(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 370 558**

(51) Int. CI.:
H04L 29/06 (2006.01)
G06F 21/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08150277 .5**
(96) Fecha de presentación: **15.01.2008**
(97) Número de publicación de la solicitud: **2081354**
(97) Fecha de publicación de la solicitud: **22.07.2009**

(54) Título: **MÉTODO Y DISPOSITIVOS PARA GESTIONAR PRIVILEGIOS DE ACCESO.**

(45) Fecha de publicación de la mención BOPI:
20.12.2011

(45) Fecha de la publicación del folleto de la patente:
20.12.2011

(73) Titular/es:
AXIS AB
EMDALAVÄGEN 14
223 69 LUND, SE

(72) Inventor/es:
Rasmusson, Martin;
Rehn, John;
Kindborg, Mattias y
Hultqvist, Sebastian

(74) Agente: **de Elzaburu Márquez, Alberto**

DESCRIPCION

Método y dispositivos para gestionar privilegios de acceso.

Campo técnico del invento

Un método y dispositivos para configurar en una red los privilegios de acceso a dispositivos conectados en red.

Antecedentes del invento

Cada vez está más extendido hacer diversos tipos de dispositivos y sus funciones accesibles mediante la conexión de los mismos a redes de ordenadores. No obstante, en la mayoría de los casos el propietario de los dispositivos o de la red no está interesado en permitir a cualquiera tener acceso a la red que tiene acceso a los dispositivos y a su funcionalidad. Con el fin de resolver este problema el sistema puede estar dispuesto para proporcionar a los usuarios unos privilegios de acceso específicos. Estos privilegios de acceso pueden por ejemplo ser tales que el usuario pueda acceder al video desde una cámara de vigilancia A pero no acceso a un control de giro e inclinación para controlar la dirección de visión de la misma cámara.

Además, a menudo se instalan esquemas de privilegios de acceso en sistemas de seguridad, por ejemplo sistemas de seguridad, protección contra robo, sistemas de control de acceso, sistemas de protección contra incendios, etc. Cuando los sistemas se usan para tales funciones críticas es muy importante disponer de un esquema para privilegios de acceso.

La mayoría de los sistemas que disponen de esquemas para el tratamiento de privilegios de acceso permiten que un administrador del sistema fije los privilegios de acceso de cada usuario individualmente para cada cámara. No obstante, la gestión de tal sistema se complica muy rápidamente y es muy complicado y pesado de manejar a medida que aumenta el número de usuarios y dispositivos. En algunos sistemas se introducen grupos de nivel de acceso o grupos de usuarios con el fin de facilitar la gestión. En estos casos la gestión se facilita por el hecho de que solamente se han de gestionar los privilegios de acceso de cada grupo.

Un ejemplo de un sistema de gestión en el que cada uno de los usuarios así como de los grupos de usuarios está puesto en práctica en el documento US 2005/0097353. Dicho documento US 2005/0097353 describe un método para la búsqueda de un subconjunto de procedimientos dentro de un conjunto de procedimientos. Cada procedimiento puede ser usado para controlar el acceso a un recurso. El conjunto de procedimientos incluye los siguientes componentes de procedimiento, un recurso, un objeto, y o bien una acción o un nombre del cometido, y en el que el objeto incluye al menos un usuario o un grupo. La búsqueda se realiza especificando uno o más criterios de búsqueda que incluyen uno o más valores de los componentes del procedimiento. Los valores de los componentes del procedimiento pueden incluso incluir uno o más caracteres de sustitución.

Además, en el documento US 6.208.379, de Oya y otros, se describen algunos métodos para gestionar privilegios de acceso. Un método descrito en el documento US 6.208.379 para facilitar la gestión de privilegios de acceso es para agrupar a los usuarios en grupos de usuarios como se ha descrito antes. De forma general, el documento US 6.208.379 describe la fijación de los privilegios de acceso de un grupo de usuarios por la selección de una cámara a partir de una lista de cámaras, que indican en una celda de diálogo que se abre tras la selección de la cámara que se han solicitado fijaciones de privilegios de acceso. A continuación se presenta un panel de control de acceso o celda de diálogo de la cámara. En el panel de control de acceso es posible seleccionar un modo de acceso predefinido. Cambiando el modo de acceso de la cámara se fijan en el sistema los privilegios de acceso predefinidos de todos los grupos de usuarios. Con el fin de fijar los privilegios de acceso en un nivel más detallado se abre una ventana de privilegio de acceso desde el panel de control de acceso. La ventana de privilegios de acceso presenta a continuación una matriz que indica los privilegios de acceso de cada grupo de usuarios en relación con cada función de la cámara seleccionada.

Los métodos expuestos en el documento US 6.208.379 y en el US 2005/0097353 son pesados de procesar, sobre todo cuando se han de fijar los privilegios de acceso a una pluralidad de cámaras diferentes. Además, los métodos no dan al administrador de los privilegios de acceso especialmente muchas alternativas cuando va a personalizar los privilegios de acceso para los diferentes usuarios.

Sumario del invento

Un objeto del invento es facilitar el establecimiento de privilegios de acceso a una pluralidad de dispositivos conectados en red y facilitar la personalización de los privilegios de acceso.

El objeto se consigue por medio de un método de acuerdo con la reivindicación 1, un servidor de acuerdo con la reivindicación 12 y un cliente de acuerdo con la reivindicación 18. Las realizaciones del invento se exponen en las reivindicaciones dependientes.

En particular, de acuerdo con un aspecto del invento, un método para configurar privilegios de acceso en un sistema de dispositivos conectados en red comprende la selección de una pluralidad de identidades de acceso, la recuperación de información de privilegios de acceso de cada una de las identidades de acceso seleccionadas de

las funciones accesibles de los dispositivos conectados en red, la acumulación de los privilegios de acceso de las identidades de acceso seleccionadas para cada una de dichas funciones accesibles de cada uno de dichos dispositivos conectados en red, la presentación de dichos privilegios de acceso acumulados para cada una de dichas funciones accesibles de cada uno de dichos dispositivos conectados en red en una interfaz que permite la edición de los privilegios de acceso acumulados, la indicación de un cambio en los privilegios de acceso acumulados para una función específica en un dispositivo conectado en red específico, y la configuración de la función específica del dispositivo conectado en red específico para permitir el acceso a los usuarios seleccionados de acuerdo con el cambio indicado de los privilegios de acceso acumulados.

De acuerdo con este método se facilitan los cambios de privilegios de acceso, sobre todo con respecto a los cambios de acceso en casos en los que los privilegios de acceso de los usuarios no están todavía relacionados entre sí en el sistema y en los que los privilegios de acceso con respecto a cuándo hay que cambiar una pluralidad de dispositivos. Realizando el acto de acumular los privilegios de acceso como se ha descrito antes se hace posible tal operación de cambio de privilegios de acceso.

De acuerdo con una realización dicha acumulación de privilegios de acceso incluye el recuento del número de identidades de acceso seleccionadas que tienen privilegios de acceso a cada una de dichas funciones de cada uno de dichos dispositivos conectados en red. La ventaja de esto es que no es una forma complicada de conseguir un valor acumulador, o en otros términos conseguir un valor que represente los privilegios de acceso de una pluralidad de usuarios individuales que no deben tener privilegios de acceso idénticos.

De acuerdo con una realización posterior el paso de acumulación mencionado anteriormente puede ser ampliado por la fijación del privilegio de acceso acumulado para una función específica de un dispositivo conectado en red en un valor que indica que todas las identidades de acceso seleccionadas tienen permitido el acceso a la función específica si dicho recuento indica que todos los usuarios seleccionados tienen permitido el acceso a la función específica, fijando el privilegio de acceso acumulado para una función específica de un dispositivo conectado en red en un valor que indica que ninguna de las identidades de acceso seleccionadas tienen permitido el acceso a la función específica si dicho recuento indica que ninguna de las identidades de acceso seleccionadas tiene permitido el acceso a la función específica, y fijando el privilegio de acceso acumulado para una función específica de un dispositivo conectado en red en un valor que indica que algunas de las identidades de acceso tienen permitido el acceso a la función si dicho recuento indica que algunas de las identidades de acceso seleccionadas tienen permitido acceso a la función. De este modo, facilitando la gestión de los privilegios de acceso de los usuarios seleccionados como las personas que gestionan los privilegios de acceso mediante el cambio de los privilegios de acceso se puede realizar una rápida visión general de la situación actual por medio de estos tres estados.

De acuerdo con otra realización más, el método comprende además el envío a través de una red de ordenadores de una información que representa dichas funciones accesibles de dichos dispositivos conectados en red de información que representa el privilegio de acceso acumulado asociado con cada una de estas funciones y de información que permite la identificación de las identidades de acceso seleccionadas a un ordenador cliente que realiza dicha presentación. Esto es ventajoso ya que el procesamiento relacionado con la indicación de los cambios de los privilegios de acceso se convierte en descentralizado, o sea, que no es necesario el servidor de acceso para “recordar” o almacenar información relativa a una solicitud procedente de un cliente. Por lo tanto, el procesamiento en el servidor de acceso puede ser simplificado y requiere menos capacidad de procesamiento y de memoria.

De acuerdo con una realización dicha información que permite la identificación de las identidades de acceso seleccionadas es una lista que incluye los identificadores de las identidades de acceso seleccionadas.

De acuerdo con otra realización dicha información que permite la identificación de las identidades de acceso seleccionadas es un identificador que identifica la localización de una lista que incluye los identificadores de las identidades de acceso seleccionadas.

En otra realización más el método comprende además el retorno a través del ordenador de la información que representa cada una de dichas funciones accesibles de cada uno de dichos dispositivos conectados en red, de los privilegios de acceso acumulados con cada una de estas funciones, y de información que permite la identificación de las identidades de acceso seleccionadas, en la que el privilegio de acceso acumulado asociado con al menos una función de un dispositivo conectado en red ha sido cambiado en relación con la información correspondiente previamente enviada a través de la red de ordenadores.

