

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 647 295**

51 Int. Cl.:

G07C 9/00

(2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **16.03.2012 PCT/EP2012/054679**

87 Fecha y número de publicación internacional: **04.10.2012 WO12130640**

96 Fecha de presentación y número de la solicitud europea: **16.03.2012 E 12709625 (3)**

97 Fecha y número de publicación de la concesión europea: **18.10.2017 EP 2691940**

54 Título: **Gestión de derechos de acceso a datos operativos y/o datos de control de edificios o de complejos de edificios**

30 Prioridad:

29.03.2011 EP 11160155

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

20.12.2017

73 Titular/es:

**INVENTIO AG (100.0%)
Seestrasse 55
6052 Hergiswil, CH**

72 Inventor/es:

BÜNTER, ADRIAN

74 Agente/Representante:

UNGRÍA LÓPEZ, Javier

ES 2 647 295 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCION

Gestión de derechos de acceso a datos operativos y/o datos de control de edificios o de complejos de edificios

5 La invención se refiere a un sistema para la gestión de derechos de acceso a datos operativos y/o datos de control de edificios o de complejos de edificios. Además, la invención se refiere a un procedimiento para el funcionamiento de un sistema de este tipo.

10 En edificios o complejos de edificios se asumen cada vez más funciones, como el manejo de estores o persianas, el manejo de una instalación de climatización con funciones correspondientes, como calefacción, refrigeración y ventilación a través de sistemas de control modernos, que automatizan el manejo. De la misma manera se realizan, por ejemplo, controles de acceso a partes de edificios o a edificios en un Campus con la ayuda de datos registrados de forma centralizada. Por lo demás, existen en muchos edificios o complejos de edificios instalaciones como por ejemplo ascensores o escaleras mecánicas, que son controlados ellos mismos de nuevo a través de controles que regulan la función de la instalación. En general, actualmente están disponibles en edificios cada vez más datos
15 funcionales y también datos de control para los diferentes sistemas descritos.

Cada vez más se requiere también que se pueda realizar un acceso a datos específicos de estos edificios o componentes desde otro lugar, es decir, de forma remota. En este caso, es concebible que se acceda solamente a
20 datos de estado, pero también es deseable que se puedan realizar a través del acceso remoto manipulaciones en datos de control, Por ejemplo que se pueda realizar una actualización de un software ejecutable en un control a través de acceso remoto.

Sin embargo, un acceso remoto de este tipo a datos específicos del edificio sólo se puede realizar de forma selectiva, de manera que se posibilita el acceso sólo a aquellas personas que disponen para el acceso también de derechos
25 de acceso. En este caso, puede ser deseable, además, para una persona un derecho de acceso específico con respecto a su papel. No obstante, también puede ser deseable un acceso limitado en el espacio en el edificio a determinadas partes o espacios del edificio.

30 Actualmente se asignan y se gestionan los derechos de acceso, en general, para las instalaciones o componentes individuales. En general, en este caso se realiza un acceso autorizado. En general en este caso se realiza un acceso de un usuario autorizado a través de las interfaces acondicionadas por el operador del edificio con los sistemas o instalaciones respectivos.

35 El documento US 2002 099945 A1 publica un sistema para el control de acceso de puertas y la gestión de llaves. En este caso se asocia a cada puerta de la caja un componente de bloqueo / control de puerta. Tales componentes están conectados entre sí para la comunicación a través de una red de comunicación. Un sistema de gestión de llaves sirve para registrar un código de identificación, que está previsto como una llave para un único usuario. El componente de bloqueo / control de puerta sirve para leer y verificar la llave del usuario, para determinar si esta llave
40 tiene autorización de acceso para una puerta de caja y activa esta puerta en virtud de esta autorización de acceso. En este caso, con la ayuda de una identidad se garantiza al usuario, sin embargo, sólo derechos de acceso a diferentes puertas de un complejo de edificios.

45 La invención tiene ahora el cometido de posibilitar un servicio central para la liberación de un acceso de datos a una o varios edificios.

