[VOLUMEN 34 · ABRIL 2003]

Ágora SIC Divulgación

SUMARIO

Gestión y uso de certificados de autorización SPKI/SDSI

Óscar Cánovas Reverte
Dpto.de Ingeniería y Tecnología de Computadores
Antonio F. Gómez Skarmeta
Dpto. Ingeniería de la Información y las Comunicaciones
Facultad de Informática
UNIVERSIDAD DE MURCIA

En este artículo se explica cuál es el papel de la certificación de autorización como herramienta básica de seguridad. Para ello, se muestra cómo es posible extender los servicios de identidad digital proporcionados mediante una PKI con el uso de certificados de autorización, en este caso utilizando la especificación SPKI/SDSI. Además de describir la estructura general del sistema de gestión del ciclo de vida de este tipo de certificados, este trabajo ilustra las ventajas que pueden derivarse de la integración de los servicios de autorización en entornos concretos de control de acceso, uno de los cuales, el control de acceso físico a instalaciones, se constituye en un ejemplo específico.

Gestión y uso de certificados de autorización SPKI/SDSI

INTRODUCCIÓN

Loren Kohnfelder definió en 1978 el término "certificado digital" como un documento firmado digitalmente que contiene tanto un nombre como una clave pública. La principal misión de los certificados era resolver de forma satisfactoria el problema de la autenticidad de las claves empleadas en los sistemas de criptografía de clave pública. Como consecuencia, hoy en día se utilizan los términos "certificado" y "certificado de identidad" como sinónimos. Sin embargo, una interpretación más relajada del término permite considerar un certificado como cualquier sentencia firmada que asocia cualquier tipo de información a una clave pública, por ejemplo la pertenencia a cierto grupo de usuarios o el privilegio de poder realizar cierta operación sobre un recurso. Este último uso, el de plasmar electrónicamente las potestades o competencias de cierta entidad mediante el uso de documentos firmados digitalmente, ha recibido el nombre genérico de "certificación de autorización".

El interés creciente que ha suscitado este tipo de certificación en la comunidad científica viene marcado por las limitaciones existentes en los estándares X.509 a la hora de abordar las cuestiones relacionadas con la autorización. Hemos de tener en cuenta que el principal objetivo de las PKIs ha sido el de proporcionar mecanismos que permitieran establecer una relación entre el nombre y las claves públicas de las entidades. 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 correspondiente.

A lo largo de los últimos años, han sido varias las especificaciones en materia de certificados de autorización propuestas por la comunidad científica (KeyNote, SAML, X.509 PMI, SPKI/SDSI). Todas ellas se caracterizan por proponer mecanismos concretos de gestión de pertenencia a grupos y de especificación de privilegios. Además, algunas proporcionan métodos genéricos de toma de decisiones de autorización e introducen el mecanismo de delegación de privilegios como herramienta fundamental de gestión de la autorización. Hasta el momento, SPKI/SDSI **[3]** es la propuesta más ampliamente analizada y utilizada en lo que a gestión de autorizaciones se refiere. Prueba de ello son las numerosas aportaciones realizadas por parte de la comunidad científica a lo largo de estos últimos años, así como las diversas implementaciones disponibles de código abierto.

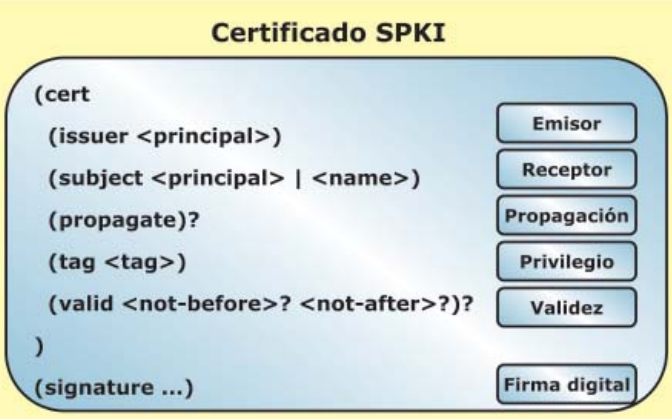

Figura 1. Certificado SPKI de autorización o atributo

Sin embargo, a pesar de la existencia de distintas propuestas, ninguna de ellas especifica cómo debe realizarse la gestión del ciclo de vida de los certificados de autorización (es decir, su creación, distribución, validación, etc.). Si bien ciertos enfoques dependientes de la aplicación pueden dar resultado en entornos reducidos, su uso en escenarios complejos puede sacar a relucir varios problemas relacionados con su escalabilidad e interoperabilidad, lo cual hace necesario plantear un sistema que sea capaz de llevar a cabo dicha gestión de forma estructurada y distribuida.

