# Retos y oportunidades de los sistemas de control de acceso basados en delegación

## Delegation in Distributed Systems: Challenges and Opportunities

O. Cánovas y A. F. Gómez Skarmeta


### Resumen

Los nuevos sistemas de control de acceso DAC y RBAC basados en certificados digitales hacen uso de la operación de delegación de privilegios. En este tipo de escenarios, los controladores de recursos normalmente disponen de una lista de control de acceso que delega la gestión de los derechos de acceso a entidades conocidas como autoridades de autorización. Estas autoridades pueden emitir certificados que deleguen dichos permisos a otras autoridades subordinadas o a usuarios finales directamente. De esta forma, la estructura de certificados generados refleja la forma en la que se gestiona la autorización. En este artículo se realizará un breve análisis de las diferentes cuestiones relacionadas con la delegación, como la gestión de privilegios, diferencia entre autoridad y posesión, anonimato y revocación.


**Palabras clave:** Certificado digital, autoridad de autorización, control de acceso, delegación, revocación.


### Summary

New DAC and RBAC certificate-oriented access control systems are based on delegation of privileges. In these scenarios, resource guards have an ACL which delegates to some authorization or naming authorities the right to manage the access to the controlled resources. These authorities can issue certificates delegating these permissions to other subordinates authorities, or to specific users. In this way, the generated structure reflects the way the authorization is managed. In this paper we present a survey of different issues related to certificate-based delegation, such as management structures, authority and ownership, anonymity, certificate distribution, and revocation.


**Keywords:** Digital Certificate, Authorization Authority, Access Control, delegation, revocation.

Los nuevos sistemas de control de acceso DAC y RBAC basados en certificados digitales hacen uso de la operación de delegación de privilegios

## 1.- Introducción

Durante los últimos años se han introducido multitud de propuestas distintas en lo relativo a modelos de autorización y control de acceso en sistemas distribuidos. El esquema más conocido es el control de acceso discrecional (DAC, Discretionary Access Control), mediante el cual los permisos se especifican haciendo uso de listas de control de acceso almacenadas en cada controlador de recursos. Sin embargo, hoy en día nos encontramos ante un panorama en el cual los sistemas actuales de computación comienzan a ser altamente distribuidos (por ejemplo los entornos de Grid Computing), con varias organizaciones implicadas, cada una con sus correspondientes políticas de seguridad. Este cambio de escenario conlleva la necesidad de redefinir los modelos de autorización en busca de un mecanismo que sea capaz de absorber el dinamismo propio de este tipo de sistemas distribuidos, ya que actualmente gestionar cómo los cambios dentro de la organización afectan al sistema de control de acceso puede ser en ocasiones una tarea ardua.

Los nuevos enfoques DAC requieren un mecanismo que soporte la delegación de privilegios entre las distintas entidades de un sistema (especialmente a lo largo de los niveles jerárquicos de una organización). La herramienta básica para realizar esta operación son los certificados digitales. Especialmente interesantes son los certificados de autorización, ya que son capaces de ligar capacidades o permisos a las entidades (e incluso la posibilidad de que éstas lo propaguen a su vez). De esta forma, resulta sencillo codificar a qué están autorizadas las entidades de un sistema.

La idea principal que hay detrás del concepto de delegación es que los controladores de recursos proporcionan el privilegio de gestionar los permisos a entidades específicas denominadas autoridades. Estas autoridades pueden emitir certificados que asignen dichos permisos a otras

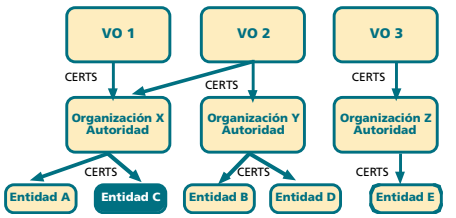
autoridades subordinadas o directamente a usuarios finales. En este artículo se analizarán algunos retos y oportunidades de los sistemas basados en delegación.

