Estandarización de servicios de autorización para aplicaciones de Internet

Standardization of Authorization Services for Internet Applications

J. López Muñoz y J. A. Montenegro

Resumen

La continua aparición de aplicaciones que hacen uso de Internet, como es el caso del comercio electrónico, necesitan de la utilización, además de los servicios de Autenticación, de los servicios de Autorización. Esta necesidad ha provocado la aparición de un marco de trabajo, por parte de la ITU, para cubrir las necesidades que anteriormente tenían las Infraestructuras de Clave Pública para cubrir los servicios de Autorización. Actualmente el concepto de certificado X.509 se ha diversificado, obteniéndose dos tipos de certificados, los certificados de identidad y los certificados de atributos. Los certificados de atributos son el mecanismo necesario para vincular los privilegios a los usuarios y posibilita especificar una vinculación con los certificados de identidad, proporcionándose así una Infraestructura de Autenticación y Autorización (AAI), mediante la unión de las PKI y las PMI.

Palabras clave: Autorización, Autenticación, Certificados de Atributos, Certificados de Identidad, PKI, PMI, AAI, Autoridad de Atributos (AA), Fuente de Autoridad (SOA), Delegación de Privilegios.

Summary

With the continuous appearance of applications using Internet –as is the case of electronic commerce–, the use of Authorization Services apart from Authentication Services is required. The ITU 2000 framework appears to cover the previous necessity not covered by Public Key Infrastructure, the Authorization Services. Actually the certificate X509 concept has been diversified and now we have two types of certificate, the identity and the attribute certificate. The last one allows binding the privilege to users, and in addition it is possible to tie up an attribute certificate to an identity certificate. This link provides a new Infrastructure, the Authentication and Authorization Infrastructure (AAI wich is the result of the union between Public Key Infrastructure (PKI) and Privilege Management Infrastructure (PMI).

Keywords: Authorization, Authentication, Attribute Certificates, Identity Certificates, PKI, PMI, AAI, Attribute Authority (AA), Source of Authority (SOA), Privilege Delegation

Actualmente el concepto de certificado X.509 se ha diversificado, obteniéndose dos tipos de certificados, los certificados de identidad y los certificados de atributos

1.- Introducción

Actualmente, los certificados digitales de identidad proporcionan, en la mayoría de las ocasiones, la solución más adecuada para dotar del Servicio de Autenticación a la totalidad de las aplicaciones desarrolladas para Internet. Sin embargo, existen entornos, como el caso del comercio electrónico, donde no es suficiente con probar quién se es, además es necesario proporcionar un mecanismo que detalle qué se tiene permitido hacer, es decir un Servicio de Autorización. El concepto de Servicio de Autorización no es nuevo, y se han desarrollado muchas soluciones que podríamos denominar "tradicionales" para resolver ese problema. Sin embargo, el problema de la escalabilidad es aún una asignatura pendiente.

Este trabajo presenta un marco de trabajo que permite resolver los problemas de escalabilidad presentes en las soluciones tradicionales. La estrecha vinculación con los certificados digitales de identidad y con las *Infraestructuras de Clave Pública* (PKI) sitúa esta solución en un lugar privilegiado para su implantación. La unión de los Servicios de Autorización y de Autenticación supone la creación de la Infraestructura de Autenticación y Autorización (AAI), que es la evolución más significativa de las PKIs.

El marco de trabajo de los certificados de atributos también define los componentes de una Infraestructura de Administración de Privilegios, que es el nuevo tipo de infraestructura creada para la gestión de atributos y privilegios de usuarios

2.- PKIs como Servicio de Autorización

Las PKIs no son las herramientas apropiadas para las aplicaciones que necesitan de Servicios de Autorización. La principal razón de esta afirmación es que los elementos básicos de la PKIs son los certificados de identidad y su razón de ser no es dar cobertura a los problemas de autorización.