Uno de los puntos principales de este artículo es mostrar cómo se ha llevado a cabo la definición de una infraestructura de autorización basada en SPKI/SDSI. Dicha infraestructura se apoya en los modelos de control de acceso basados en roles (RBAC) y en la delegación como herramienta fundamental de gestión de las autorizaciones. La otra cuestión clave aquí presentada es mostrar las posibilidades que ofrece el uso de los certificados de autorización a la hora de diseñar entornos de control de acceso. Para ello, se describirá la solución aplicada

para resolver un problema tan clásico como el control de acceso físico a dependencias (edificios, laboratorios, almacenes, etc.).

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, 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.

El primer tipo de certificado SPKI/SDSI es el de identidad o nombramiento, el cual puede ser empleado para varios propósitos, de entre los cuales destaca su uso como mecanismo de definición de grupos de usuarios. La creación de un grupo se consigue mediante la emisión de varios certificados que asocian el mismo nombre a distintos usuarios.

Los otros dos tipos de certificados SPKI/SDSI, los de atributo y los de autorización, poseen estructura (ver **figura 1**) similar entre sí, ya que la principal diferencia se encuentra en el campo *subject*, el cual puede hacer referencia a un usuario (certificado de autorización) o a un nombre (certificado de atributo). Los certificados de autorización se emplean para asignar privilegios directamente a claves, mientras que los certificados de atributo son útiles para asignar privilegios a grupos de entidades.

GESTIÓN DEL CICLO DE VIDA DE CERTIFICADOS SPKI/SDSI

Si bien la especificación SPKI/SDSI ha sido empleada con éxito en varios escenarios de aplicación distintos, la gestión de los certificados digitales, es decir, la forma en la que los usuarios solicitan los certificados de autorización, 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 **[1]** 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. 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.

Visión general

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.

Los escenarios de control de acceso basados en el concepto de delegación y en el agrupamiento de usuarios mediante roles presentan una estructura similar a la mostrada en la **figura 2.**

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 manera, 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.

Figura 2. Estructura general de la gestión de autorización

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 de credencial que conlleve a la emisión y distribución de un porcentaje de autorizaciones 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. No obstante, los privilegios también pueden ser asignados directamente a entidades finales, es decir, a claves públicas asociadas a usuarios del sistema. Este enfoque puede emplearse en los casos en los que no se haga uso del concepto de rol, o más genéricamente, cuando no se emplee ningún tipo de identificador de usuarios además de las propias claves criptográficas.

Por otro lado, las autoridades encargadas de gestionar la pertenencia a roles se denominan bajo el nombre común de

autoridades de nombramiento. Al igual que sucedía con las autoridades de autorización, una autoridad de nombramiento puede estar formada por cualquier entidad final del sistema a la cual se le hayan reconocido los privilegios de gestión de un conjunto de nombres del sistema. Es importante recalcar que dicho conjunto de nombres no tiene por qué hacer siempre referencia a nombres de grupo, sino que puede tratarse también de un conjunto de identificadores únicos de usuario; de ahí que se les denomine con el nombre genérico de autoridades de nombramiento. En el caso concreto que aquí nos ocupa, las autoridades reflejan la pertenencia mediante el uso de certificados de identidad SPKI. Al igual que sucedía con las autoridades de autorización, cada autoridad de nombramiento está regulada por una política, en este caso denominada de nombramiento, que especifica qué elementos del sistema pertenecen a un determinado rol y durante qué periodo. Por elementos del sistema se hace referencia no sólo a entidades finales o claves públicas sino también a otros roles contenidos en uno de mayor nivel, lo cual nos lleva a la definición de jerarquías de roles.

Las entidades finales, una vez que obtienen los certificados correspondientes a partir de las autoridades del sistema, generan solicitudes de acceso a los recursos protegidos por los controladores. Dichas solicitudes deben estar firmadas digitalmente mediante la clave privada asociada a la clave pública contenida en los certificados. Una vez que esto sucede, tanto las credenciales como la solicitud se envían al controlador para que contraste la veracidad de las mismas y compruebe que existe un camino de delegación desde su propia clave pública hasta la clave pública del solicitante. Consecuentemente, la cadena de delegación se valida en el mismo punto en el cual se origina, lo cual es conocido como *bucle de autorización*.