La delegación, a través de los certificados digitales, puede actuar como guía a la hora de establecer estructuras organizativas de gestión de autorizaciones que pueden ser modificadas dinámicamente

## 2.- La delegación como patrón de gestión de autorizaciones

La delegación, a través de los certificados digitales, puede actuar como guía a la hora de establecer estructuras organizativas de gestión de autorizaciones que pueden ser modificadas dinámicamente. En contraste con los esquemas clásicos basados en listas de control de acceso (ACL), el control de los derechos de acceso se encuentra ampliamente distribuido entre varias entidades confiables, lo cual simplifica el proceso de gestión al estar cada entidad encargada de gestionar sólo un subconjunto de permisos y usuarios. La figura 1 muestra un ejemplo de estructura de delegación basado en un escenario de Grid Computing. Este escenario supone que los controladores de los recursos de computación compartidos han delegado la gestión de los permisos de acceso a las autoridades de autorización de las organizaciones virtuales implicadas (VO). Como se puede apreciar, por un lado, la estructura generada por la emisión de los certificados refleja la estructura de la organización, y por otro lado, conseguir que un usuario pueda hacer uso de los recursos es tan sencillo como generar un certificado nuevo (por ejemplo el certificado de la entidad C), sin que ello conlleve la modificación de ninguna de las listas de control de acceso o políticas de seguridad existentes.

**FIGURA 1: ESTRUCTURA DE AUTORIZACIÓN BASADA EN DELEGACIÓN**




Una consecuencia directa de este estilo de gestión es la aparición de cadenas de delegación, es decir, un conjunto de certificados que contribuyen a que un cierto conjunto de permisos vaya propagándose de unas entidades a otras. Uno de los retos de los sistemas de delegación es llevar a cabo una gestión eficiente de este tipo de cadenas. Hemos de tener en cuenta que las decisiones de autorización basadas en cadenas largas pueden ser complejas, tanto desde el punto de vista computacional como desde la consideración del conjunto de recursos que se necesita para almacenarlas, obtenerlas desde repositorios o verificarlas. Además, desde el punto de vista de un atacante, las cadenas de delegación revelan demasiada información acerca del sistema (autoridades, permisos, control de propagación, entidades finales, etc.). Esto conlleva que en algunos entornos la información contenida en dichos certificados se considere confidencial y por tanto se proteja la privacidad de estas cadenas.

Una de las técnicas empleadas para solucionar algunos de los retos anteriormente planteados es llevar a cabo una reducción de las cadenas de delegación [1]. La clave de esta técnica es emitir un único certificado que aglutine toda la información contenida en la cadena de certificación, es decir, un certificado equivalente que conceda los mismos privilegios a la entidad final que se derivan de la unión de los certificados de la cadena. Este certificado, emitido por la raíz de la cadena, no contiene datos de las entidades intermedias, aportando confidencialidad, y además simplifica el proceso de obtención y validación de permisos, incrementa la eficiencia.

Ahora bien, el proceso de delegación conlleva intrínsecamente otro reto a resolver: ser capaz de especificar y hacer cumplir qué entidades están autorizadas a recibir o propagar los permisos delegados. Para ello existen varias propuestas que a continuación se describen brevemente:

- *Control booleano*. Especificar si la entidad que recibe el privilegio está a su vez autorizada para propagarlo. La principal pega de esta técnica es que no es posible implementar un control fino.
- *Control en profundidad*. Especificar el número máximo de niveles en que se puede propagar el privilegio. La principal desventaja es que no limita el número de veces en el mismo nivel.
- *Control umbral*. Establecer el número de entidades necesarias que deben actuar en conjunto para conceder un privilegio. De esta forma se limita que una única entidad se comporte de forma inapropiada, puesto que necesita la ayuda de otras.
- *Control basado en sintaxis o semántica*. La técnica consiste en especificar en los certificados las condiciones que debe cumplir la entidad receptora de un permiso, por ejemplo condiciones como la pertenencia a un grupo o la posesión de otro privilegio distinto.

