(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 656 115**

(51) Int. CI.:

G06F 17/30 (2006.01)
G06F 21/62 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **28.09.2011 E 14197287 (7)**

(97) Fecha y número de publicación de la concesión europea: **18.10.2017 EP 2863333**

(54) Título: **Un método, un aparato, un sistema de ordenador, un componente de seguridad y un medio legible por ordenador para definir derechos de acceso en una disposición de archivos basada en metadatos**

(30) Prioridad:

29.09.2010 US 924625

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.02.2018

(73) Titular/es:

M-FILES OY (100.0%)
Hermiankatu 1
33720 Tampere, FI

(72) Inventor/es:

LAITKORPI, MARKKU;
NIVALA, ANTTI;
LEPOLA, JUHA;
METSÄPELTO, ARI y
PARTANEN, TIMO

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Un método, un aparato, un sistema de ordenador, un componente de seguridad y un medio legible por ordenador para definir derechos de acceso en una disposición de archivos basada en metadatos

Campo de la invención

La presente invención se refiere a definir derechos de acceso para objetos en un sistema informático.

Antecedentes de la invención

En un sistema informático, una lista de control de acceso (ACL) es una solución de un modelo de seguridad para dar permisos a usuarios para acceder a un objeto almacenado electrónicamente. Una ACL especifica qué usuarios y/o grupos de usuarios están autorizados para acceder a objetos y qué operaciones se permiten sobre objetos dados. Las operaciones pueden incluir leer (“R”) de un objeto, escribir (“W”) en un objeto, borrar (“D”) un objeto, y ejecutar (“X”) un objeto. Tradicionalmente los usuarios se identifican por su nombre, y los grupos por sus miembros.

Además del control de acceso basado en nombre, hay una solución para un control de acceso basado en el rol. En tal sistema, el permiso para realizar cierta operación se asigna a un rol específico en lugar de a un nombre. Esto facilita el trabajo de mantenimiento debido a que la ACL no tiene que ser actualizada cada vez que se añade un nuevo usuario a una cierta función de trabajo.

Las soluciones antedichas se derivan de la denominada estructura de carpetas tradicional, donde las carpetas están situadas en una jerarquía de carpetas estática. Por lo tanto, también las ACL están limitadas a una única jerarquía de derechos de acceso. De manera similar, los roles de acceso a menudo se asignan estáticamente a partir de un conjunto predefinido de usuarios de grupos de usuarios.

Una publicación US 2008/0155652 describe un método y un sistema para usar una regla de ACL para generar una ACL para un documento incluido en un plano de archivos. Un plano de archivos incluye una pluralidad de contenedores, en donde cada contenedor es capaz de proporcionar información de gestión para documentos en el plano de archivos. Una regla de ACL indica una de una pluralidad de reglas de ACL, en donde las reglas de ACL proporcionan diferentes formas para formar unas ACL de documento de plan de archivos usando al menos una ACL definida para un contenedor y una ACL de documento de plan de archivos previos indicando usuarios habilitados para acceder al documento antes de que el documento se añada al plan de archivos. Una solicitud para añadir un documento al plan de archivos se recibe y una ACL de documento de plan de archivos se genera según la regla de ACL definida. La ACL de documento de plan de archivos está asociada con el documento en el plan de archivos.

Una publicación US 2007/0174031 describe un método para tomar una decisión de políticas. El dispositivo de decisión de políticas tiene acceso a objetos que son relacionables entre sí mediante relaciones de uno o más tipos de relación. El método comprende recibir una solicitud para la decisión de políticas, la solicitud que especifica un primer objeto de los objetos y solicitud de información, obtener una política que coincide con la solicitud de información y que es aplicable a un segundo objeto de los objetos, obtener al menos una regla de propagación asociada con la política, la al menos una regla de propagación que especifica al menos un tipo de relación del uno o más tipos de relación, verificar si existe un camino de relación, el camino de relación que enlaza el primer objeto y el segundo objeto, y que consta de una o más de las relaciones, verificar si una o más relaciones del camino de relación está de acuerdo con al menos uno del al menos un tipo de relación especificada, y si dicho camino de relación está de acuerdo, aplicar la política al primer objeto tomando la decisión de política.

Una publicación US 2002/0088000 describe un método para controlar el acceso a metadatos de imagen. El método incluye asociar usuarios que accederán a la imagen con roles, y asociar los roles con elementos de metadatos individuales. En respuesta a recibir una solicitud de acceso a los metadatos por un usuario particular, el rol del usuario se determina a partir de la solicitud y el rol del usuario se compara con los roles asociados con los elementos de metadatos para determinar qué elementos de metadatos poner a disposición del usuario.

Una publicación US 2006/0010483 describe un método para definir tipos de roles mediante asociación con ciertas acciones permisibles. Por lo tanto, un tipo de rol se puede limitar entonces a nodos de árbol jerárquico que representen recursos basados en ordenador tales como espacios de objetos dinámicos. Una vez vinculado a un nodo, se crean casos de ese tipo de rol que serán heredados por los descendientes jerárquicos de ese nodo a menos que un bloque de tipo de rol se haya establecido para el tipo de rol correspondiente.

Una publicación “Access Control: Policies, Models and Mechanisms” de Pierangela Samaration y Sabrina de Capitani di Vimercati describe diferentes políticas de control de acceso correspondientes a diferentes criterios para definir lo que se debería y lo que no se debería permitir y a diferentes definiciones de lo que significa garantizar la seguridad. La publicación enumera los conceptos básicos detrás del diseño y la aplicación de control de acceso, y apunta diferentes requisitos de seguridad que pueden necesitar ser tomados en consideración.

No obstante, estas soluciones no son adecuadas para jerarquía de carpetas basada en metadatos, como en un sistema de gestión de documentos dinámico. Esto es debido a que en el sistema de gestión de documentos

dinámico, los objetos no están situados estáticamente en la estructura de carpetas sino que su existencia en el espacio del documento varía según la circunstancia. Por lo tanto, se necesita un tipo diferente de solución de ACL para los requisitos del sistema de gestión de documentos basado en metadatos

Compendio de la invención

La invención se especifica en las reivindicaciones independientes adjuntas.

A continuación se describe una solución de ACL para disposición de archivos basada en metadatos. La solución plantea el problema desde dos puntos de vista. Primero de todo, las listas de control de acceso se forman dinámicamente por medio de componentes de seguridad a los que se refieren a través de elementos de metadatos del objeto. En segundo lugar, la solución introduce un modelo para definir las ACL por medio de pseudousuarios. Este modelo se puede utilizar por el componente de seguridad de la primera solución también.

Diversos aspectos de la invención incluyen dos métodos, un aparato, un sistema informático, y dos medios legibles por ordenador que comprenden un programa de ordenador almacenado en los mismos, que están caracterizados por lo que se expone en las reivindicaciones independientes. Diversas realizaciones de la invención se describen en las reivindicaciones dependientes.

Según un primer aspecto, un método para un sistema informático que almacena objetos electrónicos que están definidos por elementos de metadatos, comprende derivar derechos de acceso desde uno o más componentes de seguridad que se originan a partir de elementos de metadatos respectivos de al menos un objeto, y determinar los derechos de acceso eficaces para el objeto por medio de los componentes de seguridad.

Según un segundo aspecto, un aparato comprende un procesador, una memoria que incluye un código de programa de ordenador, la memoria y el código de programa de ordenador configurados para, con el procesador, hacer al aparato realizar al menos lo siguiente: almacenar objetos electrónicos que se definen mediante elementos de metadatos, derivar derechos de acceso de uno o más componentes de seguridad que se originan desde los elementos de metadatos respectivos de al menos un objeto, y determinar los derechos de acceso eficaces para el objeto por medio de los componentes de seguridad.

Según un tercer aspecto, un sistema informático comprende al menos un procesador, al menos una memoria que incluye un código de programa de ordenador, la memoria y el código de programa de ordenador configurados para, con dicho al menos un procesador, hacer que el sistema informático al menos realice: almacenar objetos electrónicos que se definen por elementos de metadatos, derivar derechos de acceso a partir de uno o más componentes de seguridad que se originan a partir de los elementos de metadatos respectivos de al menos un objeto, y determinar los derechos de acceso eficaces para el objeto por medio de los componentes de seguridad.

Según un cuarto aspecto, un medio legible por ordenador comprende instrucciones de programa de ordenador almacenadas en el mismo, en donde dichas instrucciones, cuando se ejecutan, son para almacenar objetos electrónicos que se definen mediante elementos de metadatos, para derivar derechos de acceso de uno o más componentes de seguridad que se originan a partir de los elementos de metadatos respectivos de al menos un objeto, y para determinar los derechos de acceso eficaces para el objeto por medio de los componentes de seguridad.

Según un quinto aspecto, un método para un sistema informático que almacena objetos electrónicos que se definen mediante elementos de metadatos, comprende determinar derechos de acceso para un objeto por medio de uno o más pseudousuarios.

Según un sexto aspecto, un medio legible por ordenador que comprende instrucciones de programa de ordenador almacenadas en el mismo, en donde dichas instrucciones, cuando se ejecutan, son para determinar derechos de acceso para un objeto por medio de uno o más pseudousuarios.

Según una realización, un objeto se refiere a la propia lista de control de acceso del objeto, en donde los derechos de acceso eficaces para dicho objeto se determinan por medio de componentes de seguridad como parte de la propia lista de control de acceso del objeto.