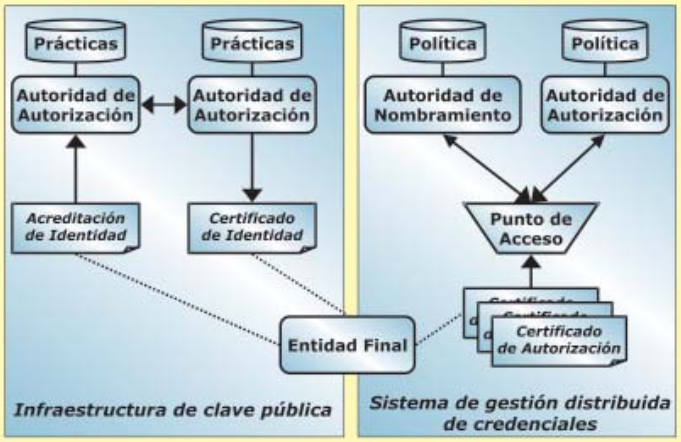

Figura 3. Extensión de una PKI mediante DCMS

Arquitectura de DCMS

El sistema DCMS se puede considerar como una extensión de los servicios proporcionados por las infraestructuras de clave pública. Mientras que las PKIs se encargan del ciclo de vida de los certificados de identidad, gestionando todas las cuestiones relacionadas con la asignación de nombres a claves, el sistema DCMS es responsable de asociar privilegios a dichas claves. Como consecuencia, tal y como muestra la **figura 3**, ambos sistemas presentan algunas similitudes en lo que a estructura y funcionalidad se refiere.

En primer lugar, ambas necesitan una infraestructura formada por entidades emisoras, entidades intermedias (o mediadoras) y usuarios finales. En el caso de la PKI, las autoridades de registro y las autoridades de certificación cooperan para tramitar las solicitudes de certificación presentadas por las entidades finales. En el caso de la infraestructura de autorización, es necesaria la presencia de elementos encargados de emitir los distintos tipos de credencial (autoridades de nombramiento y de autorización), así como la intervención de elementos intermedios capaces de poner en contacto a dichas autoridades con las entidades finales (puntos de acceso). Además, parte de ambas infraestructuras deben ser las especificaciones relacionadas con el formato de las solicitudes de certificación y formato de las políticas de seguridad. Por otro lado, en ambos casos las entidades emisoras deben seguir políticas concretas de certificación a la hora de atender las solicitudes presentadas por los usuarios finales. Para la PKI, las prácticas de certificación imponen los requisitos que deben cumplir las solicitudes y los certificados. En el caso de la infraestructura de autorización, el uso de políticas permitirá determinar si una entidad concreta puede ser asociada a un conjunto de roles o de privilegios.

A partir de la **figura 3** se pueden apreciar la entidades principales que forman parte del sistema DCMS:

– *Solicitante*. Son los usuarios que desean obtener un nuevo certificado SPKI. Para ello generan una solicitud de certificación y la envían a una autoridad en particular con el fin de obtener el certificado solicitado. Este envío puede realizarse a través de un punto de acceso o bien mediante una conexión directa entre solicitante y autoridad. La solicitud podrá estar acompañada de otros certificados con el fin de satisfacer la política de seguridad de la autoridad.

– *Punto de acceso al servicio*. Los solicitantes pueden hacer uso de los puntos de acceso a la hora de enviar sus solicitudes de certificación a las autoridades apropiadas. Si bien los puntos de acceso son elementos opcionales, pueden ser considerados elementos muy útiles para los solicitantes, ya que ocultan la localización concreta de las distintas autoridades, lo cual puede ser conveniente en escenarios con varias autoridades donde resulta complicado averiguar qué autoridad es la indicada para emitir ciertos certificados.

– *Autoridades*. Las autoridades emiten certificados SPKI en función de las solicitudes recibidas a través de los puntos de acceso o bien directamente de los solicitantes. Están controladas por políticas concretas que determinan los requisitos mínimos para obtener los certificados. Cuando una autoridad recibe una solicitud y los posibles certificados adicionales, ejecuta un algoritmo de cálculo de autorizaciones con el fin de determinar si la solicitud debe aprobarse o no.

