, Marco Normativo.* Boletín Oficial de la República Argentina 12-feb-2007, No. 31093. Disponible en: http://www.juschubut.gov.ar/04_servicios/3_firma_digital/res_6-07.html.

8. LÓPEZ, M. J. L. *Criptografía y Seguridad en Computadores.* 2004, Disponible en: http://www.themalia.es/admin/img/documentos/200506281022060.Criptografia.pdf.

9. *RESOLUCION No. 127 /2007.* Ministerio de la Informática y las Comunicaciones de la República de Cuba, 2007, 21 p. Disponible en: http://www.mic.gov.cu/.

10. ECHAVARRÍA, I. S. *"CONTRIBUCIÓN A LA VALIDACIÓN DE CERTIFICADOS EN ARQUITECTURAS DE AUTENTICACIÓN Y AUTORIZACIÓN".* Tutor: Muñoz, J. F. Tesis Doctoral, UNIVERSIDAD POLITÉCNICA DE CATALUNYA, 2007.

11. CHOUDHURY, S.; BHATNAGAR, K. y HAQUE, W. *Public Key Infrastructure Implementation and Design. New York.* 2004, Disponible en: www.hungryminds.com.

12. LODOS, J.; GAMAZO, N. y RODRÍGUEZ, Y. *Infraestructuras de llaves públicas en redes corporativas.* [Científico]. 2003, [Consultado el: 06/03/2008]. vol. XXIV.

13. TALAVERA, J. *Infraestructura para la Criptografía de Llave Pública.* 2005. Disponible en: http://www.cnc.una.py/cms/cnc/index.php?id=0,61,0,0,1,0.

14. HOUSLEY, R.; POLK, W.; FORD, W. y D. SOLO. *RFC3280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* IETF Network Working Group, Disponible en: www.ietf.org/rfc/rfc3280.txt.

15. MEALLING, M. RFC3061-A URN Namespace of Object Identifiers. 2001. Disponible en: http://www.ietf.org/rfc/rfc3061.txt.

16. TALENS-OLIAG, S. *Introducción a los certificados digitales.* publicado el: 2005, [Consultado el: 08/01/2008]. Disponible en: http://www.infocentre.gva.es/.

17. CARVAJAL, A. PKI y Firmas Digitales: Aplicaciones Reales. En *GLOBALTEKSECURITY: TECNOLOGIAS GLOBALES PARA LA SEGURIDAD DE LA INFORMACION. 2007.*

18. BARRA, M. C. *INFRA-ESTRUTURA DE CHAVES PUBLICAS BRASILEIRA (ICP-BRASIL) E A FORMACAO DO ESTADO ELETRONICO.* Tutor: Sobral, F. F. Tesis de Maestría, Departamento de Sociología Universidad de Brasilia, 2006.

19. Decisión Administrativa Nº 6/2007. Capítulo III, Infraestructura de firma digital de la República Argentina.

20. MARTÍN, E. y MARCELO, F. *PKI y Certificados Digitales: Un Mercado en Alza.* 2002, vol. 167.

21. SÁNCHEZ, J. C.; GARCÍA, J. E.; ENCINAS, L. H.; POUS, H. R., *et al. Hacia una nueva identificación electrónica del ciudadano: el DNI-e* España: Safelayer, Disponible en: http://www.safelayer.com/fileadmin/pdf/DNIe.pdf.

22. GIGLI, J. *España: Safelayer Suministrará la PKI que Sustentará el Futuro Documento Nacional de Identidad* [Consultado el: 23/03/2008] Disponible en: http://www.gobiernoelectronico.org/?q=node/3257.

23. PAGÉS, T. *La Infraestructura de Llave Pública en el Proceso de Informatización de la Sociedad Cubana.* 2008.

24. LAMPSON, B. *Protection.* En *5th Princeton Symposium on Information Science and Systems., Reprinted in ACM Operating Systems Review.* 1971.

25. LARMOUTH, J. *ASN.1 Complete.* [Científico]. 1999, 60-99 p.

26. FARRELL, S. y HOUSLEY, R. *RFC3281-An Internet Attribute Certificate Profile for Authorization* Disponible en: http://www.ietf.org/rfc/rfc3281.txt.

BIBLIOGRAFÍA

BARRA, M. C. *INFRA-ESTRUTURA DE CHAVES PUBLICAS BRASILEIRA (ICP-BRASIL) E A FORMACAO DO ESTADO ELETRONICO.* Tutor: Sobral, F. F. Tesis de Maestría, Departamento de Sociología Universidad de Brasilia, 2006.