Según una segunda realización, un componente de seguridad se origina directamente a partir del elemento de metadatos del objeto.

Según una tercera realización, un componente de seguridad se origina indirectamente a partir del elemento de metadatos del objeto.

Según una cuarta realización, el componente de seguridad se origina a partir de un elemento de metadatos de más de un objeto en cascada.

Según una quinta realización, los más de uno de los componentes de seguridad están combinados, en donde los derechos de acceso eficaces se determinan como una intersección de los más de uno de los componentes de seguridad.

Según una sexta realización, más de uno de los componentes de seguridad están combinados, en donde los derechos de acceso eficaces se determinan según una de las siguientes reglas: uno anula los otros, cada uno complementa el derecho de acceso eficaz, uno restringe los otros, uno define el máximo, uno define los derechos mínimos, o cualquier combinación de éstos.

Según una sexta realización, los derechos de acceso se definen por medio de pseudousuarios en dicho componente de seguridad.

Según una sexta realización, las personas a las que se permite acceder al documento se identifican resolviendo los pseudousuarios de los elementos de metadatos del objeto.

Según una séptima realización, las personas a las que se permite acceder al documento se identifican resolviendo los pseudousuarios de los elementos de metadatos del más de un objeto en cascada.

Según una octava realización, el sistema informático comprende un cliente y un servidor.

Otras realizaciones así como ventajas de las presentes soluciones se describen en la descripción detallada que sigue a la descripción de los dibujos.

Descripción de los dibujos

A continuación, se describirán en más detalle diversas realizaciones de la invención con referencia a los dibujos adjuntos, en los que

la Fig. 1 muestra un ejemplo simplificado de un sistema de gestión de documentos;

la Fig. 2 muestra un ejemplo de un objeto que tiene elementos de metadatos y una ACL;

las Fig. 3a, 3b muestran un ejemplo para definir una ACL para el objeto de la Fig. 2;

las Fig. 4a, 4b muestran un ejemplo para definir una ACL para el objeto de la Fig. 2 por medio de dos componentes de seguridad;

la Fig. 5 muestra otro ejemplo de un objeto que tiene elementos de metadatos y una ACL;

la Fig. 6a muestra aún un ejemplo adicional para definir una ACL para un objeto; y

la Fig. 6b muestra los derechos de acceso eficaces para el objeto de la Fig. 6a.

Descripción detallada de las realizaciones

A continuación, varias realizaciones de la invención se describirán en el contexto de un sistema de gestión de documentos dinámico. Se ha de observar, no obstante, que la invención no está limitada solamente a tal sistema. De hecho, las diferentes realizaciones tienen aplicaciones ampliamente en cualquier entorno basado en metadatos (es decir, disposición de archivos), donde se esperan seguridad y derechos de acceso.

Sistema de gestión de documentos

En este contexto, el término de sistema de gestión de documentos (DMS) se refiere a una disposición de archivos que almacena objetos que se definen por metadatos (es decir, propiedades). Otros términos que se usan típicamente para un sistema de gestión de documentos son sistema de gestión de contenidos (CMS) y sistema de gestión de datos. En la presente descripción el término “sistema de gestión de documentos” es un término general que se refiere también a sistemas de gestión de contenidos y de datos. Tales sistemas comprenden diversos rasgos para gestionar documentos electrónicos, por ejemplo, almacenamiento, versionado, indexación, búsqueda y recuperación de documentos. Se aprecia que hay sistemas de gestión de documentos tanto dinámicos como estáticos. La diferencia entre sistemas dinámicos y estáticos es la forma en que almacenan archivos. En los sistemas estáticos los archivos se almacenan por ejemplo en una jerarquía de tipo árbol constante que define las relaciones para capetas y documentos almacenados en el árbol. En los sistemas dinámicos se pueden dar identificaciones a los archivos que definen su existencia en el sistema. La ubicación observada de los archivos no es constante, sino que puede variar en un espacio virtual dependiendo de la situación.

Antes de describir la invención de una manera más detallada, se definen unos pocos términos con el fin de facilitar la lectura y la comprensión de la invención. En esta descripción, el término “documento” se refiere a un medio (un archivo) que ha sido creado por una cierta aplicación y que ha sido asociado con metadatos. Por ejemplo, una parte del texto creado usando la aplicación Microsoft Word es un archivo. “Metadatos” se refiere a información sobre las propiedades de un documento. Por ejemplo, un autor del archivo o una fecha de creación pueden representar los metadatos. El término “objeto” se refiere a un documento, y está compuesto del contenido del objeto así como de los metadatos del objeto. Los documentos y otros objetos definidos con metadatos se sitúan estática o virtualmente en la disposición del archivo. La ubicación virtual se define dando una ubicación o ubicaciones del documento en base

a sus metadatos, que entonces dirige el documento a una cierta carpeta virtual dependiendo de la ruta en la que se acerque el documento. Por lo tanto, el contenido de cada carpeta depende de los valores de propiedad actuales de los objetos y puede variar según un caso de uso y, de esta manera, es dinámico.

Un ejemplo de una disposición de archivos se ilustra en la Figura 1. Esta disposición de archivos es un sistema de gestión de documentos que comprende un servidor 100 de gestión de documentos y dispositivos 101, 102, 103, cliente que están todos interconectados. La interconexión puede ser cableada o inalámbrica y puede estar siempre sustancialmente activada o puede ser desconectada ocasionalmente. El servidor 100 está configurado para almacenar objetos (por ejemplo, documentos) que pueden ser recuperados por los dispositivos 101, 102, 103 cliente. El servidor y los dispositivos cliente cada uno incluye típicamente al menos un procesador y al menos una memoria (medio legible por ordenador) para almacenamiento de al menos un código de programa de ordenador para ejecución por el al menos un procesador. El dispositivo cliente puede ser cualquier dispositivo electrónico capaz de computación, tal como por ejemplo un ordenador personal, un ordenador portátil, un dispositivo móvil.

Como ejemplo, en la Fig. 1, el documento D1 se recupera por el dispositivo 101 cliente, mientras que el documento D2 se almacena por el dispositivo 103 cliente en el servidor 100 de gestión de documentos. El servidor 100 de gestión de documentos está configurado principalmente para almacenar documentos, pero en uso, el servidor de gestión de documentos puede tener otras funciones también, por ejemplo controla los derechos de acceso, registra las modificaciones hechas a los documentos y permite las conexiones a otros sistemas. En la Fig. 1, hay un servidor. Sin embargo, en algunos casos, el sistema informático puede comprender más de un servidor donde se divide el sistema de gestión de documentos. Un documento electrónico almacenado en el sistema de gestión de documentos es un ejemplo de un objeto. Se dan elementos de metadatos (es decir, valores de propiedad) a tal objeto, por ejemplo, un nombre de autor, un tipo de documento, un proyecto al que pertenece el documento, una clase de seguridad, un cliente, etc.

Como se mencionó, el sistema de gestión de documentos puede ser dinámico de modo que las carpetas sean virtuales, y los documentos se sitúen virtualmente en carpetas dependiendo del punto de vista del usuario que se construye sobre la parte superior de los metadatos. La presente solución se puede utilizar sin embargo en un sistema de gestión de archivos que almacena de manera estática carpetas que comprenden archivos. Los documentos pueden tener más de una ubicación en el sistema de gestión de documentos dinámicos, pero el documento como tal es el mismo documento en todas las ubicaciones. En otras palabras, el documento se almacena en el sistema de gestión de documentos solamente una vez, pero se le dan múltiples ubicaciones en base a sus elementos de metadatos. Por lo tanto, el término “ubicación” se debería interpretar tanto como ubicación física como virtual dependiendo de la disposición del archivo para cubrir tanto el sistema de gestión de documentos dinámico como el sistema de gestión de archivos. Sin embargo, con el fin de utilizar la presente solución, los objetos (por ejemplo, documentos, carpetas) tienen que estar asociados con metadatos. Esto significa que, por ejemplo, cada documento tiene una estructura de propiedad que define al menos una parte de los metadatos (es decir, elemento de metadatos) para el documento.

Un ejemplo de un objeto que comprende elementos de metadatos se ilustra en la Fig. 2. Aquí, el objeto es un documento “Meeting_minutes.doc” creado por Carl Smith que actúa como secretario de la reunión para el proyecto “Fiesta de verano”. El director del proyecto para este proyecto es Holly Quinn (no se muestra en la Fig. 2). Se entiende que los metadatos 200 del objeto comprenden elementos de metadatos para del objeto, cuyos elementos de metadatos definen un autor, un proyecto, un tipo de documento, una clase de seguridad, un cliente y un número de identificación para del documento. Cada uno de estos elementos de metadatos se pueden teclear (o introducir por cualquier método conocido) o seleccionar de una lista predeterminada de valores.

Se puede ver que el objeto 200 se refiere a una ACL 204 que comprende un componente 202 por defecto que asigna un derecho de acceso completo a Carl Smith. Se aprecia que la ACL se puede asociar con el objeto por otros medios también, por ejemplo, por inclusión, por enlace, por referencia directa, por referencia indirecta, etc.