De acuerdo con una realización la al menos una función de un dispositivo conectado en red para el cual ha sido cambiado el privilegio de acceso se etiqueta con el fin de indicar que el privilegio de acceso acumulado en esta particular función ha sido cambiado en relación con la correspondiente información previamente enviada a través de la red de ordenadores. La ventaja de esto es que una operación de configuración de los privilegios de acceso del sistema de acuerdo con los privilegios de acceso acumulados desde el cliente puede ser fácilmente extraída de la información relativa a los privilegios de acceso no cambiados. Por lo tanto, tal esquema puede ahorrar potencia y tiempo de procesamiento.

En otra realización dicha acción de indicar un cambio en los privilegios de acceso acumulados en una función específica en un dispositivo conectado en red específico solamente permite el cambio de un privilegio de acceso de una función específica de un dispositivo conectado en red específico para permitir que todos los usuarios identificados por las identidades de acceso seleccionadas accedan a la función específica o para permitir que ninguno de los usuarios seleccionados acceda a la función específica.

De acuerdo con otra realización la selección de una pluralidad de identidades de acceso incluye la selección de una pluralidad de identidades de acceso a partir de las identidades de acceso registradas para usar el sistema.

En una realización posterior la selección de las identidades de acceso incluye la selección de los usuarios individuales.

En otra realización más la selección de las identidades de acceso incluye la selección de los grupos de usuarios.

De acuerdo con otro aspecto del invento un servidor para manejar los privilegios de acceso en un sistema de dispositivos conectados en red comprende un gestor de los privilegios de acceso dispuesto para recuperar información de los privilegios de acceso de identidades de acceso seleccionadas individualmente a las funciones accesibles asociadas con los dispositivos conectados en red, y dispuesto para generar un mensaje que incluye los privilegios de acceso acumulados en vista de las identidades de acceso seleccionadas de dichas funciones de los dispositivos conectados en red, un acumulador de privilegios de acceso dispuesto para acumular los privilegios de acceso de las identidades seleccionadas de dichas funciones accesibles de los dispositivos conectado en red a partir de dicha información recuperada, y un configurador de privilegios de acceso dispuesto para configurar los privilegios de acceso de las funciones accesibles de los dispositivos conectados en red de las identidades de acceso seleccionadas de acuerdo con un mensaje recibido que incluye un indicador que indica que los privilegios de acceso de dicha función del dispositivo conectado en red tiene que ser cambiado.

Un servidor que tiene esta configuración lo hace posible para facilitar las operaciones de cambio de privilegios de acceso de usuarios individuales y una pluralidad de dispositivos conectados en red. Esto puede ser particularmente cierto para operaciones en las que los privilegios de acceso de usuarios no relacionados con una pluralidad de dispositivos tienen que ser cambiados. Acumulando los privilegios de acceso como se ha descrito antes se posibilita tal operación de cambio de privilegios de acceso.

De acuerdo con una realización dicho acumulador de privilegios de acceso está dispuesto para acumular los privilegios de acceso mediante el recuento del número de identidades de acceso seleccionadas que tienen privilegios de acceso a cada una de dichas funciones accesibles de los dispositivos conectados en red.

La ventaja de esto consiste en que no es una forma complicada de conseguir un valor acumulador, o en otros términos conseguir un valor que represente los privilegios de acceso de una pluralidad de usuarios individuales que no han de tener privilegios de acceso idénticos.

De acuerdo con una realización posterior el acumulador de privilegios de acceso está además dispuesto para fijar el privilegio de acceso de una función específica de un dispositivo conectado en red en un valor que indica que todas las identidades de acceso seleccionadas tienen permitido el acceso a la función específica si dicho recuento indica que todos los usuarios seleccionados tienen permitido el acceso a la función específica, a fijar el privilegio de acceso acumulado para una función específica de un dispositivo conectado en red en un valor que indica que ninguna de las identidades de acceso seleccionadas tiene permitido el acceso a la función específica si dicho recuento indica que ninguna de las identidades de acceso seleccionadas tiene permitido el acceso a la función específica, y a fijar el privilegio de acceso acumulado para una función específica de un dispositivo conectado en red en un valor que indica que algunas de las identidades de acceso seleccionadas tienen permitido el acceso a la función si dicho recuento indica que algunas de las identidades de acceso seleccionadas tienen permitido el acceso a la función.

Este acumulador de privilegios de acceso facilita la gestión de los privilegios de acceso de los usuarios seleccionados ya que a la persona que gestiona los privilegios de acceso cambiando dichos privilegios de acceso se le puede dar una rápida visión general de la situación actual por medio de estos tres estados.

De acuerdo con otra realización el gestor de los privilegios de acceso está dispuesto para incluir en dicho mensaje generado información que representa las funciones accesibles de los dispositivos conectados en red, el privilegio de acceso acumulado asociado con cada función incluida, e información que permita la identificación de las identidades de acceso seleccionadas.

De acuerdo con otra realización más el sistema es un sistema de monitorización.

En otra realización las identidades de acceso incluyen una identidad de usuario y en una realización posterior las identidades de acceso incluyen una identidad de grupo de usuarios.

De acuerdo con otro aspecto más del invento un cliente para cambiar los privilegios de acceso a funciones de dispositivos conectados en red de un sistema comprende una pantalla y medios para la introducción de datos, medios para seleccionar las identidades de acceso, estando dichos medios dispuestos para presentar las identidades de acceso en la pantalla y para permitir que un usuario del cliente seleccione las identidades de acceso por medio de los medios de introducción de datos, y medios para cambiar los privilegios de acceso de identidades de acceso seleccionadas a funciones accesibles de los dispositivos conectados en red, estando dichos medios dispuestos para presentar en la pantalla los privilegios de acceso acumulados con relación a dichas funciones accesibles de los dispositivos conectados en red, para permitir que un usuario del cliente seleccione y cambie los privilegios de acceso acumulados de las funciones presentadas, y para generar un mensaje que incluya información de los privilegios de acceso acumulados cambiados.

Este cliente puede presentar la ventaja de facilitar el cambio de los privilegios de acceso a una pluralidad de dispositivos conectados en red y para personalizar los privilegios de acceso de los usuarios.

De acuerdo con una realización los medios para cambiar los privilegios de acceso están dispuestos para recibir un mensaje a través de una interfaz de la red, dicho mensaje incluye información que representa las funciones accesibles de los dispositivos conectados en red, información que representa los privilegios de acceso acumulados asociados con cada una de estas funciones, e información que permite la identificación de las identidades de acceso seleccionadas.

De acuerdo con otra realización dicho mensaje generado incluye información que representa las funciones accesibles de los dispositivos conectados en red, información que representa los privilegios de acceso acumulados asociados con cada una de estas funciones, un indicador que indica cada uno de los privilegios de acceso acumulados que ha sido cambiado, e información que permite la identificación de las identidades de acceso seleccionadas.

De acuerdo con otra realización más la información que permite la identificación de las identidades de acceso seleccionadas es una lista que incluye los identificadores de las identidades de acceso seleccionadas.

De acuerdo con una realización posterior la información que permite la identificación de las identidades de acceso seleccionadas es un identificador que identifica la situación de una lista que incluye los identificadores de los usuarios seleccionados.

En el contexto de la presente aplicación el dispositivo conectado en red debería ser considerado como un dispositivo que incluye los circuitos para permitir el envío y la recepción de señales y/o mensajes por una red de ordenadores y en la que el dispositivo está dispuesto para enviar por la red de ordenadores datos o información resultante de la funcionalidad del dispositivo.

Un posterior campo de aplicabilidad del presente invento será evidente a partir de la descripción detallada dada a continuación. No obstante, se debería entender que la descripción detallada y los ejemplos específicos, en tanto que indican unas realizaciones preferidas del invento, se han dado solamente a modo de ilustración, ya que a partir de la descripción detallada a las personas expertas en la técnica les serán evidentes varios cambios y modificaciones dentro del espíritu y alcance del invento.

Breve descripción de los dibujos

Otras características y ventajas del presente invento serán evidentes a partir de la siguiente descripción detallada de una realización actualmente preferida con respecto a los dibujos que se acompañan, en los que:

la Figura 1 es una visión general de un sistema de acuerdo con una realización del invento;
la Figura 2 es un diagrama de bloques de un servidor de acceso de acuerdo con una realización del invento;
la Figura 3 ilustra datos relativos al invento y almacenados en una base de datos del servidor de acceso de acuerdo con una realización del invento;
la Figura 4 ilustra una matriz de privilegios de acceso acumulados de acuerdo con una realización del invento;
la Figura 5 ilustra un mensaje de información enviado desde el servidor de acceso al cliente de acuerdo con una realización del invento;
la Figura 6 ilustra una matriz de privilegios de acceso acumulados que ha de ser enviada desde el cliente al servidor de acuerdo con una realización del invento;
la Figura 7 es un diagrama de bloques de un cliente de acuerdo con una realización del invento;
la Figura 8 ilustra una Interfaz Gráfica de Usuario (GUI) para seleccionar usuarios de acuerdo con una realización del invento;
la Figura 9 ilustra una GUI para cambiar los privilegios de acceso de usuarios seleccionados a las funciones de dispositivos conectados en red de acuerdo con una realización del invento;
la Figura 10 es un diagrama de flujos que ilustra un método para cambiar los privilegios de acceso asociados con funciones de los dispositivos conectados en red;

la Figura 11 es un diagrama que ilustra la relación temporal entre señales entre el servidor de acceso y el cliente de acuerdo con una realización del invento; y
la Figura 12 es un diagrama que ilustra la relación temporal entre las señales entre el servidor de acceso y el cliente de acuerdo con una realización del invento.