Uno de los tópicos más controvertidos sobre el control de acceso es dilucidar si un administrador puede también ejercer los permisos que está otorgando

## 3.- Autoridad y posesión de permisos

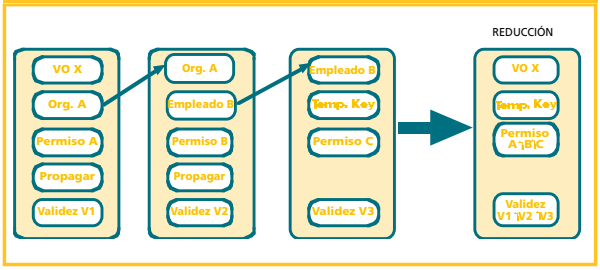
Uno de los tópicos que más controversia ha producido en la literatura sobre control de acceso es dilucidar si un administrador puede también ejercer los permisos que está otorgando. Aunque parece que no hay acuerdo generalizado, lo que resulta evidente es que un sistema de control de acceso debería ser lo suficientemente flexible como para permitir que ambas opciones se pudieran materializar. En principal problema es que los esquemas actuales de certificación (X.509, SAML) no permiten realizar ese tipo de control, puesto que resulta muy difícil evitar que un administrador se otorgue privilegios a sí mismo con otra apariencia (otra clave pública, por ejemplo).

Otra cuestión relacionada es la implementación de un servicio de transferencia de privilegios. Se ha de tener en cuenta que emitir un certificado no invalida otros certificados existentes, es decir, el emisor no pierde sus privilegios. Sin embargo, la transferencia implica la revocación de los privilegios del emisor, es decir, la asignación y revocación debe realizarse de forma atómica. Dado que con los actuales sistemas de certificación es imposible demostrar que una entidad no tiene cierto privilegio (no se permiten las sentencias negativas), la implementación de un servicio de transferencia es otro desafío a resolver.

## 4.- Anonimato

Aunque pudiera parecer que la presencia de gran cantidad de certificados limita el anonimato de los usuarios que acceden a los recursos, para aquellos entornos en los que dicho anonimato resulte un requisito, es posible aplicar la técnica de la reducción para hacer que el usuario actúe de incógnito. La figura 2 ilustra este método basado en el uso de claves temporales no registradas, y de corta duración, como medio para ocultar la identidad. Dado que las claves públicas de los usuarios suelen estar asociadas a nombres mediante certificados X.509, la presencia en los certificados reducidos de claves temporales elimina toda huella.

FIGURA 2: REDUCCIÓN PARA CONSEGUIR ANONIMATO



Los certificados de autorización deben ser revocados cuando los permisos especificados dejen de ser válidos

## 5.- Revocación de certificados de delegación

Los certificados de autorización 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 identidad en las PKIs, es que debemos distinguir entre dos tipos: la revocación sencilla de un usuario final, y la revocación más compleja de una entidad intermedia 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 intermedia puede conllevar también una revocación propagada, es decir, la anulación de todos o parte de los privilegios emitidos por dicha entidad. Quizá sea fácil entender esto si vemos a dicha entidad como un jefe de sección que ha podido emitir privilegios en el pasado y que ahora ha sido sustituido. Nos encontraremos ante una revocación propagada sólo en el caso en el que se haya demostrado una actitud inapropiada en el jefe, en otro caso se podría decidir mantener los privilegios propagados. Para implementar este último tipo de revocación es necesario hacer uso de sellos de tiempo y periodos de inhabilitación, tal y como se explica en [2], lo que constituye un campo abierto de investigación, dado que los esquemas actuales de certificación no incluyen este tipo de elementos.

### Referencias


[1] O. Cánovas Reverte, *Propuesta de una infraestructura de clave pública y su extensión mediante un sistema distribuido de gestión de credenciales basado en delegación y roles*. Tesis Doctoral. Universidad de Murcia. Enero 2003. URL: http://ditec.um.es/~ocanovas/phd.html

[2] B. Sadighi and M. Sergot, Revocation Schemes for Delegated Authorities. *Proceedings of IEEE 3rd International Workshop on Policies for Distributed Systems and Networks*, 2002.



**Óscar Cánovas Reverte**
(ocanovas@um.es)
Dpto. de Ingeniería y Tecnología de Computadores
**Antonio F. Gómez Skarmeta**
(skarmeta@um.es)
Dpto. de Ingeniería de la Información y las Comunicaciones
Facultad de Informática
Universidad de Murcia