Listas de control de acceso accionadas por metadatos dinámicos

Pasemos a la Fig. 3a donde se usa como ejemplo “Meeting_minute.doc” mostrada en la Fig. 2. En la Fig. 3a, se ilustra un objeto que comprende elementos 300 de metadatos para el proyecto “Fiesta de Verano”. El proyecto “Fiesta de Verano” comprende un elemento de metadatos para un director de proyecto el valor del cual es Holly Quinn. Otros elementos de metadatos definen que la fiesta se celebra el 14 de julio en Andorra cada año impar. El cliente del proyecto es HorseWhisp Inc. Se entiende que el proyecto se refiere a un componente 303 de seguridad que define los derechos de acceso de modo que el acceso de lectura y escritura (“RW”) se asigne a Holly Quinn y el acceso de lectura (“R”) se asigne a los Miembros de la Fiesta de Verano. Se aprecia que el componente de seguridad se puede asociar con el objeto (por ejemplo, proyecto) por otros medios también, por ejemplo, por inclusión, por enlace, por referencia directa, por referencia indirecta, etc.

Según la presente solución, este componente de seguridad 303 del proyecto “Fiesta de verano” define los derechos de acceso a cualquier objeto referente al proyecto “Fiesta de Verano” (es decir, cualquier objeto que tenga un elemento de metadatos que defina “Fiesta de Verano”), incluyendo “Meeting_minute.doc”. Por lo tanto, Holly Quinn puede leer y escribir “Meeting_minute.doc” y los participantes del proyecto “Fiesta de Verano” pueden leer

"Meeting_minute.doc". Los derechos de acceso que se originan desde un componente de seguridad del elemento de metadatos del objeto se pueden llamar "permisos de propagación/derechos de acceso" debido a que se propagan a la propia ACL del objeto, como se muestra en la Figura 3b. El objeto "Meeting_minute.doc" tiene una propiedad "Proyecto", el valor del cual es "Fiesta de verano". El proyecto "Fiesta de verano" se refiere a un componente 303 de seguridad que define el acceso a objetos que se refieren a dicho proyecto. Por lo tanto, la ACL 204 del objeto 200 cumple con el contenido del componente 303 de seguridad. Como resultado de esto, la ACL 204 del objeto 200 comprende su propio componente 202 por defecto que asigna derecho de acceso completo a Carl Smith y el componente 302 propagado que asigna derecho de acceso de lectura y escritura a Holly Quinn y acceso de lectura a los Miembros de la Fiesta de Verano. Se aprecia que este componente de seguridad es una especie de componente viral que se puede difundir entre los objetos del sistema de gestión de documentos siempre y cuando esos objetos se refieran a elementos de metadatos que se refieran además a (o estén asociados de otra forma a) un componente de seguridad. También se aprecia que la propagación puede ser física o virtual. La diferencia entre éstas es que en propagación física, el componente de seguridad se copia físicamente o se transmite a la ACL del objeto antes de evaluar realmente los derechos de acceso. Por otra parte, en propagación virtual, el componente de seguridad se incorpora dinámicamente desde el elemento de metadatos mientras que está siendo evaluada la ACL del objeto.

La Figura 4a ilustra el mismo ejemplo que se muestra en las Fig. 2 y 3, pero proporciona más información para "Meeting_minute.doc". En la Figura 4a, un objeto "Secreto" 400 se refiere a un componente 403 de seguridad que da derechos de RW a un equipo ejecutivo a lo sumo. Debido a que "Meeting_minute.doc" tiene un valor de propiedad "Secreto", este objeto 400 de clase de seguridad define además los derechos de acceso al documento "Meeting_minute.doc". Se entiende (véase la Fig. 4b) que ahora "Meeting_minute.doc" tiene una ACL 204 que está definida por el propio componente 202 por defecto del objeto y por dos componentes propagados: uno 302 que asigna "RW" a Holly Quinn y "R" a los Miembros de la Fiesta de Verano; y el otro 402 que asigna derechos de RW al equipo ejecutivo a lo sumo. Los derechos de acceso eficaces resultantes para el objeto se pueden determinar según reglas predeterminadas que comprenden instrucciones sobre cómo los componentes separados están dispuestos entre sí.

Se ha de observar en este ejemplo que cualquier objeto que tenga una referencia al elemento de metadatos "Fiesta de Verano" puede tener los derechos de acceso según el componente de seguridad de ese proyecto particular. De forma similar, cualquier objeto que tenga una referencia al elemento de metadatos "Secreto" puede tener los derechos de acceso según el componente de seguridad de esa clase de seguridad particular. Sin embargo, adicionalmente es posible configurar mediante qué propiedades, los componentes de seguridad se pueden propagar a la ACL del objeto. Por ejemplo, se podría hacer referencia a un elemento de metadatos del proyecto mediante varias propiedades, tales como "Proyecto del Cliente" y "Proyecto para Propósitos de Seguimiento", pero solamente la propiedad "Proyecto del Cliente" se configuraría para permitir la propagación.

Mediante la primera solución, la determinación del derecho de acceso se propaga fácilmente por todo el sistema de gestión de documentos cuando se modifica el componente de seguridad de origen. Sin embargo, la ACL resultante para el objeto también se puede modificar por el usuario si los componentes propagados permiten al usuario hacerlo así. Por ejemplo, el componente de seguridad del elemento de metadatos "Secreto" se podría configurar para rechazar cualquier modificación debido a su naturaleza predominantemente confidencial.

Como se mencionó anteriormente, los derechos de acceso eficaces se pueden determinar según reglas predeterminadas. Por ejemplo, en las Fig. 4a, 4b, los derechos de acceso eficaces para el documento en cuestión se pueden determinar como una intersección parcial de los tres componentes dentro de la ACL 204. Esto significa que los derechos de acceso de RW se designan a Carl Smith o Holly Quinn solamente si también son miembros del equipo ejecutivo. En tal caso, el control completo que se asigna a Carl Smith se reduce a RW, debido a que el componente de seguridad de "Secreto" define los derechos máximos. De manera similar, se dan permisos para el objeto a tales Miembros de la Fiesta de Verano que también son miembros del Equipo Ejecutivo. Sin embargo, en tal caso, el permiso R de tales Miembros de la Fiesta de Verano no se amplía a RW. Merece la pena mencionar que en algunos casos "Max: Equipo Ejecutivo" puede elegir no indicar ningún derecho de acceso particular. En tal situación, los derechos de acceso de las personas se preservan de otros componentes de seguridad, pero el conjunto máximo de personas eficaces se determina según su pertenecía al Equipo Ejecutivo.

En algunos casos, los derechos de acceso eficaces se pueden formar combinando cada componente propagado al que se hace referencia, por lo que cada componente propagado complementa los derechos de acceso completos del objeto como en el ejemplo de las Fig. 3a, 3b. Se aprecia que cualquier componente de seguridad puede restringir, complementar, anular o definir la restricción máxima o la mínima para los otros componentes de seguridad o determinar según cualquier combinación de aquéllos. La naturaleza del componente de seguridad depende del caso de uso y se puede especificar por separado.

En el ejemplo mostrado en las Fig. 4a, 4b, hay dos componentes de seguridad que definen los derechos de acceso para el documento. Sin embargo, podría haber aún más componentes de seguridad para un objeto. Cada componente de seguridad tiene su propio factor determinante. Por ejemplo, es posible establecer el componente de seguridad de la clase de seguridad "Secreto" como el componente de seguridad dominante, el cual restringe siempre los otros componentes. Por otra parte, es posible hacer referencia a un elemento de metadatos llamado "nota" que

tiene un componente de seguridad “min: Todos: R”. Esto puede anular otros componentes de seguridad y dar a todos un acceso de lectura. Para superar cualquier conflicto que ocurre entre componentes, el sistema puede comprender una política de gestión de conflictos de ACL que se puede configurar para establecer prioridades para los componentes de seguridad.

Además, es posible usar cualquier componente de seguridad que se origine a través de referencias de elementos de metadatos indirectos a través de varios objetos. Esto significa que el elemento de metadatos del objeto no incluye ningún componente de seguridad por sí mismo, sino que comprende un elemento de metadatos que se refiere o bien a un componente de seguridad o bien comprende aún otro elemento de metadatos que incluye un componente de seguridad. Básicamente, tal cadena de componentes de seguridad puede ser tan larga como puedan encontrarse componentes de seguridad a lo largo del camino a través de los objetos en cascada.

La idea detrás de esta primera solución de la invención es recuperar componentes de seguridad en base a los metadatos del objeto, y combinarlos para definir automáticamente los derechos de acceso para el objeto. Sin embargo, como se mencionó anteriormente, algunas veces el usuario puede desear establecer o modificar los derechos de acceso resultantes del objeto manualmente. En tal caso simple, los derechos de acceso establecidos manualmente afectan solamente al objeto en cuestión y no se propagan más. Por otra parte, si el usuario desea cambiar el contenido del componente de seguridad por ejemplo del proyecto, entonces la ACL de cualquier objeto al que se refiera ese proyecto se puede actualizar automáticamente en consecuencia. Esta actualización automática puede ocurrir inmediatamente después de que se haya cambiado el componente de seguridad, o después de un cierto período de tiempo. En algunos casos, la actualización automática también se puede ignorar.

En esta solución, los ajustes del derecho de acceso no dependen de la ubicación física del objeto en el sistema de gestión de documentos, como en las soluciones de la técnica relacionada, sino de la ACL compuesta de componentes de seguridad derivados por medio de los metadatos del objeto. Esta ACL entonces se puede incluir en los metadatos del objeto en el nivel del objeto y/o en la versión específicamente.