Anteriormente, en la especificación de la ITU de 1997, se proporcionaba –dentro del estándar– una alternativa al uso de los certificados de atributos, como era la inclusión de los atributos del usuario dentro del certificado de identidad, a través de la extensión *Subject Directory Attributes*. Esta última solución, aunque puede ser válida para problemas triviales, resulta insuficiente ante un sistema con un uso intensivo del Servicio de Autorización.

La razón fundamental es que los certificados de identidad están pensados para un periodo de vigencia relativamente largo en comparación con los derechos de acceso o los privilegios del usuario, los cuales poseen un dinamismo mayor relativo al cambio de estado. Esto produce una inevitable avalancha de revocaciones que provoca en el sistema una reducción de la funcionalidad, disminuyendo la calidad del servicio prestado.

Además, el servicio de autorización posee ciertas características adicionales intrínsecas, como la delegación y sustitución transitoria, que no son soportadas mediante el uso de los certificados de identidad.

3.- Introducción de un nuevo tipo de infraestructuras: las PMIs y sus componentes

En su revisión del año 2000 del X.509, la ITU dio un paso más hacia la solución de esta problemática. Esta revisión ha definido formalmente el marco de trabajo para los certificados de atributos, e incluye la especificación de los objetos de datos utilizados para representar este tipo de certificados.

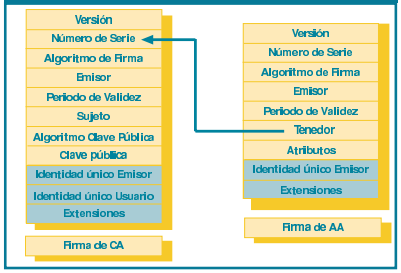
Los certificados de atributos están firmados por una *Autoridad de Atributos* (AA), que es como se pasa a denominar a la autoridad habilitada para realizar la asignación de privilegios y que, según la ITU, no tiene por qué ser la misma que la que emite certificados de identidad. Además, el marco de trabajo de los certificados de atributos también define los componentes de una *Infraestructura de Administración de Privilegios* (PMI), que es el nuevo tipo de infraestructura creado para la gestión de atributos y privilegios de usuarios.

Respecto a la estructura del certificado de atributos, se observa en la parte derecha de la figura su parecido con la de los certificados de identidad, encontrando en ella los campos habituales de *versión*, *número de serie*, *algoritmo de firma*, *emisor*, *periodo de validez*, e incluso los campos opcionales *identificador único de emisor* y de *extensiones*. Existen, sin embargo, otros campos nuevos, como son el campo *tenedor*, y el propio campo de *atributos*, que podrá contener información respecto a la pertenencia a grupos, identificación de cargos, valores límite de transacciones, horas de realización de ciertas operaciones, límites temporales, etc.

Es conveniente resaltar que, a diferencia de lo que ocurre en el certificado de identidad, es posible no dejar explícita la identificación del usuario en el certificado de atributos, sino que utiliza el campo *tenedor* para enlazar este certificado con el correspondiente certificado de identidad del usuario, como muestra la figura, mediante la utilización en el campo tenedor del número de serie del certificado de identidad del usuario sobre el que se expresan los atributos o privilegios. De esta forma, la PKI autentica a aquellos usuarios de quien la PMI emite certificados de atributos.

Ésta no es la única solución, como alternativa, el campo *tenedor* puede contener el valor resumen de la clave pública, o bien el del certificado de identidad completo. Lógicamente podrá contener el identificador del usuario en el caso de que no exista vínculo con una PKI cuando se dé el caso que la PMI coexista con algún otro esquema de autenticación.

ESTRUCTURA DE LOS CERTIFICADOS DE ATRIBUTOS Y SU RELACIÓN CON LOS CERTIFICADOS DE IDENTIDAD



De la herencia aportada por las PKIs, existen denominaciones paralelas en las PMIs. La entidad, *Fuente de Autoridad* (SOA), es un tipo específico de AA, y desempeña un papel análogo al de la Autoridad Raíz en las PKIs. A la SOA se le considera la responsable última en la asignación de un conjunto de privilegios. En cuanto al concepto de revocación, tenemos la *Lista de Revocación de Certificados de Atributos Revocados* (ACRL) con el mismo formato y administración que las típicas CRLs.