Descripción detallada de una realización

En la Figura 1 se representa de forma esquemática un sistema de acuerdo con una realización del invento. El sistema incluye un servidor de acceso 10 dispuesto para controlar y gestionar los privilegios de acceso de los dispositivos conectados en red 12, 14 y 16. Además el sistema incluye un cliente 18 que puede ser usado para acceder a la información en el servidor de acceso 10 con relación a los privilegios de acceso del sistema, y una red que conecta el servidor 10, los dispositivos conectados en red 12, 14 y 16, y el cliente 18.

El servidor de acceso 10 es un servidor que controla los privilegios de acceso de los usuarios registrados a los dispositivos conectados en red en el sistema. Los dispositivos conectados en red 12, 14 y 16 pueden ser cualquier dispositivo conectado a una red y dispuesto para ser controlado o proporcionar datos a través de la red. El cliente 18 puede ser un ordenador que posibilita un registro sistemático de datos por parte del administrador en el servidor 10 y el acceso a la información asociada con los privilegios de acceso de las identidades de acceso registradas a funciones de los dispositivos conectados en red 12, 14 y 16. De acuerdo con una realización, las identidades de acceso pueden ser identidades de usuarios y/o identidades de grupos de usuarios.

Los dispositivos conectados en red 12, 14 y 16 pueden, tal como se ha manifestado antes, cualquier dispositivo que proporciona datos sobre la red y/o que sea controlable a través de la red. Por ejemplo, un dispositivo conectado en red puede ser una cámara de vídeo 12 con la posibilidad de comunicar a través de la red para entregar vídeo a un servidor de vídeo y/o para recibir señales de control, por ejemplo controlando cualquiera de o cualquier combinación de giro, inclinación, abertura, frecuencia de imagen, resolución de imagen, etc. Tal cámara 12 conectada en red puede ser normalmente operada con fines de monitorización o de vigilancia. Otro ejemplo de un dispositivo conectado en red es un sistema de control de entrada 14 usado para controlar el acceso a instalaciones o zonas cerradas. Sin embargo, una persona experta en la técnica puede considerar muchos otros dispositivos.

De acuerdo con una realización del invento el servidor de acceso 10 incluye todos los componentes y funciones de un servidor ordinario que está dispuesto para manejar, enviar y recibir datos a través de una red de ordenadores. Por lo tanto, el servidor de acceso 10 incluye una CPU, Unidad Central de Proceso, 52 para el procesamiento de las funciones de un servidor ordinario así como las funciones relativas al invento. Además, el servidor de acceso incluye una memoria transitoria 54 para el almacenamiento temporal de datos, información, instrucciones, etc con relación a las funciones de un servidor ordinario así como a las funciones relacionadas con el invento. La memoria transitoria 54 puede por ejemplo ser una RAM, Memoria de Acceso Aleatorio. Además, el servidor de acceso incluye una interfaz de la red 56 para permitir la comunicación con otros dispositivos conectados a la red, por ejemplo los dispositivos conectados en red. Una persona experta sabe cómo aplicar una interfaz de la red.

El servidor de acceso 10 incluye también una memoria no transitoria 58 que puede ser un disco duro, una unidad de estado sólido, o cualquier dispositivo de almacenamiento de datos capaz de almacenar datos incluso cuando con el suministro de energía al dispositivo interrumpido. A la vista del invento la memoria no transitoria está dispuesta para almacenar información de los privilegios de acceso de los usuarios registrados a las funciones de los dispositivos conectados en red en el sistema. La capacidad de almacenamiento tiene que ser adaptada en consecuencia. Además el servidor de acceso puede incluir una interfaz 60 de base de datos para gestionar la entrada y salida de datos a y desde la base de datos. La base de datos puede estar dispuesta en la memoria no transitoria 58 aunque también puede estar dispuesta en otro punto de almacenamiento conectado a la red.

Además de todas las funciones ordinarias y con el fin de configurar o reconfigurar los privilegios de acceso el servidor de acceso 10 puede incluir medios para gestionar la selección de las identidades de acceso 62, medios para gestionar los privilegios de acceso 64, y medios para configurar los privilegios de acceso 66.

Los medios para gestionar la selección de las identidades de acceso 62 están dispuestos para recuperar y enviar una lista de identidades de acceso a un ordenador cliente para la selección de las identidades de acceso. La lista de identidades de acceso puede ser recuperada de la base de datos que incluye los privilegios de acceso asociados con las identidades de acceso registradas, por ejemplo usuarios registrados y/o grupos de usuarios registrados, o puede ser recuperada de un servidor de gestión de usuarios asociado a la red, es decir un servidor que gestione los datos requeridos para autentificar el registro sistemático en la red. Por ejemplo, tal servidor puede incluir el Directorio Activo si el sistema de red es una red basada en Microsoft.

La selección de las identidades de acceso puede estar basada en una cualquiera de esas listas. La lista asociada con el registro sistemático autentificado en la red es ventajosamente usada cuando a nuevas identidades de acceso, es decir no registradas para acceso a los dispositivos conectados en red, se les tiene que dar acceso a los dispositivos conectados en red que requieren privilegios de acceso. La lista de las identidades de acceso registradas para acceder a los dispositivos conectados en red puede ser usada ventajosamente en la selección de las identidades de acceso para las cuales hay que realizar los privilegios de acceso. Además, en el contexto de la

presente aplicación el término identidades de acceso, a la vista de las identidades de acceso para cambiar privilegios de acceso, puede incluir identidades de usuario y/o identidades de grupos de usuarios. En el caso de un grupo de usuarios que es seleccionado y registrado se almacena una identidad del usuario. El grupo de usuarios puede estar dispuesto para incluir identificadores de usuarios de los usuarios asociados con el grupo de usuarios, lo que permite la recuperación de los usuarios incluidos en el grupo de usuarios cuando sea necesario. Esto hace posible seleccionar grupos de usuarios y usuarios únicos para una operación de gestión en los privilegios de acceso y después, si los usuarios del grupo de usuarios cambian los privilegios de acceso del grupo de usuarios, permanece pero cambian los privilegios de acceso de un usuario que abandona o que es añadido al grupo de usuarios.

La lista 90 de identidades de acceso, véase la Figura 3, se almacena en la base de datos del servidor de acceso o se muestra la base de datos asociada al servidor de acceso de acuerdo con una realización. Además de dicha lista 90 de identidades de acceso registradas para acceder a los dispositivos conectados en red la base de datos del servidor de acceso almacena una lista 92 de los dispositivos conectados en red y de las funciones accesibles de los dispositivos y una lista 94 en la que un privilegio de acceso se asocia a cada función de cada dispositivo y para cada una de las identidades de acceso. La lista 94 puede ser almacenada como una lista o una matriz, aunque con el fin de facilitar la descripción de la información contenida en la lista la describiremos como una matriz, y de ahora en adelante se hará referencia a la lista 94 como la matriz 94 de privilegios de acceso. De este modo, la matriz 94 de privilegios de acceso es una combinación de la lista de las identidades de acceso registradas 90, de la lista 92 de dispositivos conectados en red, y de los privilegios de acceso de estas identidades de acceso en relación con las funciones de los dispositivos conectados en red. Una forma de describir una realización de tal matriz 94 de privilegios de acceso, véase el ejemplo de la Figura 3, es hacer que cada línea represente un dispositivo conectado en red y una combinación de identidades de acceso, por ejemplo la línea 1 de la matriz representa el dispositivo conectado en red 1 y la identidad de acceso 1, la línea 2 representa el dispositivo conectado en red 1 y la identidad de acceso 2, la línea 3 representa el dispositivo conectado en red 1 y la identidad de acceso 3, la línea 4 representa el dispositivo 2 y la identidad de acceso 1, la línea 5 representa el dispositivo conectado en red 2 y la identidad de acceso 2, etc, y hacer que cada columna represente una función de los dispositivos.

Volviendo ahora a la Figura 2, los medios para gestionar la selección de las identidades de acceso 62 están dispuestos para recibir del cliente una indicación de las identidades de acceso seleccionadas. Un gestor 68 de la matriz de privilegios de acceso está dispuesto para añadir las identidades de acceso seleccionadas si dichas identidades de acceso seleccionadas son identidades de acceso que no están registradas en la matriz de privilegios de acceso. Además, el gestor de la matriz de privilegios de acceso puede estar dispuesto para enviar la información desde la matriz de privilegios de acceso asociada con las identidades de acceso seleccionadas a un acumulador 70 de los privilegios de acceso.

El acumulador 70 de los privilegios de acceso está dispuesto para acumular los privilegios de acceso de las identidades de acceso seleccionadas en una estructura de información que tiene que ser enviada al ordenador cliente con el fin de permitir cambios de los privilegios de acceso que han de ser realizados en el ordenador cliente. El acumulador 70 de privilegios de acceso hace un recuento de cuántas identidades de acceso seleccionadas están registradas como que tienen acceso a cada una de las funciones de cada uno de los dispositivos conectados en red. Si todas las identidades de acceso seleccionadas tienen acceso a una función específica de un dispositivo conectado en red se crea una entrada con relación a esta función particular en este dispositivo particular que afirma que todas las identidades de acceso seleccionadas tienen acceso. Si ninguna de las identidades de acceso seleccionadas tiene acceso a una función específica de un dispositivo conectado en red se crea una entrada con relación a esta función particular en este dispositivo particular que afirma que ninguna de las identidades de acceso seleccionadas tiene acceso. En este sistema se usa un tercer indicador. Este tercer indicador se usa si algunas pero no todas las identidades de acceso seleccionadas tienen acceso a una función específica de un dispositivo conectado en red y después se crea una entrada con relación a esta función particular en este dispositivo particular que afirma que algunas de las identidades de acceso seleccionadas tienen acceso. Por lo tanto, la lista o matriz acumulada identifica por medio de tres estados los privilegios de acceso acumulados de las identidades de acceso seleccionadas a cada función de cada dispositivo conectado en red. En la Figura 4 se muestra un ejemplo de una parte de una matriz acumulada. Dichos tres estados pueden ser referidos o indicados en la transmisión de datos por un indicador de “acceso a todo”, un indicador de “acceso a nada”, y un indicador de “acceso a algo”. En una realización el indicador de “acceso a todo” está indicado como un valor VERDADERO, el indicador de “acceso a nada”, está indicado como un valor FALSO, y el indicador de “acceso a algo” está indicado como un indicador NULO.