– *Políticas*. Se trata de documentos digitales que condicionan la toma de decisiones de las autoridades. Una política establece el conjunto válido de solicitantes de certificados SPKI así como los permisos que pueden obtenerse y la posibilidad de delegarlos.

APLICACIÓN AL CONTROL DE ACCESO FÍSICO

El control de acceso físico implica la provisión de mecanismos que impidan la entrada de usuarios no autorizados a determinados recintos, tales como laboratorios de investigación, despachos o almacenes. Estamos hablando de un problema clásico, en el cual hay un conjunto de aspectos muy definidos a los que debe aportarse solución. En primer lugar, encontramos el problema de la distribución de claves, es decir, cómo proporcionar las claves apropiadas a los usuarios autorizados que pueden hacer uso de ellas. En relación con esto, las claves pueden ser canceladas o revocadas como respuesta a ciertas situaciones que impliquen una amenaza de seguridad. Por otro lado, es necesario especificar cómo será gestionada la información de los usuarios, es decir, sus datos personales y sus privilegios de acceso.

La mayor parte de los sistemas actuales de control de acceso físico siguen un enfoque claramente centralizado basado en el uso de algún tipo de tarjeta inteligente. Por ejemplo, una situación típica es la de un usuario que dispone de datos identificativos que presenta a un dispositivo especial localizado a la entrada de un recinto concreto. En estos entornos clásicos, el dispositivo no conoce qué identificadores son válidos por lo que debe realizar una consulta a la base de datos central para obtener los privilegios del usuario en cuestión. Dicha base de

datos contiene una tabla por cada uno de los dispositivos que se encuentran instalados, y cada tabla está compuesta por distintos registros que contienen, entre otros campos, un identificador de usuario y el conjunto de permisos asignados al mismo. Cuando un usuario es autorizado a realizar una acción determinada se introduce un nuevo registro en la tabla asociada al dispositivo correspondiente. Por el contrario, si se desea anular los permisos de cierto usuario basta con eliminar de la base de datos el registro correspondiente. En lo que respecta a la verificación de usuarios, ésta se realiza mediante una consulta remota a la base de datos. Con el fin de garantizar la integridad de los datos intercambiados y la autenticidad de los interlocutores, es aconsejable utilizar conexiones SSL entre cada uno de los dispositivos y los servidores de aplicación que acceden a la base de datos.

Si bien esta propuesta centralizada se está utilizando de forma satisfactoria en muchos entornos y proporciona soluciones a la mayoría de los problemas relacionados con el control de acceso, presenta algunas carencias que pueden ser solventadas siguiendo un enfoque descentralizado basado en el uso de certificados de autorización.

En primer lugar, el enfoque centralizado requiere una conectividad permanente con la base de datos central. Cuando ésta se rompe, los dispositivos podrían continuar proporcionando servicio basándose sólo en las copias locales de la información de autorización. De hecho, en algunos entornos no resulta sencillo disponer de conectividad a la red de comunicaciones, lo cual impide poder utilizar un enfoque de este tipo. Sería aconsejable que el sistema de control de acceso fuera realmente distribuido, no por el hecho de estar basado en dispositivos distribuidos geográficamente sino por la posibilidad de ejercer sus funciones sin depender de un punto central. El uso de certificados de autorización permite que los terminales puedan operar en modo desconectado y puedan determinar si un usuario está autorizado a realizar la acción solicitada sin necesidad de consultar a ninguna entidad externa.

Por otro lado, si el escenario en el cual se desarrolla en sistema de control de acceso está constituido por una comunidad de usuarios extensa, la tarea de gestionar cada dispositivo, la lista de usuarios autorizados o la copia local de la información de autorización puede resultar muy compleja. Una solución más acertada es definir grupos de usuarios a los cuales asignar conjuntos de permisos en lugar de gestionar cada usuario de forma individual. No obstante, realizar dicha definición haciendo uso de una base de datos central presenta los mismos problemas derivados de la falta de conectividad que aparecían en el caso de las autorizaciones individuales. Una vez más, una solución más apropiada sería emplear certificados de autorización para codificar tanto la pertenencia a grupos como la asignación de permisos a dichos grupos.