Asignación de rol de acceso accionado por metadatos

La Figura 5 ilustra un ejemplo de la presente solución desde otro punto de vista. Se entiende que el contenido de la Fig. 5 se asemeja al contenido de la Fig. 2. Sin embargo, lo que es diferente es que la ACL 502 del objeto 501 asigna derechos de acceso a los pseudousuarios – “Autor”, “Director” - en lugar de a identidades de persona. El término “pseudousuario” es un atributo que se refiere a un elemento de metadatos que representa un usuario o un grupo de usuarios. Este atributo se denomina “pseudousuario” siempre que el elemento del usuario carezca de un valor. Se puede reconocer fácilmente que este tipo de solución hace posible definir una ACL aunque el objeto no tenga ningún valor para los elementos de metadatos en cuestión. Por ejemplo, Carl Smith recibirá derechos completos en el momento en que se dé “Carl Smith” como valor al elemento de metadatos “Autor”. De manera similar, Elliot Morris recibirá derechos de acceso de RW en el momento en que “Elliot Morris” se dé como un valor al elemento de metadatos “Director”. Debido a la presente solución, las modificaciones de los valores para “Autor” y “Director” se pueden resolver automáticamente en la ACL del objeto sin requerir que el usuario modifique directamente los derechos de acceso eficaces en la ACL. Si Holly Quinn tomase el lugar de Elliot Morris, el usuario solamente tiene que definir “Holly Quinn” como el valor de “Director”, y los derechos de RW se designarán automáticamente a Holly Quinn.

La Figura 6a ilustra cómo la solución de la Fig. 5 se puede utilizar por la primera solución (mostrada en las Fig. 2-4). En este ejemplo, se crea un componente 603 de seguridad. Este componente de seguridad asigna derechos de acceso a los pseudousuarios, por ejemplo según la notación “*ObjetodeReferencia.Rol:DerechodeAcceso*”. En la Fig. 6a, el componente de seguridad 603 define “*ObjetodeReferencia.RepresentantedelSubcontratista*: R” se refiere a un elemento de metadatos “representante del subcontratista” del documento de referencia (objetivo); “*ObjetodeReferencia.CoordinadordeExternalización*: COMPLETO” se refiere a un elemento de metadatos “coordinador de subcontratación” del documento de referencia (objetivo); y “*ObjetodeReferencia.Proyecto.DirectordeProyecto*: R” se refiere a un elemento de metadatos “proyecto” del documento de referencia (objetivo). Este componente 603 de seguridad se relaciona con el objeto 600 de contrato de externalización que define el tipo para los documentos.

Ahora, Michael McBoss crea un nuevo documento “contract.doc” 601 que comprende elementos de metadatos. Uno de los elementos de metadatos define que el tipo de documento es un “Contrato de Externalización”. También, el documento “contract.doc” se refiere a un proyecto “Control de Calidad de Pato de Goma” 606 que tiene a Gary Gantt como director de proyecto. Michael McBoss establece elementos de metadatos adicionales al documento, por ejemplo, el Representante del Subcontratista es Sammy van Slave y los coordinadores de Externalización son Michael McBoss y Kyle Kapitan. Se ha de observar que el objeto 601 también comprende una ACL 604 que tiene un componente por defecto, donde – según la segunda solución – un pseudousuario “Autor” recibe derechos completos.

En el momento en que los elementos de metadatos de “contract.doc” tengan valores para coordinador de externalización y representante del subcontratista, emergerán los derechos de acceso. Se ha de observar que el componente 603 de seguridad se puede haber creado antes que el objeto “Contract.doc”. Por lo tanto, no tiene que

prestarse atención a las identidades de las personas, sino que pueden existir de manera independiente. En el momento en que el componente 603 de seguridad se propaga a cualquier objeto, afectará a los derechos de acceso de cualquier objeto cuyos elementos de metadatos se puedan usar para resolver las referencias de pseudousuarios.

La Figura 6b muestra ahora los derechos 605 de acceso resueltos para el objeto 601. Como resultado de la propagación, Sammy van Slave obtiene permiso de lectura, Michael McBoss obtiene derechos completos, Kyle Kapitan también obtiene derechos completos y Gary Gantt obtiene permiso de lectura. En la práctica, la resolución se puede realizar físicamente, como se muestra en la Fig. 6b, o dinámicamente (virtualmente), o mezclando estos dos extremos.

La flexibilidad de la segunda solución se puede entender a partir de las Fig. 6a y 6b. Por ejemplo, cuando el director de proyecto cambia debido a que Gary Gantt está marchándose de la empresa, y Flo C. Hart se hace cargo como Director de Proyecto de Control de Calidad de Pato de Goma, el cambio se propaga automáticamente al “contract.doc” y, por lo tanto, el acceso de lectura se da automáticamente a Flo C. Hart en lugar de a Gary Gantt.

En conclusión

En el anterior, se han descrito dos tipos de soluciones para el modelo de seguridad basado en metadatos.

En la primera solución, los derechos de acceso para un objeto se derivan de elementos de metadatos referidos que se refieren además a un componente de seguridad que comprende información sobre los derechos de acceso. En la segunda solución, los derechos de acceso se derivan de los pseudousuarios. La segunda solución también se puede utilizar en la primera solución, de modo que el componente de seguridad comprenda la notación para pseudousuarios y sus derechos de acceso.

En anteriores, las soluciones contienen ejemplos donde o bien el componente de seguridad o bien el pseudousuario está un paso separado del objeto de referencia. Sin embargo, es posible tener más de un nivel de referencia de metadatos entre el componente de seguridad y el objeto de referencia y/o más de un nivel de referencia de metadatos entre el componente de seguridad y el pseudousuario.

Las diversas realizaciones de la invención se pueden implementar con la ayuda de un código de programa de ordenador que reside en una memoria y hace que los aparatos pertinentes, tales como el servidor y el dispositivo cliente, lleven a cabo la invención. Estas soluciones se pueden realizar en un dispositivo solamente o se pueden dividir dependiendo de cuántos datos se almacenan en el dispositivo cliente. Además, los dispositivos y el sistema pueden comprender otros dispositivos y operaciones que mejoren su rendimiento. Por ejemplo, una interacción humano-máquina se puede configurar en cualquier etapa de la solución, cuando sea apropiado. Es obvio que la presente invención no se limita únicamente a las realizaciones presentadas anteriormente, sino que se puede modificar dentro del alcance de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método para un sistema informático que almacena objetos electrónicos que se definen mediante metadatos que comprenden una o más propiedades que tienen valores, en donde uno o más de los objetos electrónicos están asociados con una lista de control de acceso, dicha lista de control de acceso que define un usuario de un dispositivo cliente autorizado para acceder a un objeto electrónico y operaciones que el usuario está autorizado a realizar en dicho objeto electrónico, en donde el método comprende

- recibir una solicitud de acceso a un objeto (601) electrónico de dichos objetos electrónicos desde un dispositivo cliente; y

- como respuesta a la solicitud recibida, permitir que el usuario del dispositivo cliente acceda al objeto (601) electrónico según dicha lista de control de acceso; el método que además comprende

- dicho objeto (601) electrónico que se refiere mediante un valor de propiedad de los metadatos de dicho objeto electrónico a un componente (603) de seguridad que comprende un atributo y derechos de acceso definidos para dicho atributo;

caracterizado por que el método además comprende

- identificar un usuario al que se permite acceder al objeto (601) electrónico a partir de un valor de propiedad de metadatos de otro objeto, cuyo otro objeto se determina usando el atributo, en donde dicho atributo está siendo formado de al menos una primera parte que define un objeto de referencia y una segunda parte que define una cadena de referencias a propiedades de objetos que comienzan desde dicho objeto de referencia, en donde un valor de la propiedad a la que se refiere en la cadena de referencias define el siguiente objeto que tiene la siguiente propiedad a la que se refiere, en donde la segunda última referencia en la cadena de referencias define dicho otro objeto, y la última referencia de la cadena de referencias define una propiedad de dicho otro objeto que tiene un valor que define el usuario; y

- propagar el componente de seguridad a la lista de control de acceso de dicho objeto electrónico para dar dichos derechos de acceso al usuario identificado.