Volviendo a la Figura 2, los medios para gestionar los privilegios de acceso 64 están dispuestos para generar un mensaje que incluye una información que permite un cambio de los privilegios de acceso del cliente. Esta información puede consistir en los privilegios de acceso acumulados y en cada función asociada de cada dispositivo conectado en red y en una lista de identidades de acceso seleccionadas, por ejemplo la matriz acumulada y una lista de las identidades de acceso seleccionadas. En la Figura 5 se muestra un ejemplo del contenido de tal mensaje. La lista de identidades de acceso seleccionadas puede ser representada en el mensaje que incluye la información de configuración de los privilegios de acceso como un enlace o puntero hacia tal lista almacenada en el servidor o hacia

cualquier otro lugar de la red. De hecho, la lista de las identidades de acceso seleccionadas no está necesariamente presente o incluso no es usada en el cliente.

Además, los medios para configurar los privilegios de acceso 66 están dispuestos para recibir una solicitud de configuración por parte del cliente. Dicha solicitud recibida incluye los privilegios de acceso acumulados ajustados para cada función asociada de cada dispositivo conectado en red y la lista de las identidades de acceso seleccionadas. Si la lista de identidades de acceso no es enviada al cliente como se ha descrito antes se devuelve el enlace o puntero enviado desde el servidor de acceso al cliente. Los medios para configurar los privilegios de acceso 66 están también dispuestos para dar instrucciones al gestor 68 de la matriz de los privilegios de acceso para fijar los privilegios de acceso en la matriz de privilegios de acceso de acuerdo con la solicitud de configuración de dichos privilegios de acceso. En una realización la solicitud recibida incluye adicionalmente un indicador para cada función de cada dispositivo y cuyo indicador indica si han cambiado los privilegios de acceso de la función del dispositivo para las identidades de acceso seleccionadas en relación con los privilegios de acceso de la lista acumulada enviada desde el servidor de acceso 10. Los bits sucios 98 pueden ser usados para indicadores de los privilegios de acceso cambiados como está indicado en el ejemplo de una lista acumulada devuelta mostrada en la Figura 6. En el ejemplo de la Figura 6 un conjunto de bits sucios fijado en “1” indica los privilegios de acceso cambiados, y un conjunto de bits sucios fijado en “0” indica que no hay cambios en los privilegios de acceso. La posición de los bits sucios puede también estar presente en la lista acumulada enviada desde el servidor de acceso al cliente.

En la Figura 7 se ha mostrado un cliente que puede ser usado en el invento. El cliente incluye una interfaz de la red 102, una CPU 104, una memoria 106, unos medios de introducción de datos 108 y una pantalla 110. La interfaz de la red 102 está dispuesta para posibilitar la comunicación con otros dispositivos conectados a la red, por ejemplo el servidor de acceso. Las personas expertas en la técnica saben cómo poner en práctica una interfaz de la red. La CPU 104 está dispuesta para procesar las funciones del cliente y la memoria se usa para el almacenamiento de información, por ejemplo el almacenamiento temporal de las instrucciones ejecutadas, etc. El cliente puede ser cualquier ordenador general, tal como un puesto de trabajo, un ordenador personal, un ordenador portátil pequeño, un teléfono inalámbrico, un Asistente Digital Personal, etc, o puede ser un ordenador especializado diseñado para ser un cliente del servidor de acceso solamente.

El cliente incluye medios para seleccionar las identidades de acceso 112 y medios para cambiar los privilegios de acceso 114. Los medios para seleccionar las identidades de acceso 112 están dispuestos para acceder al servidor de acceso y solicitar al servidor de acceso que proporcione información de las identidades de acceso del sistema o de los usuarios de la red. A partir de esta información el operador del cliente puede seleccionar dichas identidades de acceso seleccionadas y devolver una lista de las identidades de acceso seleccionadas.

En una realización los medios para seleccionar usuarios 112 están dispuestos para visualizar una interfaz en la que el usuario del cliente sea capaz de elegir entre añadir nuevas identidades de acceso o cambiar los privilegios de acceso de las identidades de acceso ya registradas. Además está dispuesto para enviar al servidor de acceso una indicación de cuál de las opciones el usuario del cliente seleccionó al servidor de acceso. Además, los medios para seleccionar las identidades de acceso 112 están dispuestos para recibir una lista de identidades de acceso y presentar el contenido de la lista en la pantalla 110 a través de una interfaz que permite la selección de las identidades de acceso a partir de la lista. En la Figura 8 se muestra un ejemplo de tal interfaz. Los usuarios pueden ser marcados por medio de la indicación de cada línea que presenta unas identidades de acceso de interés, y cuando se marcan los usuarios de interés el botón de selección se usa para enviar la lista de las identidades de acceso seleccionadas al servidor de acceso.

Los medios para cambiar los privilegios de acceso 114 están dispuestos para recibir un mensaje de información que incluye información que permita un cambio de los privilegios de acceso por medio del cliente. Esta información puede consistir en los privilegios de acceso acumulados y cada función asociada de cada dispositivo conectado en red y una lista de las identidades de acceso seleccionadas, por ejemplo la lista acumulada y una lista de las identidades de acceso seleccionadas, como se ha descrito en conexión con el servidor de acceso. En la Figura 5 se muestra un ejemplo de un mensaje de información. Los medios para cambiar los privilegios de acceso incluyen además unos medios para presentar la información del mensaje de información en una interfaz que permite al usuario del cliente cambiar los privilegios de acceso. En la Figura 9 se muestra un ejemplo de tal interfaz para cambiar los privilegios de acceso. En esta realización particular de la interfaz los dispositivos conectados en red, presentados como cámaras y dispositivos I/O, están categorizados y dispuestos bajo etiquetas independientes 120, 122 de la interfaz. Cada dispositivo está presentado en una línea separada, las funciones están presentadas en columnas, y los privilegios de acceso acumulados de cada función de cada dispositivo están presentados en la intersección del dispositivo conectado en red y la función. Una “x” indica que todas las identidades de acceso seleccionadas tienen acceso, una celda vacía indica que ninguna de las identidades de acceso seleccionadas tiene acceso, y una “o” indica que algunas identidades de acceso, pero no todas, tienen acceso. La interfaz está dispuesta para alternativamente cambiar de “x” a vacío y de y de vacío a “x” en respuesta al usuario que selecciona la celda. En casos en los que el privilegio de acceso está indicado por “o” puede ser cambiado a “x” o vacío pero un vacío o “x” no puede ser cambiado a “o”. Por lo tanto, solamente es posible indicar si todas o ninguna de las identidades de acceso seleccionadas han de tener acceso. Cuando los usuarios del cliente han terminado con el cambio de los

privilegios de acceso ha de seleccionarse el botón OK. Los medios para cambiar los privilegios de acceso están dispuestos para cambiar la lista acumulada de acuerdo con los cambios indicados en la interfaz e indicar cada privilegio de acceso cambiado, esto es cada privilegio de acceso a una función cambiado de un dispositivo conectado en red, con un indicador que indica un cambio de los privilegios de acceso de todos los usuarios seleccionados con respecto a la función del dispositivo conectado en red. Esta indicación puede ser puesta en práctica fijando un bit sucio como se ha comentado anteriormente en conexión con el servidor de acceso.

Los medios para cambiar los privilegios de acceso 114 están también dispuestos para enviar al servidor de acceso la lista acumulada cambiada por el usuario del cliente.

De acuerdo con otro aspecto del invento se ha puesto en práctica en el sistema un método para configurar privilegios de acceso para funciones de dispositivos conectados en red, véase la Figura 10. El sistema puede ser cualquier sistema de autorización que permita la gestión de los privilegios de acceso. El sistema puede ser un sistema que aplique la puesta en práctica de la discriminación de solamente permitir dispositivos de acceso de usuarios que estén registrados como que tiene permitido su acceso al usuario particular. Por ejemplo, el sistema puede ser un acceso al módulo de autorización o a la gestión del sistema a dispositivos y/o funciones de un sistema de seguridad, a un sistema de vigilancia, a un sistema de monitorización, etc, y en el que los usuarios de sistemas diferentes han de tener acceso a los diferentes dispositivos y tal vez incluso tipos de acceso diferentes a los dispositivos a los que tienen acceso.

Un usuario de un ordenador cliente, el método puede ser restringido a este usuario que tiene privilegios de administrador para la red y para el sistema o a este usuario que tiene privilegios de administrador para el sistema solamente, inicia la configuración de los privilegios de acceso para funciones de los dispositivos conectados en red en el sistema haciendo que el cliente opere para enviar una solicitud de una lista de identidades de acceso, paso 602. En respuesta a la solicitud el servidor proporciona acceso a una lista de identidades de acceso registradas para uso de la red y/o para uso del sistema, paso 604. En el cliente la lista de identidades de acceso es presentada a continuación, por ejemplo por medio de la interfaz descrita en conexión con la Figura 8. El usuario que opera el cliente a continuación hace que el cliente opere y seleccione las identidades de acceso que tienen los privilegios de acceso que han de ser gestionados, paso 606.

Por medio del invento puede ser ventajoso seleccionar las identidades de acceso que han de tener una pluralidad de privilegios de acceso idénticos debido a que la interfaz para gestionar los privilegios de acceso está dispuesta para procesar las identidades de acceso de forma idéntica. Las identidades de acceso seleccionadas son después usadas en el servidor de acceso para preparar una matriz de privilegios de acceso acumulados solamente de las identidades de acceso seleccionadas. Si las identidades de acceso seleccionadas son identidades de acceso no registradas en el sistema entonces las identidades de acceso seleccionadas han de ser añadidas a las identidades de acceso registradas del sistema, por ejemplo las identidades de acceso pueden ser registradas para la red, por ejemplo autentificadas, pero no el sistema, por ejemplo autorizadas para el sistema.