CARVAJAL, A. PKI y Firmas Digitales: Aplicaciones Reales. En: *GLOBALTEKSECURITY: TECNOLOGIAS GLOBALES PARA LA SEGURIDAD DE LA INFORMACION. 2007.*

CASAS, G. y ARTURO, J. M. Introducción a la Criptología. *Universidad Nacional Autónoma de México.*

CHOUDHURY, S. y BHATNAGAR, K., *et al. Public Key Infrastructure Implementation and Design. New York.* 2004, Disponible en: www.hungryminds.com.

Decisión Administrativa 6/2007 Jefatura de Gabinete de Ministros. Firma Digital, Marco Normativo. Boletín Oficial de la República Argentina 12/02/2007, vol. 31093, 3 p. Disponible en: http://www.juschubut.gov.ar/04_servicios/3_firma_digital/res_6-07.html.

ECHAVARRÍA, I. S. *"CONTRIBUCIÓN A LA VALIDACIÓN DE CERTIFICADOS EN ARQUITECTURAS DE AUTENTICACIÓN Y AUTORIZACIÓN".* Tutor: Muñoz, J. F. Tesis Doctoral, UNIVERSIDAD POLITÉCNICA DE CATALUNYA, 2007.

FARRELL, S. y HOUSLEY, R. *RFC3281-An Internet Attribute Certificate Profile for Authorization.* Disponible en: http://www.ietf.org/rfc/rfc3281.txt.

Fundamentos de criptografía y de PKI [Científico]. 2002, [Consultado el: 02/03/2008]. Disponible en: http://www.idg.es/iworld/impart.asp?id=131016.

GIGLI, J. *España: Safelayer Suministrará la PKI que Sustentará el Futuro Documento Nacional de Identidad* [Consultado el: 23/03/2008] Disponible en: http://www.gobiernoelectronico.org/?q=node/3257.

GIROLAMO, C. D. *Implementación y uso de PKI (Public key infraestructure – Infraestructura de llave pública).* 2006.

HOUSLEY, R.; POLK, W., *et al. RFC3280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* IETF Network Working Group, Disponible en: www.ietf.org/rfc/rfc3280.txt.

ILUSTRE COLEGIO DE ABOGADOS DE MADRID, CERTIFICADO DE ABOGADO EJERCIENTE, POLÍTICA DE CERTIFICACIÓN. 2005.

ITU-T. *Recommendation X.509: Information Processing Systems - Open Systems Interconnection - The Directory: Authentication Framework (Technical Corrigendum), International Telecommunication Union* Disponible en: http://www.itu.int/rec/T-REC-X.509-200003-I.

KOHNFELDER, L. *Towards a Practical Public-key Cryptosystem.* Tutor: Len Adleman, Profesor Asistente. Massachusetts Institute of Technology, 1978.

LAMPSON, B. *Protection.* En *5th Princeton Symposium on Information Science and Systems., Reprinted in ACM Operating Systems Review.* 1971.

LARMOUTH, J. *ASN.1 Complete.* [Científico]. 1999, 60-99 p.

LODOS, J.; GAMAZO, N., *et al. Infraestructuras de llaves públicas en redes corporativas.* [Cientifico]. 2003, [Consultado el: 06/03/2008]. vol. XXIV,

LÓPEZ, M. J. L. *Criptografía y Seguridad en Computadores.* 2004, Disponible en: http://www.themalia.es/admin/img/documentos/200506281022060.Criptografia.pdf.

MARTÍN, E. y MARCELO, F. *PKI y Certificados Digitales: Un Mercado en Alza,* Comunicaciones World, 2002, vol. 167.

MEALLING, M. RFC3061 - A URN Namespace of Object Identifiers. 2001, Disponible en: http://www.ietf.org/rfc/rfc3061.txt.

PAGÉS, T. *La Infraestructua de Llave Pública en el Proceso de Informatización de la Sociedad Cubana.* 2008.

RESOLUCION No. 127 /2007. Ministerio de la Informática y las Comunicaciones de la República de Cuba, 2007, 21 p. Disponible en: http://www.mic.gov.cu/.

REVERTE, Ó. C. y SKARMETA, A. G. Gestión y uso de certificados de autorización SPKI/SDSI. *Ágora SIC*, 2003, vol. 34.

SÁNCHEZ, J. C.; GARCÍA, J. E., *et al. Hacia una nueva identificación electrónica del ciudadano: el DNI-e* España: Safelayer, Disponible en: http://www.safelayer.com/fileadmin/pdf/DNIe.pdf.

SILVA, G. M. *Diseño e Implementación de una Autoridad Certificadora en Plataformas Móviles.* INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY, 2005.

TALAVERA, J. *Infraestructura para la Criptografía de Llave Pública.* 2005. [Consultado el: 22/01/2008] Disponible en: http://www.cnc.una.py/cms/cnc/index.php?id=0,61,0,0,1,0.

TALENS-OLIAG, S. *Introducción a los certificados digitales.* 2005,. [Consultado el: 08/01/2008] Disponible en: http://www.infocentre.gva.es/.