2. Un aparato que comprende un procesador, y una memoria que almacena objetos electrónicos que se definen mediante metadatos que comprenden una o más propiedades que tienen valores, en donde uno o más de los objetos electrónicos están asociados con una lista de control de acceso, dicha lista de control de acceso que define un usuario de un dispositivo cliente autorizado para acceder a un objeto electrónico y operaciones que el usuario está autorizado a realizar en dicho objeto electrónico, dicha memoria que además incluye un código de programa de ordenador, en donde la memoria y el código de programa de ordenador se configuran, con el procesador, para hacer que el aparato

- reciba una solicitud de acceso a un objeto (601) electrónico de dichos objetos electrónicos desde un dispositivo cliente;

- como respuesta a la solicitud recibida, permita que el usuario del dispositivo cliente acceda al objeto (601) electrónico según dicha lista de control de acceso;

- dicho objeto (601) electrónico que se refiere mediante un valor de propiedad de los metadatos de dicho objeto electrónico a un componente (603) de seguridad que comprende un atributo y derechos de acceso definidos para dicho atributo;

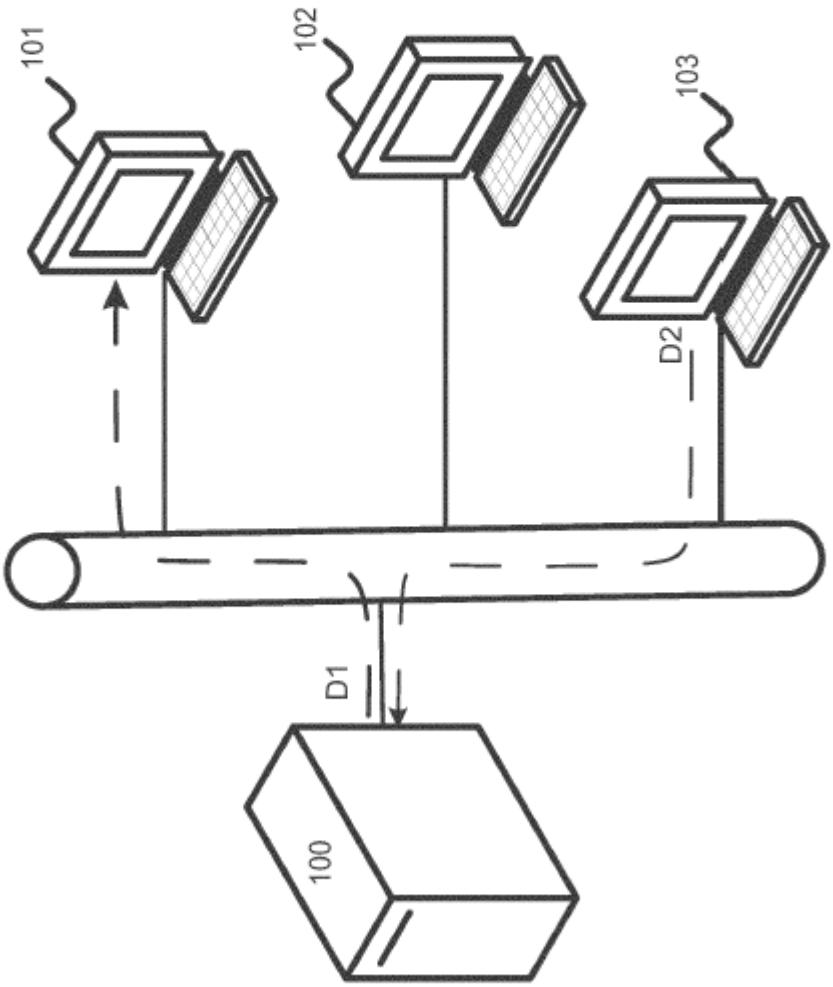
caracterizado por que el aparato se hace además

- que identifique un usuario al que se permite acceder al objeto (601) electrónico a partir de un valor de propiedad de metadatos de otro objeto, cuyo otro objeto se determina usando el atributo, en donde dicho atributo está siendo formado de al menos una primera parte que define un objeto de referencia y una segunda parte que define una cadena de referencias a propiedades de objetos que comienzan desde dicho objeto de referencia, en donde un valor de la propiedad a la que se refiere en la cadena de referencias define el siguiente objeto que tiene la siguiente propiedad a la que se refiere, en donde la segunda última referencia en la cadena de referencias define dicho otro objeto, y la última referencia de la cadena de referencias define una propiedad de dicho otro objeto que tiene un valor que define el usuario; y

- que propague el componente de seguridad a la lista de control de acceso de dicho objeto electrónico para dar dichos derechos de acceso al usuario identificado.

3. Un medio legible por ordenador que comprende instrucciones de programa de ordenador almacenadas en el mismo, caracterizado por que dichas instrucciones, cuando se ejecutan, son para implementar el método como se especifica en la reivindicación 1.

Fig. 1



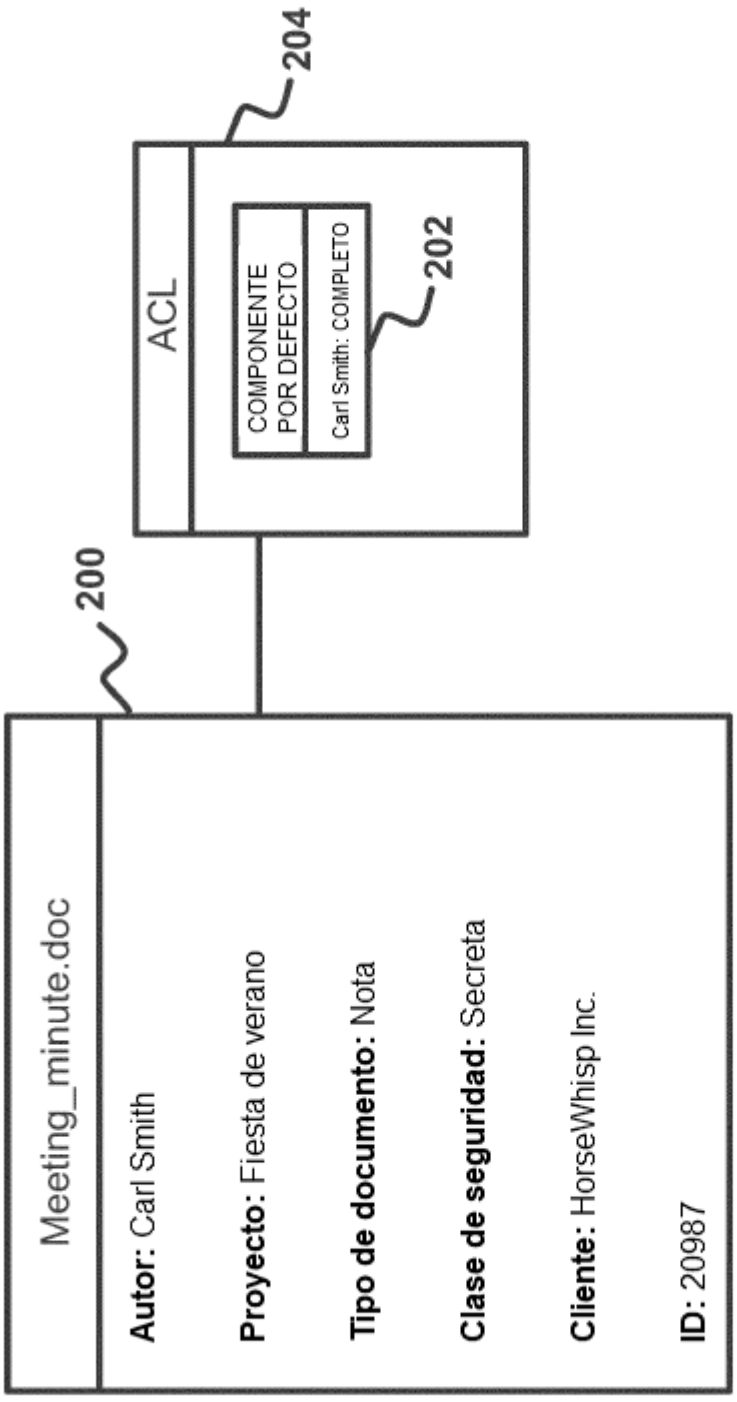

204
ACL
COMPONENTE POR DEFECTO
Carl Smith: COMPLETO
202
200
Meeting_minute.doc
Autor: Carl Smith
Proyecto: Fiesta de verano
Tipo de documento: Nota
Clase de seguridad: Secreta
Cliente: HorseWhisp Inc.
ID: 20987