Por lo tanto, el servidor de acceso recupera los privilegios de acceso asociados con las identidades de acceso seleccionadas, paso 608, y después se cuenta y se acumula el número de identidades de acceso que tienen acceso a cada función de cada uno de los dispositivos, paso 610. Esto puede ser realizado haciendo que el servidor cuente el número de identidades de acceso seleccionadas que tienen acceso a cada función de cada dispositivo conectado en red y que genera privilegios de acceso acumulados comparando el número de identidades de acceso seleccionadas que tienen acceso a cada función de cada dispositivo conectado en red con el número de identidades de acceso seleccionadas. Los privilegios de acceso acumulados pueden representar bien todas las identidades de acceso seleccionadas que tienen acceso, ninguna de las identidades de acceso seleccionadas que tienen acceso, o algunas de las identidades de acceso seleccionadas que tienen acceso. De acuerdo con una realización todas las identidades de acceso seleccionadas de los privilegios de acceso acumulados que tienen acceso están representadas por un valor “VERDADERO”, ninguna de las identidades de acceso seleccionadas que tienen acceso está representada por un valor “FALSO”, y algunas de las identidades de acceso seleccionadas que tienen acceso están representadas por un valor “NULO”.

A partir de los privilegios de acceso acumulados resultantes el servidor genera una estructura de datos, paso 612, que incluye una pluralidad de introducciones de datos, representando cada una un dispositivo conectado en red, una función asociada con el dispositivo conectado en red, y los privilegios de acceso acumulados para esta particular función de este particular dispositivo en relación con las identidades de acceso seleccionadas. La estructura de datos incluye una de esas estructuras de datos para cada función de cada dispositivo conectado en red. La estructura de datos generada es después enviada al cliente junto con la lista de las identidades de acceso seleccionadas. En una realización la lista de las identidades de acceso seleccionadas enviada al cliente es sustituida por un enlace o un puntero hacia la lista, y a continuación la lista puede ser almacenada en el servidor.

Cuando la estructura de privilegios de acceso acumulados asociados con funciones y dispositivos conectados en red es recibida en el cliente una interfaz del cliente presenta la información en la pantalla conectada al cliente, paso 614.

De acuerdo con una realización se presenta en una interfaz la información de la estructura de datos de los privilegios de acceso acumulados para presentación y cambio de los privilegios de acceso, por ejemplo en una interfaz como la descrita en conexión con la Figura 9. A continuación se permite al operador del cliente que cambie los privilegios de acceso acumulados a través de la interfaz solamente mediante la selección de un privilegio de acceso específico, el cual tras cada selección alterna entre todas las identidades de acceso seleccionadas que dan acceso y ninguna de las identidades de acceso seleccionadas que dan acceso.

Cada cambio de privilegios de acceso se almacena en la estructura de datos y puede ser indicado con un indicador, por ejemplo un bit sucio. En ese momento el operador en el cliente decide que el cambio de los privilegios de acceso con relación a las identidades de acceso seleccionadas están finalizados, en este momento al cliente se le da la instrucción de devolver la estructura de datos cambiados al servidor de acceso junto con la lista de identidades de acceso seleccionadas, y la estructura de datos de los privilegios de acceso acumulados se devuelve al servidor de acceso, paso 618.

Tras la recepción de la estructura de datos cambiados el servidor busca un indicador que indique un privilegio de acceso cambiado y configura de nuevo la función particular del dispositivo conectado en red particular asociado a este indicador para todos los usuarios seleccionados de la lista de identidades de acceso seleccionadas, paso 620. La búsqueda y configuración se repite hasta que se han encontrado todas las entradas que están indicadas como cambiadas. Entonces ya está en marcha la nueva configuración de los privilegios de acceso del sistema.

El paso 602 de la Figura 10 en el que un usuario hace que el cliente opere para enviar una solicitud de una lista de identidades de acceso puede dar como resultado una o dos recuperaciones diferentes de identidades de acceso o de usuarios autentificados. El usuario que opera el cliente puede decidir añadir posteriores identidades de acceso al sistema, y en tal caso el servidor de acceso recupera la lista de usuarios o grupos de usuarios desde un servidor que gestiona el acceso y la autentificación de la red. Los usuarios seleccionados quedarán entonces también registrados en el registro del sistema. Por otra parte, el usuario que opera el cliente puede decidir cambiar los privilegios de las identidades de acceso que ya tienen privilegios de acceso al sistema. A continuación el servidor de acceso recupera la lista de las identidades de acceso en el servidor de acceso.

En la Figura 11 se describe la señalización entre el cliente y el servidor. El ejemplo dado en la Figura 11 se refiere a una situación en la que el usuario del cliente intenta añadir nuevos usuarios al sistema. A continuación el usuario indica que él intenta añadir usuarios o grupos de usuarios y el cliente envía una solicitud al servidor de acceso de una lista de todos los usuarios de la red, 702, a partir de la cual en el cliente se puede realizar una selección. El servidor de acceso establece contacto con el acceso a la red y el servidor de autentificación y recupera información de usuario y envía los datos al cliente, 704. En el cliente se realiza una selección de usuarios y se envía una solicitud para rectificar/fijar los privilegios de acceso de los usuarios seleccionados, 706. En respuesta a esta solicitud el servidor de acceso devuelve una estructura de información que incluye los privilegios de acceso acumulados de los usuarios seleccionados a la vista de cada función de cada dispositivo conectado en red, 708. La estructura de datos es rectificada en el cliente y la estructura de información rectificada es devuelta al servidor de acceso, 710. La estructura de información rectificada puede incluir un indicador que indica los privilegios de acceso que han sido rectificados.

En la Figura 12 se muestra un esquema de señalización similar al esquema de la Figura 11. El ejemplo se refiere a una situación en la que el usuario intenta rectificar los privilegios de acceso de las identidades de acceso ya registradas. Por lo tanto, el cliente envía un mensaje solicitando las identidades de acceso registradas, 722, y recibe los datos que identifican las identidades de acceso registradas, 724. El usuario en el cliente realiza a continuación una selección a partir de estos datos y realiza la misma señalización que en la Figura 11, es decir las señales 726-730 corresponden a las señales 706-710 de la Figura 11.

REIVINDICACIONES

1. Método para la configuración de privilegios de acceso en un sistema de dispositivos conectados en red (12, 14, 16), comprendiendo dicho método:

seleccionar una pluralidad de identidades de acceso;
recuperar información de privilegios de acceso de cada una de las identidades de acceso seleccionadas a las funciones accesibles de los dispositivos conectados en red (12, 14, 16);
caracterizado por
acumular los privilegios de acceso de las identidades de acceso seleccionadas para cada una de dichas funciones accesibles de cada uno de dichos dispositivos conectados en red (12, 14, 16), en el que dicha acumulación de los privilegios de acceso incluye el recuento del número de identidades de acceso seleccionadas que tienen privilegios de acceso a cada una de dichas funciones de cada uno de dichos dispositivos conectados en red (12, 14, 16);
presentar dichos privilegios de acceso acumulados para cada una de dichas funciones accesibles de cada uno de dichos dispositivos conectados en red (12, 14, 16) en una interfaz que permite la edición de los privilegios de acceso acumulados;
indicar un cambio en los privilegios de acceso acumulados a una función específica en un dispositivo conectado en red específico (12, 14, 16); y
configurar la función específica del dispositivo conectado en red específico (12, 14, 16) para permitir el acceso por las identidades de acceso seleccionadas de acuerdo con el cambio indicado de los privilegios de acceso acumulados.

2. Método de acuerdo con la reivindicación 1, en el que dicha acumulación de privilegios de acceso incluye además:

fijar el privilegio de acceso acumulado para una función específica de un dispositivo conectado en red (12, 14, 16) en un valor que indica que todas las identidades de acceso seleccionadas tienen permitido el acceso a la función específica si dicho recuento indica que todas las identidades de acceso seleccionadas tienen permitido el acceso a dicha función específica;
fijar el privilegio de acceso acumulado para una función específica de un dispositivo conectado en red en un valor que indica que ninguna de las identidades de acceso tiene permitido el acceso a la función específica si dicho recuento indica que ninguna de las identidades de acceso tiene permitido el acceso a dicha función específica; y
fijar el privilegio de acceso acumulado para una función específica de un dispositivo conectado en red en un valor que indica que algunas de las identidades de acceso seleccionadas tienen permitido el acceso a la función si dicho recuento indica que algunas de las identidades de acceso seleccionadas tienen permitido el acceso a dicha función.

3. Método de acuerdo con cualquiera de las reivindicaciones 1-2, que además comprende el envío por medio de una red de ordenadores (20) de información que representa dichas funciones accesibles de dichos dispositivos conectados en red (12, 14, 16), información que representa el privilegio de acceso acumulado asociado con cada una de estas funciones, e información que posibilita la identificación de las identidades de acceso seleccionadas, a un ordenador cliente (18) que realiza dicha presentación.

4. Método de acuerdo con la reivindicación 3, en el que la información que posibilita la identificación de las identidades de acceso seleccionadas es una lista (90) que incluye los identificadores de las identidades de acceso seleccionadas.

5. Método de acuerdo con la reivindicación 3, en el que la información que posibilita la identificación de las identidades de acceso seleccionadas es un identificador que identifica la situación de una lista que incluye los identificadores de las identidades de acceso seleccionadas.

6. Método de acuerdo con cualquiera de las reivindicaciones 3-5, que además comprende la devolución por medio de la red de ordenadores (20) de información que representa cada una de dichas funciones accesibles de cada uno de dichos dispositivos conectados en red (12, 14, 16), de privilegios de acceso acumulados con cada una de estas funciones, y de información que posibilita la identificación de las identidades de acceso seleccionadas, en el que el privilegio de acceso acumulado asociado con al menos una función de un dispositivo conectado en red ha sido cambiado en relación con la correspondiente información anteriormente enviada a través de la red de ordenadores (20).