Por último, la propuesta centralizada carece de mecanismos robustos de no repudio de solicitante. Es cierto que tanto la base de datos como los dispositivos realizan apuntes de las acciones que han sido solicitadas por los usuarios; sin embargo, dichos apuntes no constituyen un mecanismo robusto de cara a ser utilizados como prueba de no repudio. La información registrada es susceptible de ser modificada por cualquier intruso capaz de acceder a parte de la información almacenada en la base de datos. Aunque es posible utilizar algunas soluciones basadas en el cifrado de datos para almacenar información confidencial en sistemas no confiables, lo realmente necesario es poder disponer de información generada por el solicitante, y no por los dispositivos o la propia base de datos, que pueda ser utilizada como una evidencia irrefutable de las peticiones realizadas. Para ello, tal y como se vio en el apartado anterior, es conveniente que las solicitudes de servicio vayan firmadas digitalmente por los usuarios. De esta forma podrán ser utilizadas, junto con las decisiones de autorización, para adoptar las medidas pertinentes tras un incidente de seguridad.

Nuestro grupo de investigación ha desarrollado un sistema descentralizado de control de acceso físico **[2]** completamente basado en el uso del sistema DCMS, lo que implica que la gestión de las autorizaciones se realice según el esquema RBAC y el mecanismo de delegación de privilegios. Por un lado, el esquema RBAC permite separar la gestión de la pertenencia de los usuarios a roles de la asignación de privilegios concretos a dichos roles, lo cual simplifica enormemente la gestión de las autorizaciones. La pertenencia se implementa mediante la emisión de certificados SPKI de identidad mientras que la asignación de privilegios a los roles se realiza mediante certificados SPKI de atributo. Los certificados de pertenencia se almacenan siempre en la tarjeta inteligente del usuario asociado, el cual dispone de un par de claves asimétricas. Los certificados de atributo pueden ser almacenados tanto en las tarjetas de los usuarios como en los propios dispositivos.

Por otro lado, la delegación de privilegios permite que los dispositivos asignen la responsabilidad de la gestión de los mismos a entidades externas que actuarán como autoridades. De esta forma, el dispositivo no es sólo el punto de cumplimiento de la política de control de acceso sino también el inicio de la cadena de autorización. El dispositivo es capaz de tomar decisiones de autorización analizando tanto los certificados de credencial que mantiene almacenados como los presentados por los usuarios. El usuario presenta al dispositivo solicitudes de acceso firmadas digitalmente mediante su clave privada. A continuación, el dispositivo intenta construir una cadena de certificados que partiendo de él mismo sea capaz de llegar hasta la clave pública del usuario pasando por las distintas autoridades del sistema. En el caso de que logre hallar una prueba de autorización, el dispositivo lleva a cabo la acción correspondiente y almacena dicha prueba con el propósito de registrar evidencias que puedan ser utilizadas en caso de incidencia.

CONCLUSIONES

La certificación de autorización ofrece una nueva gama de servicios orientados a complementar las funciones básicas de las infraestructuras de clave pública. En este sentido, cobra especial sentido 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. Las propuestas introducidas en este artículo muestran cómo es posible utilizar los modelos basados en roles y la delegación con el fin de diseñar infraestructuras de certificación de privilegios capaces de dar soporte a entornos distribuidos claramente descentralizados. ❖

Óscar Canovas Reverte
Profesor Ayudante de Universidad
Dpto.de Ingeniería y Tecnología de Computadores
ocanovas@um.es

Antonio F. Gómez Skarmeta
Profesor Titular de Universidad
Dpto. de Ingeniería de la Información y las Comunicaciones
skarmeta@dif.um.es

Facultad de Informática
UNIVERSIDAD DE MURCIA

REFERENCIAS

[1] O. Cánovas y A. F. Gómez. *A Distributed Credential Management System for SPKI-Based Delegation Scenarios.* En Proceedings of 1st Annual PKI Research Workshop, pp. 65-76. Abril 2002

[2] O. Cánovas, A. F. Gómez, H. Martínez y G. Martínez. *Different Smartcard-based Approaches to Physical Access Control*. En Proceedings of Infrastructure Security Conference 2002, volumen 2437 de Lecture Notes in Computer Science, pp. 214-226. Springer Verlag, octubre 2002

[3] C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas y T. Ylonen. *SPKI Certificate Theory*, Septiembre 1999. Request For Comments (RFC) 2693.