Fig.2

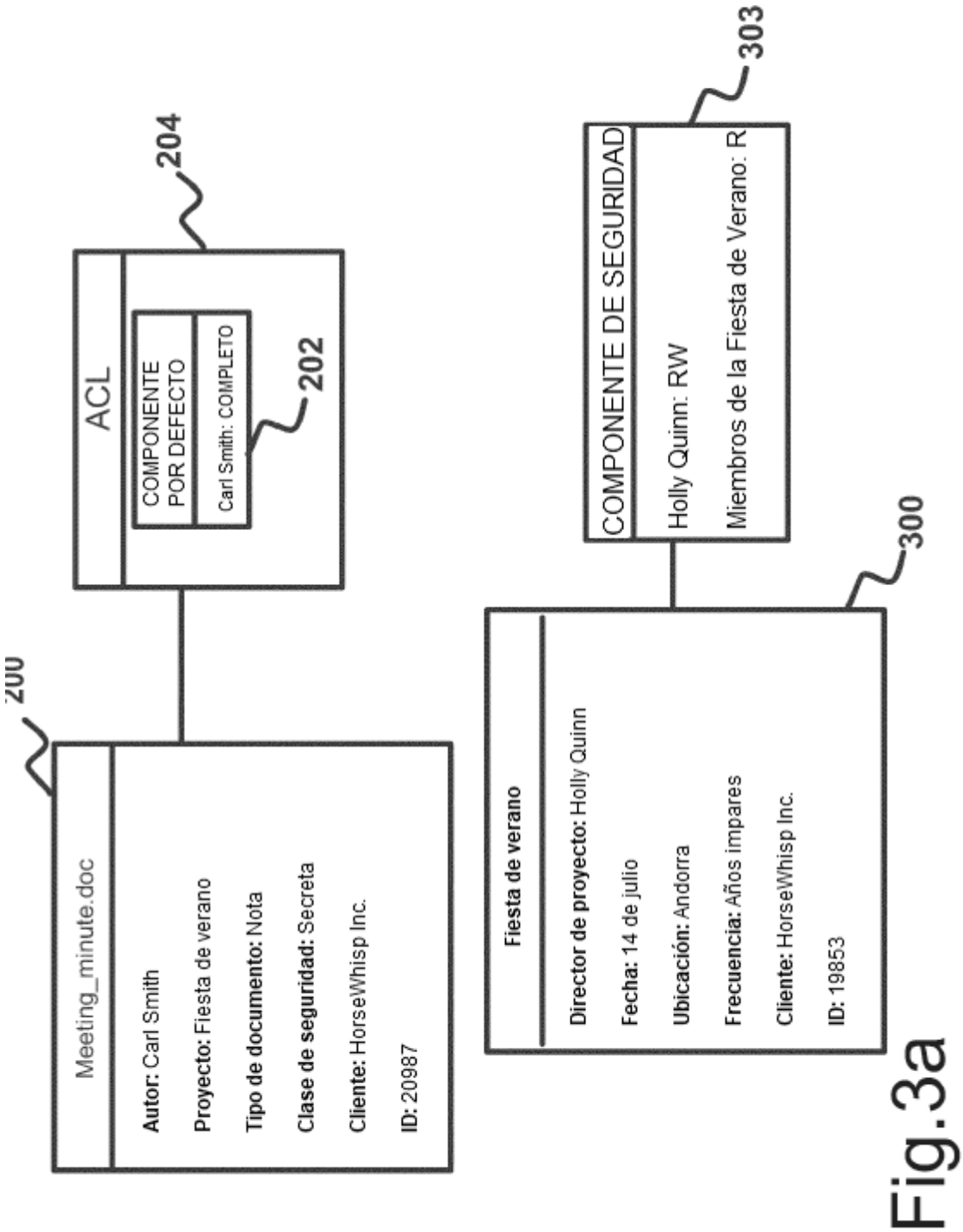

200
Meeting_minute.doc
Autor: Carl Smith
Proyecto: Fiesta de verano
Tipo de documento: Nota
Clase de seguridad: Secreta
Cliente: HorseWhisp Inc.
ID: 20987
ACL
COMPONENTE POR DEFECTO
Carl Smith: COMPLETO
202
204
Fiesta de verano
Director de proyecto: Holly Quinn
Fecha: 14 de julio
Ubicación: Andorra
Frecuencia: Años impares
Cliente: HorseWhisp Inc.
ID: 19853
300
COMPONENTE DE SEGURIDAD
Holly Quinn: RW
Miembros de la Fiesta de Verano: R
303

Fig.3a

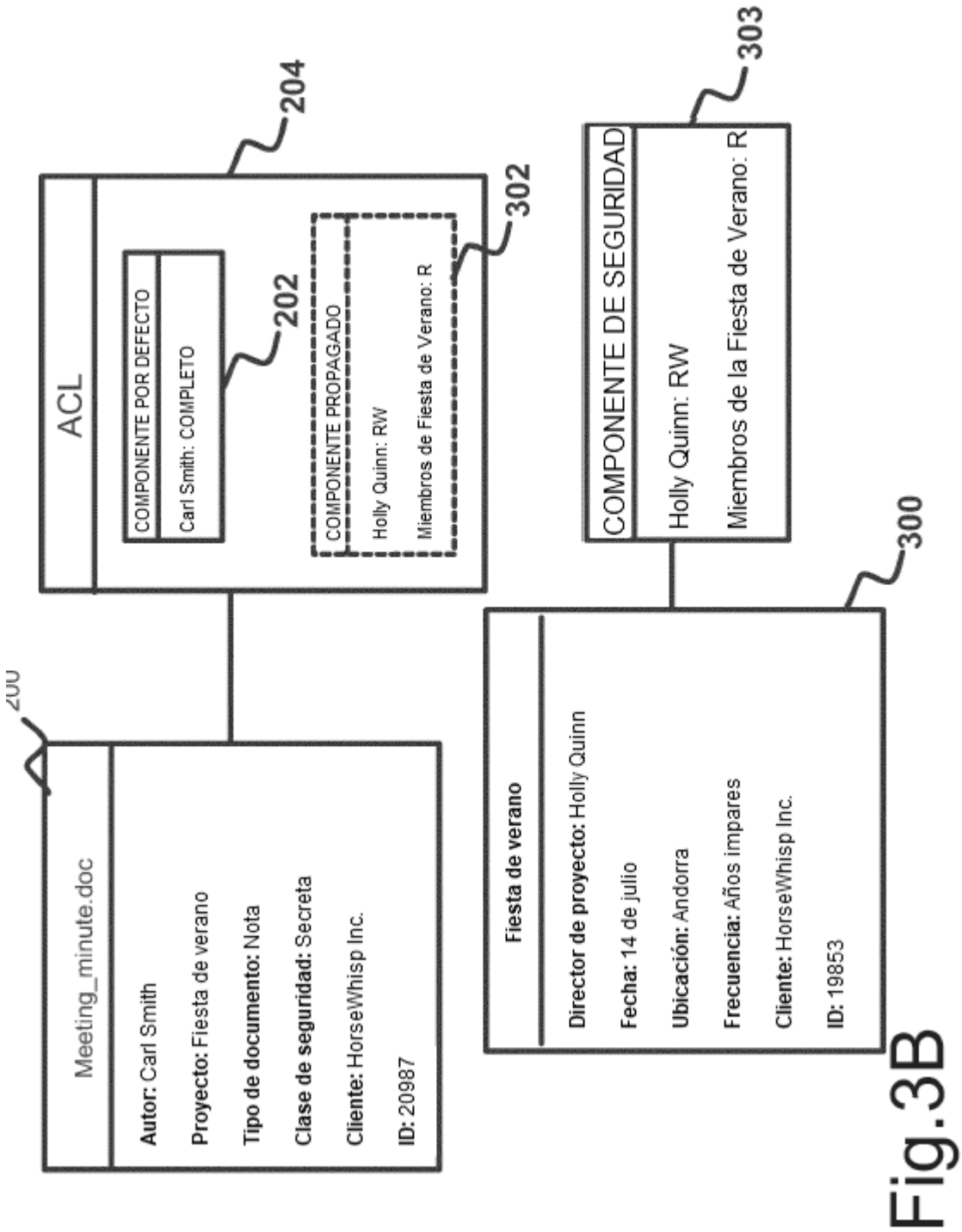

200
Meeting_minute.doc
Autor: Carl Smith
Proyecto: Fiesta de verano
Tipo de documento: Nota
Clase de seguridad: Secreta
Cliente: HorseWhisp Inc.
ID: 20987
ACL
COMPONENTE POR DEFECTO
Carl Smith: COMPLETO
202
COMPONENTE PROPAGADO
Holly Quinn: RW
Miembros de Fiesta de Verano: R
302
204
COMPONENTE DE SEGURIDAD
Holly Quinn: RW
Miembros de la Fiesta de Verano: R
303
Fiesta de verano
Director de proyecto: Holly Quinn
Fecha: 14 de julio
Ubicación: Andorra
Frecuencia: Años impares
Cliente: HorseWhisp Inc.
ID: 19853
300