7. Método de acuerdo con la reivindicación 6, en el que al menos una función de un dispositivo conectado en red (12, 14, 16) para el que ha sido cambiado el privilegio de acceso acumulado se etiqueta con el fin de indicar que el privilegio de acceso acumulado a esta función particular ha sido cambiado en relación con la correspondiente información anteriormente enviada a través de la red de ordenadores (20).

8. Método de acuerdo con cualquiera de las reivindicaciones 1-7, en el que dicha acción de indicar un cambio en los privilegios de acceso acumulados a una función específica en un dispositivo conectado en red específico (12, 14, 16) solamente hace posible cambiar un privilegio de acceso de una función específica de un dispositivo conectado en red específico (12, 14, 16) para permitir que todos los usuarios identificados por las identidades de acceso seleccionadas accedan a la función específica o no permitir a ninguno de los usuarios seleccionados acceder a la función específica.

9. Método de acuerdo con cualquiera de las reivindicaciones 1-8, en el que la selección de una pluralidad de identidades de acceso incluye la selección de una pluralidad de identidades de acceso a partir de las identidades de acceso registradas para usar el sistema.

10. Método de acuerdo con cualquiera de las reivindicaciones 1-9, en el que la selección de las identidades de acceso incluye la selección de usuarios individuales.

11. Método de acuerdo con cualquiera de las reivindicaciones 1-10, en el que la selección de las identidades de acceso incluye la selección de grupos de usuarios.

12. Servidor para gestionar los privilegios de acceso en un sistema de dispositivos conectados en red (12, 14, 16), comprendiendo el servidor:

unos medios (62) para gestionar la selección de las identidades de acceso dispuestas para recibir de un cliente (18) una indicación de las identidades de acceso seleccionadas;
caracterizado por
un gestor (68) de privilegios de acceso dispuesto para recuperar información de los privilegios de acceso de las identidades de acceso seleccionadas a las funciones accesibles asociadas con los dispositivos conectados en red (12, 14, 16) y dispuesto para generar un mensaje que incluya los privilegios de acceso acumulados en vista de las identidades de acceso seleccionadas para dichas funciones de los dispositivos conectados en red (12, 14, 16);
un acumulador (70) de privilegios de acceso dispuesto para acumular los privilegios de acceso de las identidades de acceso seleccionadas para dichas funciones de los dispositivos conectados en red (12, 14, 16) a partir de dicha información recuperada mediante el recuento del número de identidades de acceso seleccionadas que tienen privilegios de acceso a cada una de dichas funciones accesibles de los dispositivos conectados en red (12, 14, 16); y
un configurador (66) de privilegios de acceso dispuesto para configurar los privilegios de acceso de las funciones accesibles de los dispositivos conectados en red (12, 14, 16) para las identidades de acceso seleccionadas de acuerdo con un mensaje recibido que incluye un indicador (98) que indica que los privilegios de acceso de dicha función del dispositivo conectado en red (12, 14, 16) ha de ser cambiado.

13. Servidor de acuerdo con la reivindicación 12, en el que dicho acumulador de privilegios de acceso está dispuesto para
fijar el privilegio de acceso acumulado para una función específica de un dispositivo conectado en red (12, 14, 16) en un valor que indica que todas las identidades de acceso seleccionadas tienen permitido el acceso a la función específica si dicho recuento indica que todos los usuarios seleccionados tienen permitido el acceso a dicha función específica;
fijar el privilegio de acceso acumulado para una función específica de un dispositivo conectado en red (12, 14, 16) en un valor que indica que ninguna de las identidades de acceso seleccionadas tiene permitido el acceso a la función específica si dicho recuento indica que ninguna de las identidades de acceso seleccionadas tiene permitido el acceso a dicha función específica; y
fijar el privilegio de acceso acumulado para una función específica de un dispositivo conectado en red (12, 14, 16) en un valor que indica que algunas de las identidades de acceso seleccionadas tienen permitido el acceso a la función específica si dicho recuento indica que algunas de las identidades de acceso seleccionadas tienen permitido el acceso a dicha función.

14. Servidor de acuerdo con cualquiera de las reivindicaciones 12-13, en el que el gestor (68) de los privilegios de acceso está dispuesto para incluir en dicho mensaje generado la información que representa las funciones accesibles de los dispositivos conectados en red (12, 14, 16), el privilegio de acceso acumulado asociado con cada función incluida, y la información que posibilita la identificación de las identidades de acceso seleccionadas.

15. Servidor de acuerdo con cualquiera de las reivindicaciones 12-14, en el que el sistema es un sistema de monitorización.

16. Servidor de acuerdo con cualquiera de las reivindicaciones 12-15, en el que el identificador de acceso incluye una identidad de usuario.

17. Servidor de acuerdo con cualquiera de las reivindicaciones 12-16, en el que el identificador de acceso incluye una identidad de grupo de usuarios.

18. Cliente para cambiar los privilegios de acceso a funciones de los dispositivos conectados en red (12, 14, 16) de un sistema, comprendiendo dicho cliente:

una pantalla (110);
unos medios de introducción de datos (108);
caracterizado por
medios para seleccionar identidades de acceso (112), estando dichos medios (112) dispuestos para acceder a un servidor de acceso (10) y para solicitar al servidor de acceso (10) que proporcione información de las identidades de acceso del sistema o de los usuarios de la red, y estando dichos medios (112) dispuestos para presentar las identidades de acceso en la pantalla (110) y para permitir a un usuario del cliente que seleccione las identidades de acceso a través de los medios de introducción de datos (108); y
medios para cambiar los privilegios de acceso (114) para identidades de acceso seleccionadas a funciones accesibles de los dispositivos conectados en red (12, 14, 16), estando dichos medios (114) dispuestos para presentar los privilegios de acceso acumulados relativos a dichas funciones accesibles de los dispositivos conectados en red (12, 14, 16) en la pantalla (110) para permitir que un usuario del cliente seleccione y cambie los privilegios de acceso acumulados para las funciones presentadas, y para generar un mensaje que incluya información de los privilegios de acceso acumulados;
en el que dichos privilegios de acceso acumulados incluyen introducciones de datos relativas a cuántas de las identidades de acceso seleccionadas que están registradas tienen acceso a cada una de las funciones de cada uno de los dispositivos conectados en red (12, 14, 16).

19. Cliente de acuerdo con la reivindicación 18, en el que los medios (114) para cambiar los privilegios de acceso están dispuestos para recibir un mensaje a través de una interfaz de la red (102), incluyendo dicho mensaje información que representa las funciones accesibles de los dispositivos conectados en red (12, 14, 16), información que representa los privilegios de acceso acumulados asociados con cada una de estas funciones, e información que posibilita la identificación de las identidades de acceso seleccionadas.

20. Cliente de acuerdo con cualquiera de las reivindicaciones 18-19, en el que dicho mensaje generado incluye información que representa las funciones accesibles de los dispositivos conectados en red (12, 14, 16), información que representa los privilegios de acceso acumulados asociados con cada una de estas funciones, un indicador (98) que indica cada uno de los privilegios de acceso acumulados que ha sido cambiado, e información que posibilita la identificación de las identidades de acceso seleccionadas.

21. Cliente de acuerdo con cualquiera de las reivindicaciones 19 ó 20, en el que la información que posibilita la identificación de las identidades de acceso seleccionadas es una lista (90) que incluye los identificadores de las identidades de acceso seleccionadas.

22. Cliente de acuerdo con cualquiera de las reivindicaciones 19 ó 20, en el la información que posibilita la identificación de las identidades de acceso seleccionadas es un identificador que identifica la situación de una lista (90) que incluye las identidades de los usuarios seleccionados.

23. Cliente de acuerdo con cualquiera de las reivindicaciones 18-22, en el que cada introducción de datos relativos a cuántas de las identidades de acceso seleccionadas que están registradas como que tienen acceso a cada una de las funciones de cada uno de los dispositivos conectados en red (12, 14, 16) se refiere bien a
que todas las identidades de acceso seleccionadas están registradas como que tienen acceso a una función específica de un dispositivo conectado en red (12, 14, 16);
que ninguna de las identidades de acceso seleccionadas está registrada como que tiene acceso a una función específica de un dispositivo conectado en red (12, 14, 16); o
que algunas de las identidades de acceso seleccionadas están registradas como que tienen acceso a una función específica de un dispositivo conectado en red (12, 14, 16).