Se pueden usar varios modelos de PMI 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

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.

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 *tenedor 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 tenedor son suficientes como para realizar una determinada operación sobre el objeto. La decisión sobre si el verificador permite o no al tenedor realizar la operación solicitada se basa en cuatro factores: *privilegios del tenedor*, *política de privilegios*, *variables de entorno* y *sensibilidad del método del objeto*.

El *modelo de control*, o de control de accesos, se usa básicamente para esas aplicaciones y muestra cómo el verificador controla el acceso al método del objeto, por parte del tenedor, 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 tenedor 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 SOA es la responsable de la asignación inicial de privilegios, y autoriza al tenedor a actuar como una AA. Ésta puede a su vez delegar en otra AA todos o parte de

Algunas de las iniciativas más avanzadas en el ámbito de los servicios de autorización son:
• El Proyecto PERMIS
• La Arquitectura AAAARCH
• El Proyecto AKENTI
• El proyecto PAPI

esos privilegios que posee, o bien delegar directamente 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 tenedores.

5.- Ejemplos de arquitecturas

En este apartado se describen muy brevemente algunas de las iniciativas más avanzadas en el ámbito de los servicios de autorización.

El Proyecto PERMIS (PrivilEge and Role Management Infrastructure Standards validation) es un proyecto europeo del V Programa Marco que comenzó en enero de 2001 y finalizará en el próximo mes de septiembre. En este proyecto se aboga por el uso de un esquema PKI+PMI en el que las autoridades son siempre entidades diferentes para una y otra infraestructura. Su objetivo es el uso de los certificados de atributos para aplicaciones de control de acceso.

La Arquitectura AAAARCH (Authentication, Authorization and Accounting ARCHitecture) nace de un grupo de investigación del IRTF (Internet Research Task Force). Sus objetivos son definir una generación de arquitecturas que incorporen un conjunto de servidores AAA genéricos interconectados y los interfaces (a alto nivel y de forma abstracta) entre los diferentes componentes de la arquitectura. Esta se centra en dar soporte de servicios AAA que: (i) puedan interoperar a través de los límites de las organizaciones, (ii) sean extensibles a la mayoría de los servicios de Internet, (iii) contengan mecanismos de seguridad acordes con las políticas locales y (iv) proporcione mecanismos independientes de administración de sesiones.

El Proyecto AKENTI es un proyecto originario del Lawrence Berkeley National Laboratory, y se centra también en el control de accesos. Este trabajo estudia los problemas de las aplicaciones de acceso restringido a recursos que están controlados por más de una entidad. Su objetivo de diseño es alcanzar en las aplicaciones de control de accesos un nivel de expresividad similar al humano, reflejando en la políticas de acceso cuestiones de autorización, privilegios y responsabilidad. Por otro lado, no se utilizan certificados de atributos X.509, sino certificados propios. Tampoco se hace uso de una PMI, sino de un servidor, denominado servidor Akenti, que analiza los certificados y concede el acceso a los recursos. Sin embargo, sí hace uso de una PKI que gestiona certificados de identidad X.509, utilizados por el servidor anteriormente mencionado a la hora de la toma de decisiones.

El proyecto PAPI (Punto de Acceso a Proveedores de Información) es un sistema para el control de acceso a la información ofrecida a través de Internet. Su principal característica, como su nombre indica, es que proporciona un punto de acceso común a los proveedores de información. Para alcanzar dicho objetivo, los procedimientos para la autenticación de un usuario son cuestiones locales para la organización a la que el usuario pertenece, facilitando de esta forma la administración, mientras que los proveedores de información mantienen el control sobre el acceso a los recursos que ellos ofrecen.

Javier López Muñoz
(jlm@lcc.uma.es)
José A. Montenegro Montes
(monte@lcc.uma.es)
Dpto. de Lenguajes y Ciencias de la Computación
ETSI Informática - Universidad de Málaga