Fig.3B

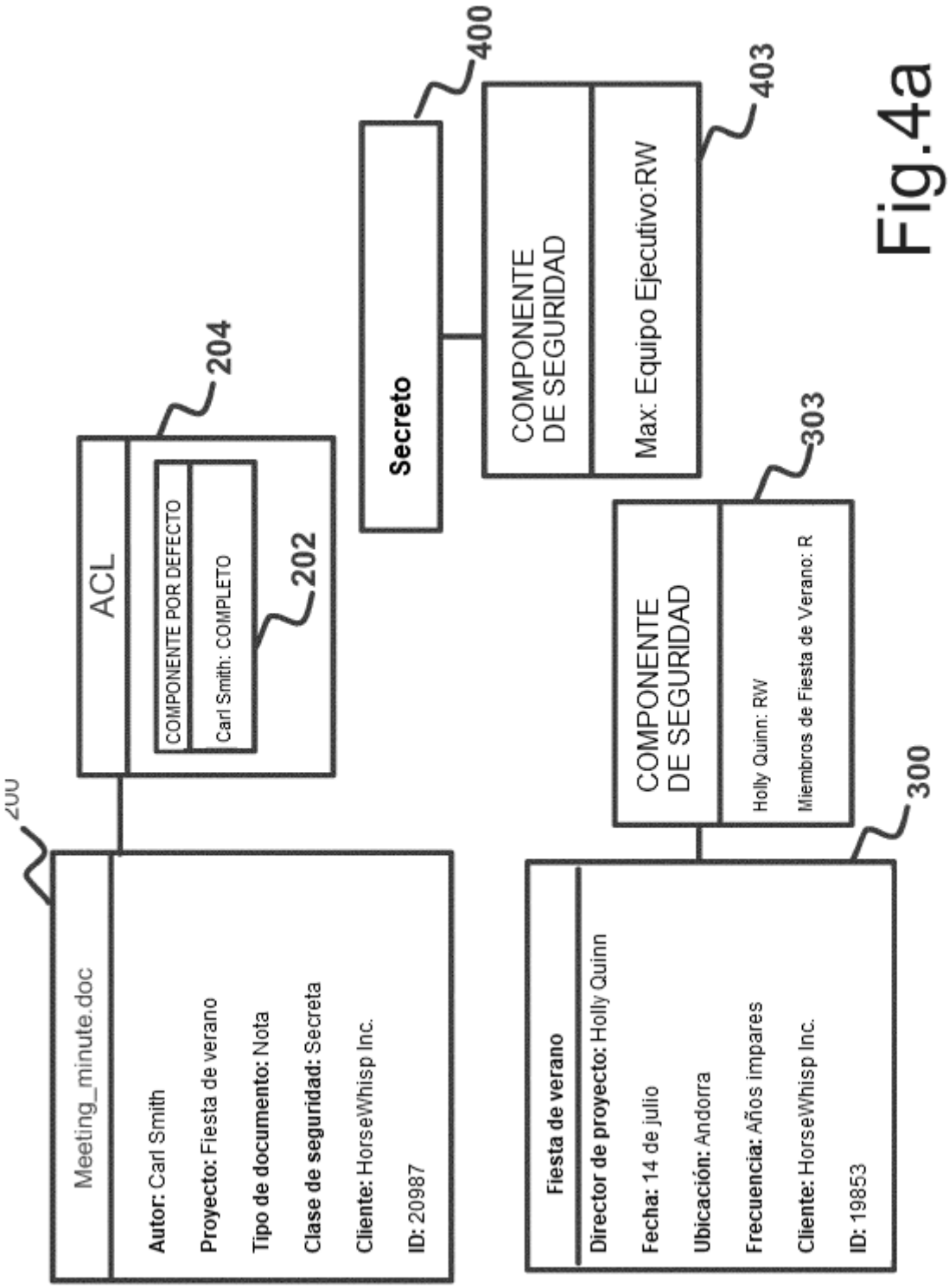

Meeting_minute.doc
Autor: Carl Smith
Proyecto: Fiesta de verano
Tipo de documento: Nota
Clase de seguridad: Secreta
Cliente: HorseWhisp Inc.
ID: 20987
200
ACL
COMPONENTE POR DEFECTO
Carl Smith: COMPLETO
202
204
Secreto
400
COMPONENTE DE SEGURIDAD
Max: Equipo Ejecutivo:RW
403
COMPONENTE DE SEGURIDAD
Holly Quinn: RW
Miembros de Fiesta de Verano: R
303
Fiesta de verano
Director de proyecto: Holly Quinn
Fecha: 14 de julio
Ubicación: Andorra
Frecuencia: Años impares
Cliente: HorseWhisp Inc.
ID: 19853
300

Fig.4a

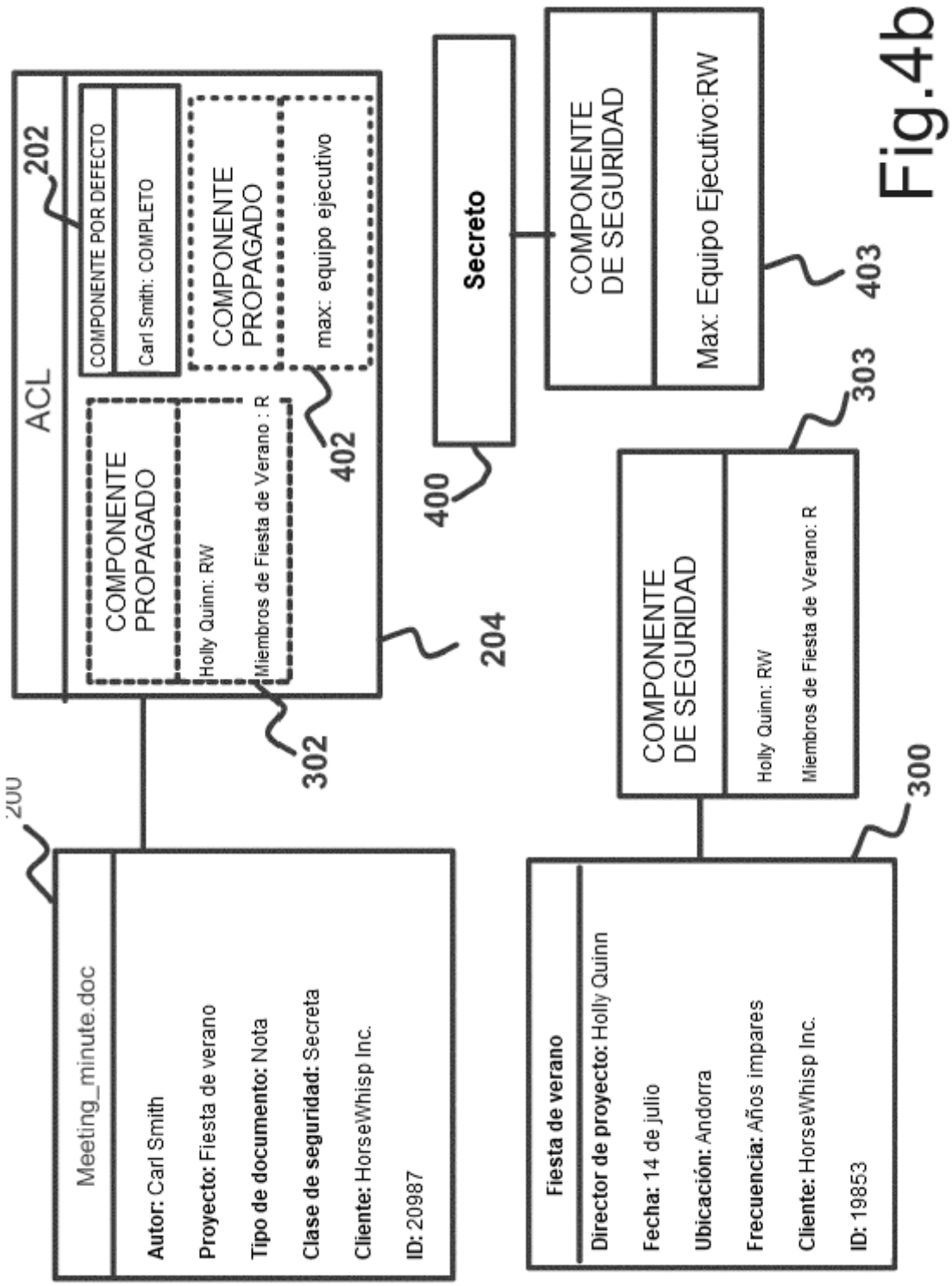

Meeting_minute.doc
Autor: Carl Smith
Proyecto: Fiesta de verano
Tipo de documento: Nota
Clase de seguridad: Secreta
Cliente: HorseWhisp Inc.
ID: 20987
200
ACL
202
COMPONENTE POR DEFECTO
Carl Smith: COMPLETO
COMPONENTE PROPAGADO
Holly Quinn: RW
COMPONENTE PROPAGADO
Miembros de Fiesta de Verano : R
302
max: equipo ejecutivo
402
204
400
Secreto
COMPONENTE DE SEGURIDAD
Max: Equipo Ejecutivo:RW
403
COMPONENTE DE SEGURIDAD
Holly Quinn: RW
Miembros de Fiesta de Verano: R
303
Fiesta de verano
Director de proyecto: Holly Quinn
Fecha: 14 de julio
Ubicación: Andorra
Frecuencia: Años impares
Cliente: HorseWhisp Inc.
ID: 19853
300

Fig.4b

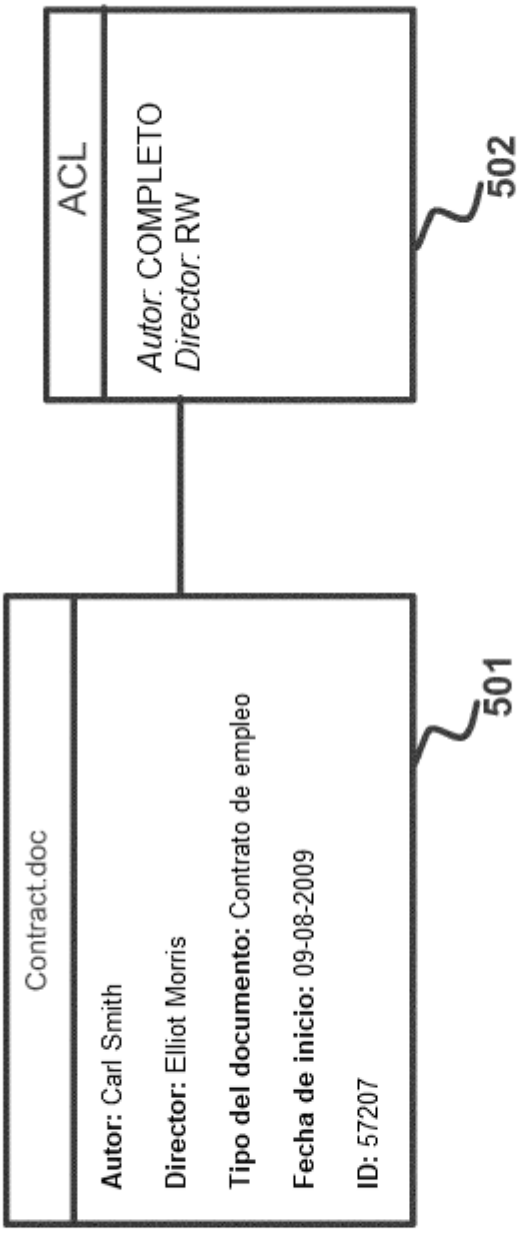

Contract.doc
Autor: Carl Smith
Director: Elliot Morris
Tipo del documento: Contrato de empleo
Fecha de inicio: 09-08-2009
ID: 57207
501
ACL
Autor: COMPLETO
Director: RW
502