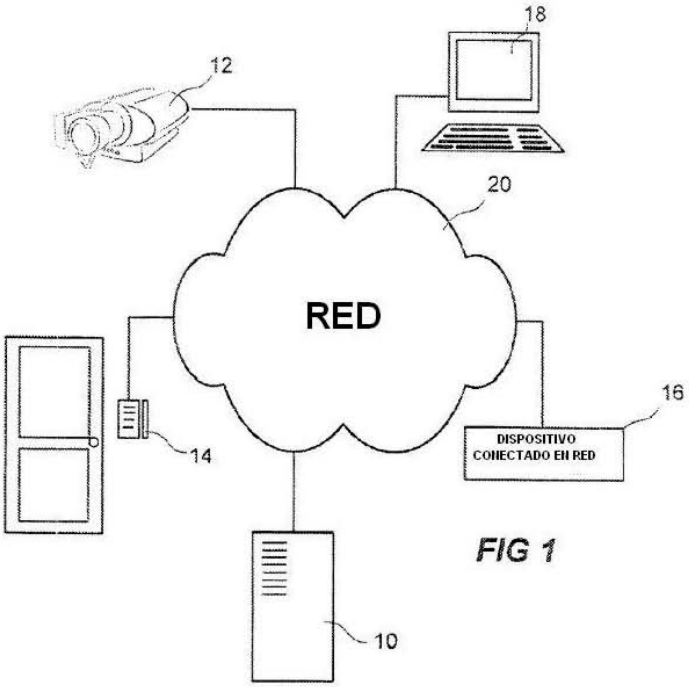

FIG 1

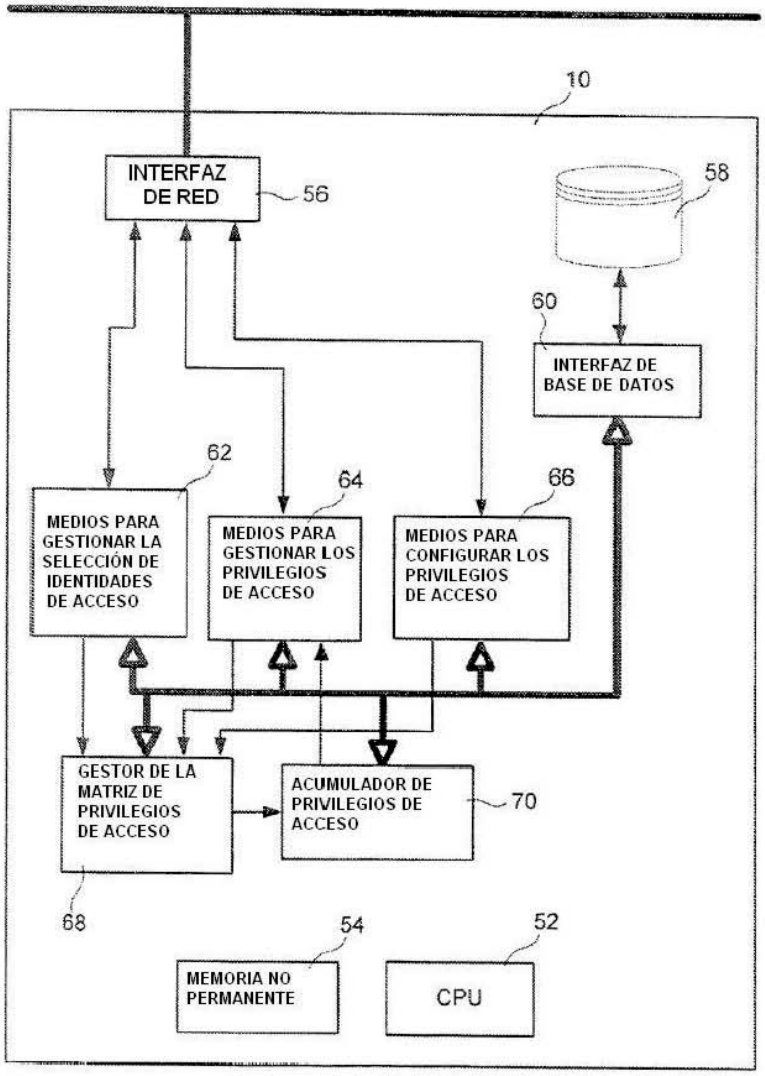
10
INTERFAZ DE RED
56
58
60
INTERFAZ DE BASE DE DATOS
62
MEDIOS PARA GESTIONAR LA SELECCIÓN DE IDENTIDADES DE ACCESO
64
MEDIOS PARA GESTIONAR LOS PRIVILEGIOS DE ACCESO
66
MEDIOS PARA CONFIGURAR LOS PRIVILEGIOS DE ACCESO
GESTOR DE LA MATRIZ DE PRIVILEGIOS DE ACCESO
ACUMULADOR DE PRIVILEGIOS DE ACCESO
70
68
54
MEMORIA NO PERMANENTE
52
CPU

FIG 2

ID/USUARIO	FUNCIONES				
	FNC1	FNC2	FNC3	FNC4	
ND1 AI1	1	0	1	1	
ND1 AI2	1	1	0	0	
ND1 AI3	1	1	1	1	
ND2 AI1	0	0	0	0	
ND2 AI2	1	1	1	1	

FIG 3

ND	FUNCIONES				
	FNC1	FNC2	FNC3	FNC4	
ND 1	VERDADERO	FALSO	NULO	NULO	
ND 2	VERDADERO			—	

FIG 4

ND	FUNCIONES								
	FNC1		FNC2		FNC3		FNC4		
ND1	VERDAD	0	VERDAD	1	VERDAD	1	NULO	0	
ND2	VERDAD	0	VERDAD	1	VERDAD	0	---	0	

98 98 98 98

FIG 6

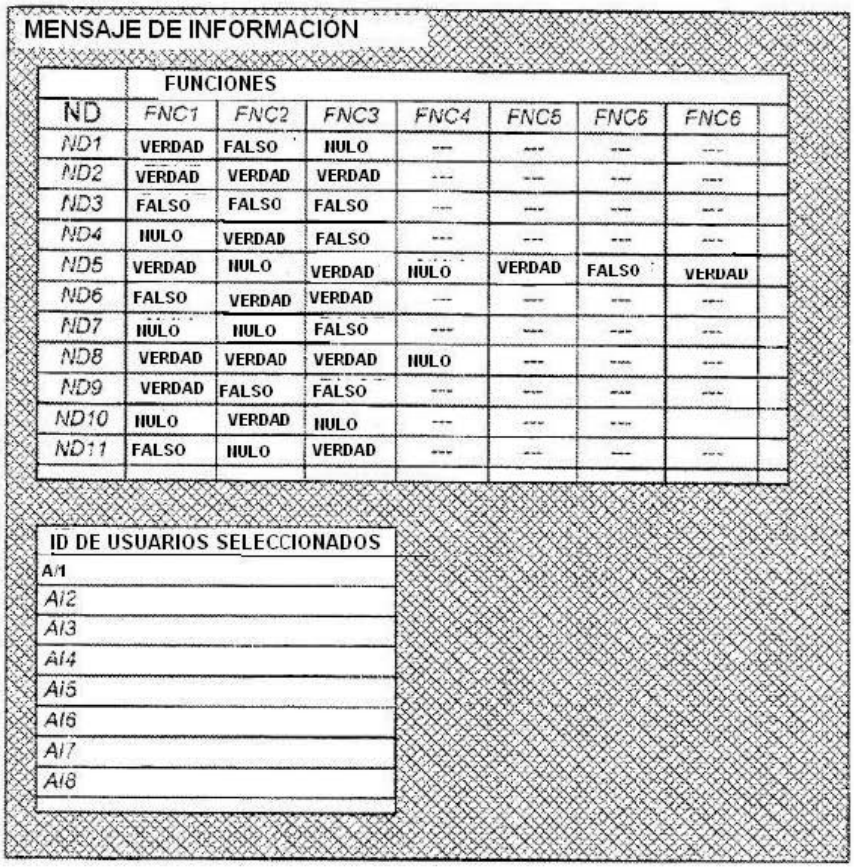
MENSAJE DE INFORMACIÓN
FUNCIONES
ND
FNC1
FNC2
FNC3
FNC4
FNC5
FNC6
FNC6
ND1 VERDAD FALSO NULO --- --- --- ---
ND2 VERDAD VERDAD VERDAD --- --- --- ---
ND3 FALSO FALSO FALSO --- --- --- ---
ND4 NULO VERDAD FALSO --- --- --- ---
ND5 VERDAD NULO VERDAD NULO VERDAD FALSO VERDAD
ND6 FALSO VERDAD VERDAD --- --- --- ---
ND7 NULO NULO FALSO --- --- --- ---
ND8 VERDAD VERDAD VERDAD NULO --- --- ---
ND9 VERDAD FALSO FALSO --- --- --- ---
ND10 NULO VERDAD NULO --- --- ---
ND11 FALSO NULO VERDAD --- --- --- ---
ID DE USUARIOS SELECCIONADOS
AI1
AI2
AI3
AI4
AI5
AI6
AI7
AI8

FIG 5

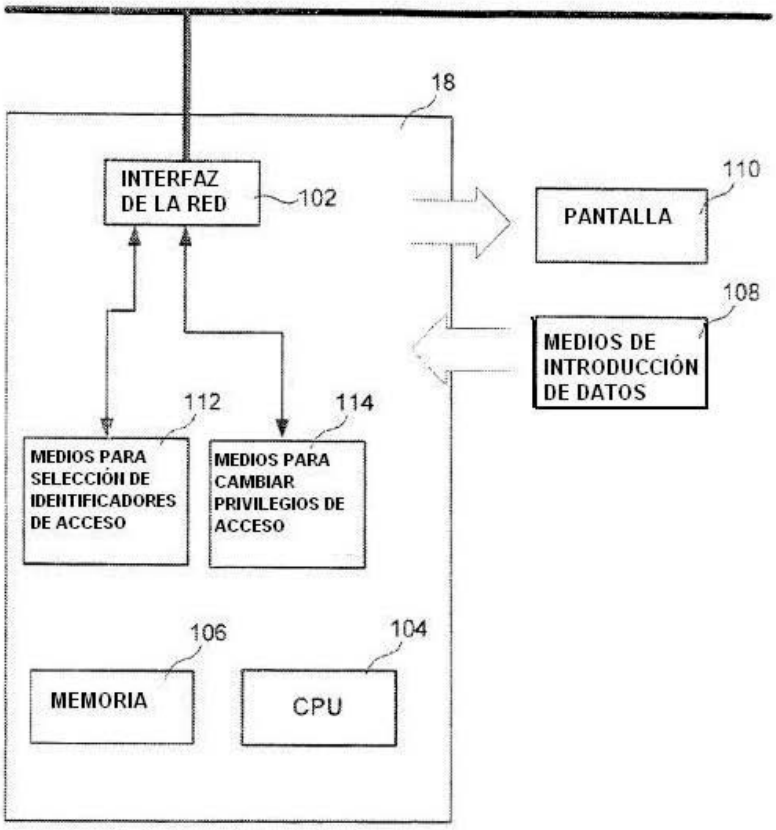
18
INTERFAZ DE LA RED
102
PANTALLA
110
MEDIOS DE INTRODUCCIÓN DE DATOS
108
112
MEDIOS PARA SELECCIÓN DE IDENTIFICADORES DE ACCESO
114
MEDIOS PARA CAMBIAR PRIVILEGIOS DE ACCESO
106
MEMORIA
104
CPU