Fig.5

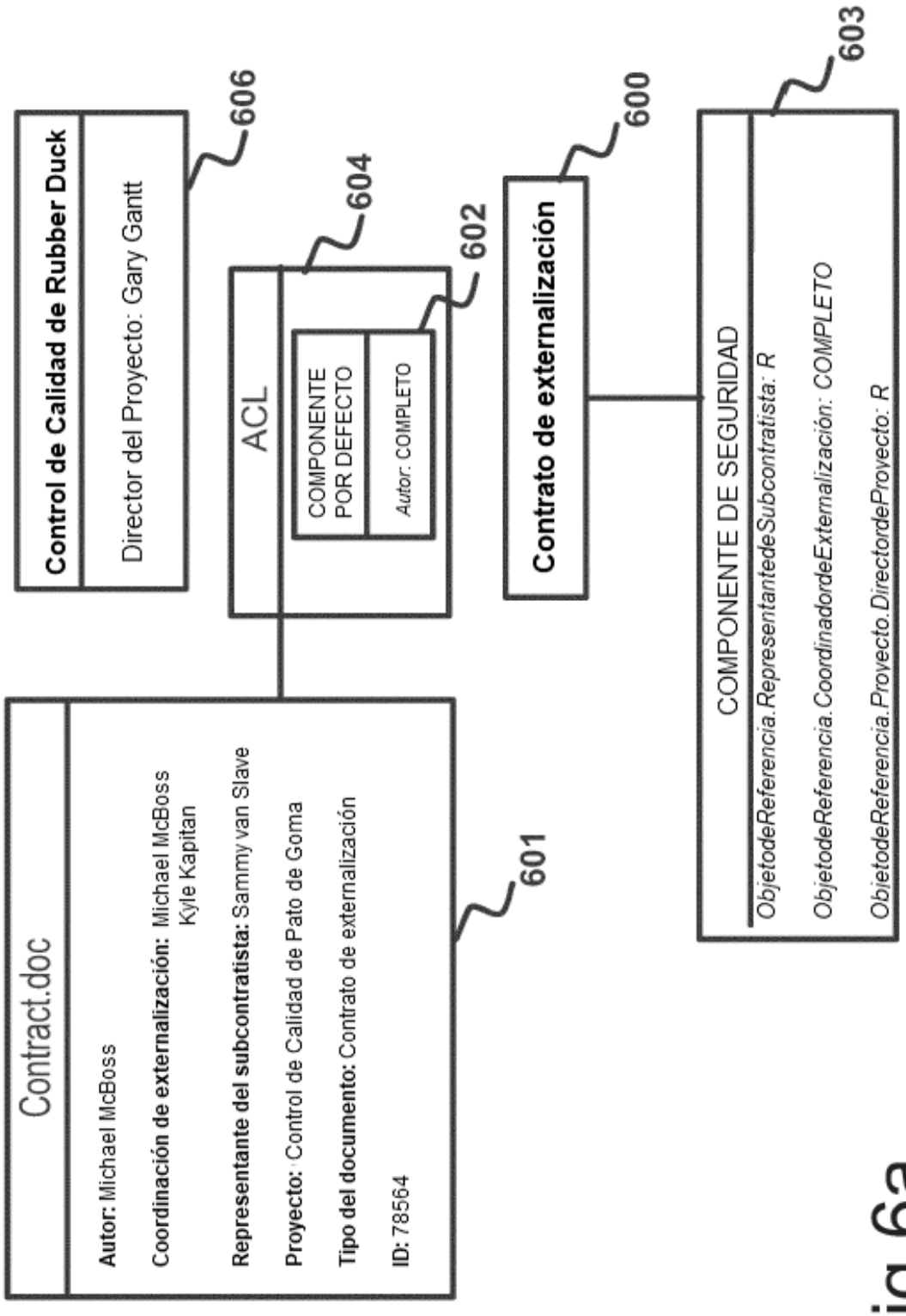

Control de Calidad de Rubber Duck
Director del Proyecto: Gary Gantt
606
ACL
COMPONENTE POR DEFECTO
Autor: COMPLETO
604
602
Contract.doc
Autor: Michael McBoss
Coordinación de externalización: Michael McBoss
Kyle Kapitan
Representante del subcontratista: Sammy van Slave
Proyecto: Control de Calidad de Pato de Goma
Tipo del documento: Contrato de externalización
ID: 78564
601
Contrato de externalización
600
COMPONENTE DE SEGURIDAD
ObjetodeReferencia.RepresentantedeSubcontratista: R
ObjetodeReferencia.CoordinadordeExternalización: COMPLETO
ObjetodeReferencia.Proyecto.DirectordeProyecto: R
603

Fig.6a

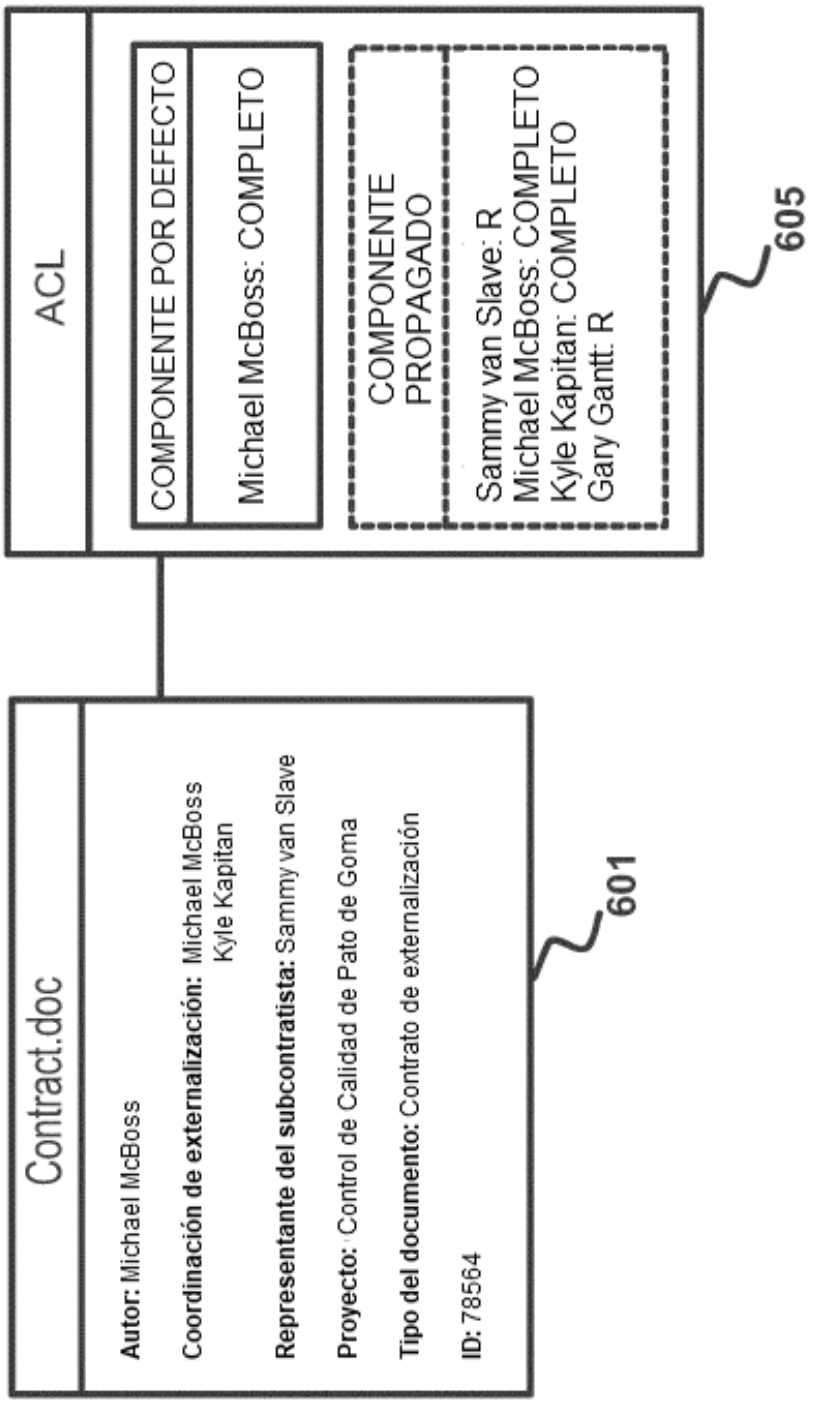

Contract.doc
Autor: Michael McBoss
Coordinación de externalización: Michael McBoss
Kyle Kapitan
Representante del subcontratista: Sammy van Slave
Proyecto: Control de Calidad de Pato de Goma
Tipo del documento: Contrato de externalización
ID: 78564
601
ACL
COMPONENTE POR DEFECTO
Michael McBoss: COMPLETO
COMPONENTE PROPAGADO
Sammy van Slave: R
Michael McBoss: COMPLETO
Kyle Kapitan: COMPLETO
Gary Gantt: R
605

Fig.6b