FIG 7

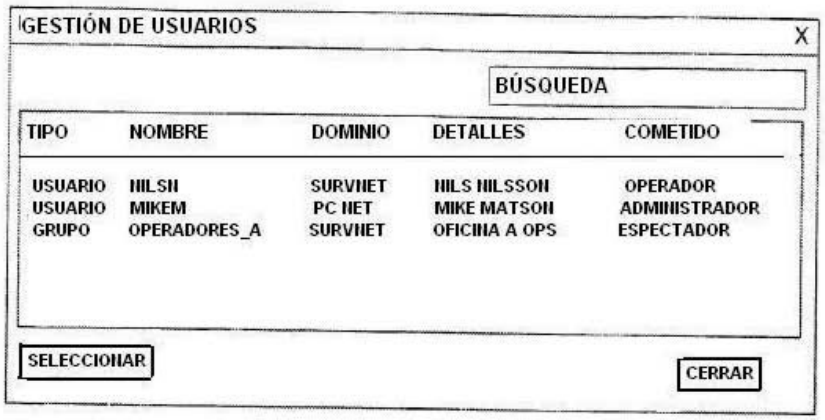
GESTIÓN DE USUARIOS
X
BÚSQUEDA
TIPO
NOMBRE
DOMINIO
DETALLES
COMETIDO
USUARIO NILSH SURVNET NILS NILSSON OPERADOR
USUARIO MIKEM PC NET MIKE MATSON ADMINISTRADOR
GRUPO OPERADORES_A SURVNET OFICINA A OPS ESPECTADOR
SELECCIONAR
CERRAR

FIG 8

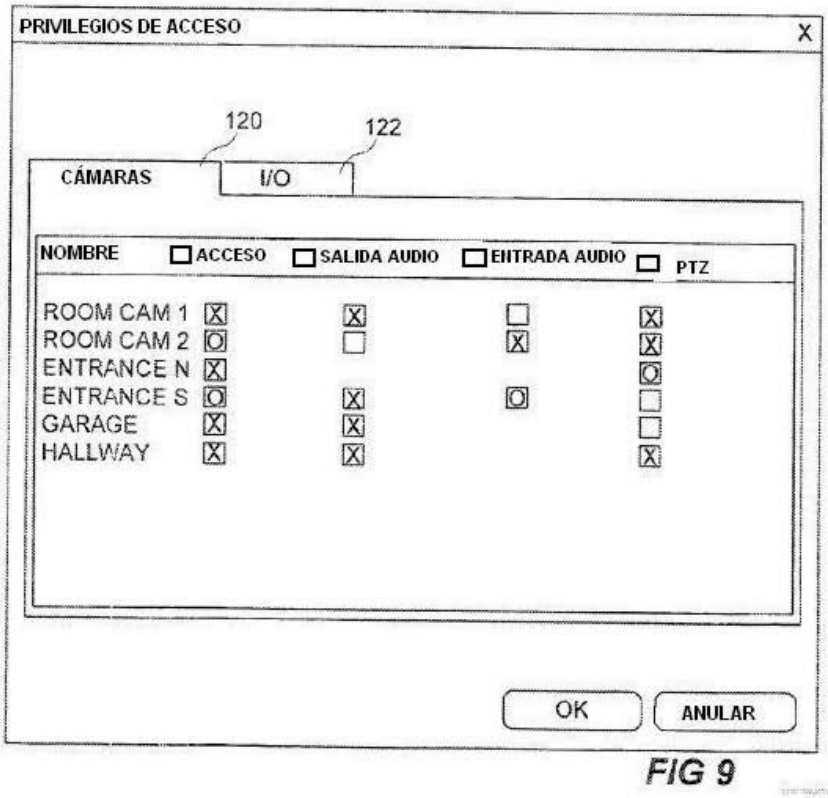
PRIVILEGIOS DE ACCESO
X
120
122
CÁMARAS
I/O
NOMBRE
ACCESO
SALIDA AUDIO
ENTRADA AUDIO
PTZ
ROOM CAM 1
ROOM CAM 2
ENTRANCE N
ENTRANCE S
GARAGE
HALLWAY
OK
ANULAR

FIG 9


602
CLIENTE SOLICITA LA LISTA DE IDENTIDADES DE ACCESO
604
EL SERVIDOR PROPORCIONA ACCESO A LA LISTA DE IDENTIDADES DE ACCESO
606
SE GESTIONAN Y SELECCIONAN LAS IDENTIDADES DE ACCESO PROPUESTAS PARA TENER SUS PRIVILEGIOS DE ACCESO
608
RECUPERAR LOS PRIVILEGIOS DE ACCESO ASOCIADOS CON LAS IDENTIDADES DE ACCESO SELECCIONADAS
610
ACUMULACIÓN DE PRIVILEGIOS DE ACCESO
612
GENERAR LA ESTRUCTURA DE DATOS DE LOS PRIVILEGIOS DE ACCESO ACUMULADOS
614
PRESENTACIÓN EN EL CLIENTE DE LA ESTRUCTURA DE DATOS DE LOS PRIVILEGIOS DE ACCESO ACUMULADOS
616
CAMBIAR PRIVILEGIOS DE ACCESO ACUMULADOS, FIJAR BITS SUCIOS
618
DEVOLVER AL SERVIDOR DE ACCESO LA ESTRUCTURA DE DATOS CAMBIADOS
620
CAMBIAR LOS PRIVILEGIOS DE ACCESO A LAS FUNCIONES INDICADAS CAMBIADOS DE TODAS LAS ENTIDADES DE ACCESO SELECCIONADAS

FIG 10

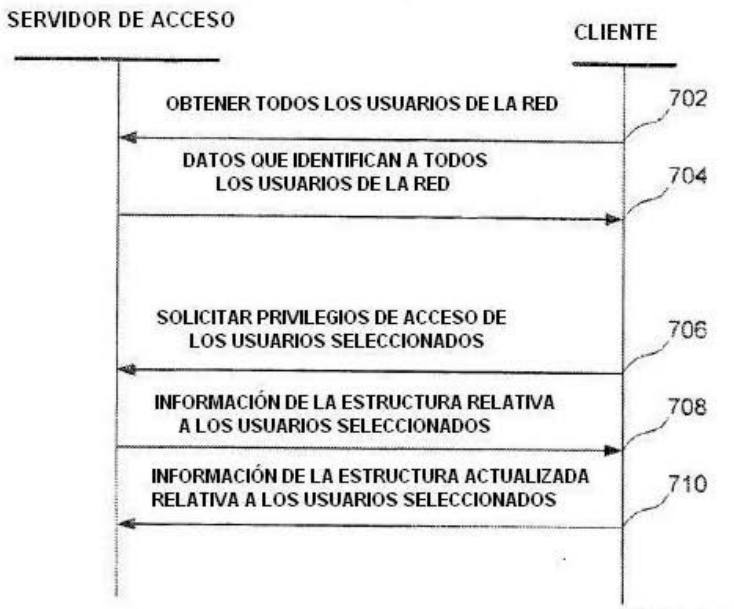
SERVIDOR DE ACCESO
CLIENTE
OBTENER TODOS LOS USUARIOS DE LA RED
702
DATOS QUE IDENTIFICAN A TODOS LOS USUARIOS DE LA RED
704
SOLICITAR PRIVILEGIOS DE ACCESO DE LOS USUARIOS SELECCIONADOS
706
INFORMACIÓN DE LA ESTRUCTURA RELATIVA A LOS USUARIOS SELECCIONADOS
708
INFORMACIÓN DE LA ESTRUCTURA ACTUALIZADA RELATIVA A LOS USUARIOS SELECCIONADOS
710

FIG 11

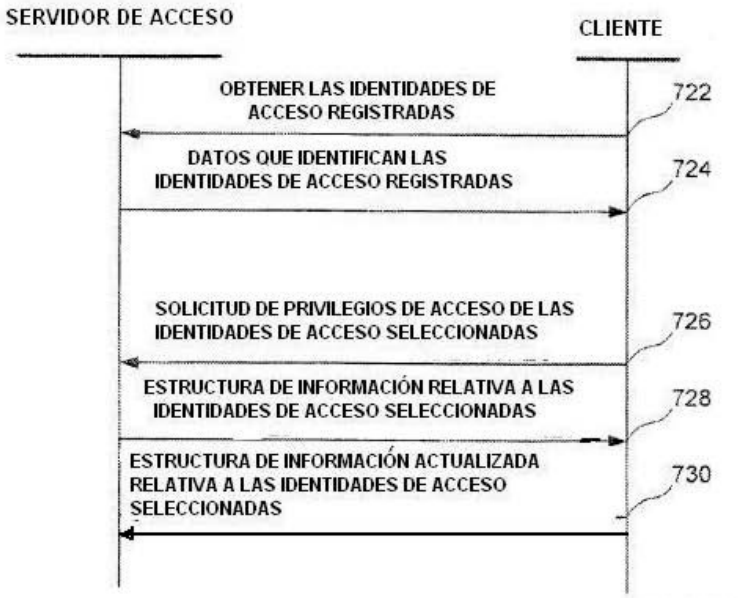
SERVIDOR DE ACCESO
CLIENTE
OBTENER LAS IDENTIDADES DE ACCESO REGISTRADAS
722
DATOS QUE IDENTIFICAN LAS IDENTIDADES DE ACCESO REGISTRADAS
724
SOLICITUD DE PRIVILEGIOS DE ACCESO DE LAS IDENTIDADES DE ACCESO SELECCIONADAS
726
ESTRUCTURA DE INFORMACIÓN RELATIVA A LAS IDENTIDADES DE ACCESO SELECCIONADAS
728
ESTRUCTURA DE INFORMACIÓN ACTUALIZADA RELATIVA A LAS IDENTIDADES DE ACCESO SELECCIONADAS
730

FIG 12