El cometido se soluciona por medio de un sistema para la gestión de derechos de acceso de usuarios a datos operativos y/o datos de control de edificios o de complejos de edificios, en el que el sistema presenta lo siguiente: un primer servidor para un servicio de autorización de edificios con al menos una base de datos de autorización para el
50 registro de derechos de acceso específicos de los usuarios para determinados edificios o complejos de edificios, un segundo servidor para un servicio de liberación de la comunicación con una base de datos de autorización para el registro de usuarios registrados en el sistema, en el que la base de datos de autorización presenta una lista de todos los usuarios dotados con derechos de acceso específicos de los usuarios, en el que en la lista están depositados para cada usuario dotado con derechos de acceso aquellos edificios o complejos de edificios, para los que el usuario dispone de derechos de usuario, en el que el servicio de liberación de la comunicación está previsto para la liberación de una comunicación de un usuario con los edificios o complejos de edificios depositados para él en la lista y en el que el servicio de autorización de edificios está previsto para la liberación de los derechos de acceso
55 específicos para el usuario a datos operativos y/o de control del edificio o del complejo de edificios sobre la base de los derechos de acceso depositados en la base de datos de autorización.

60 El cometido se soluciona, además, por medio de un procedimiento para el funcionamiento de un sistema para la gestión de un derechos acceso a datos operativos y/o datos de control de edificios o de complejos de edificios, en el que un servicio de liberación de la comunicación que se ejecuta en un primer servidor libera una comunicación de un usuario anunciado con una identidad con los edificios o complejos de edificios depositados para él en una lista,

cuando su identidad coincide con una identidad depositada en la lista y un servicio de autorización de edificios, que se ejecuta en un segundo servidor después de realizar la liberación de la comunicación, concede derechos de acceso específicos para el usuario a datos operativos y/o de control del edificio o del complejo de edificios sobre la base de datos depositados en una base de datos de autenticación.

5 La invención se basa en el reconocimiento de que es ventajoso posibilitar derechos de acceso a datos específicos de los edificios a través de un sistema, en el que la autenticación de un usuario, que quiere tener acceso a los datos, se realiza de forma separada de los derechos de acceso específicos registrados para el usuario correspondiente. La autenticación de un usuario registrado se puede realizar de esta manera de forma sencilla a través de una aplicación, por ejemplo una aplicación de la Web, que es proporcionada por un prestador de servicios. 10 En este caso, el servicio que regula la autenticación del usuario necesita informaciones especiales, a cuyos datos específicos o bien fuentes de datos tiene acceso el usuario. De la misma manera, no se necesita ninguna información sobre el papel especial que cumple el usuario en el sistema. El servicio de autenticación sólo tiene que determinar si el usuario está registrado, en general, y está autorizado para el acceso, es decir, la comunicación con determinados edificios o complejos de edificios. El operador del sistema no tiene que disponer, por lo tanto, de datos 15 confidenciales.

Los datos confidenciales pueden ser gestionados más bien directamente en la gestión del edificio. A tal fin, los usuarios registrados en el sistema están depositados con su identidad y también su papel, es decir, la función que 20 pueden ejercer y lo que podrían hacer con los datos liberados para la comunicación. De la misma manera se registra hasta que extensión disponen de los derechos de acceso. Por lo tanto, e, tratamiento específico de los datos se puede realizar propiamente en el lugar por la gestión de edificios. No obstante, un anuncio de un usuario del sistema se puede realizar también en el puesto central a través del servicio de autorización para los edificios respectivos registrados en el sistema.

25 De esta manera se puede posibilitar de una forma sencilla también el acceso de usuarios a los más diferentes edificios o complejos de edificios, que son gestionados en el sistema. Por lo tanto, el usuario a través de su identidad única, con la que está depositado en el sistema, tiene la posibilidad de acceder a diferentes edificios de diferentes propietarios y allí llamar los datos operativos o bien también realizar intervenciones como una actualización de los datos. El sistema es ventajoso especialmente para trabajos de servicio, porque, por ejemplo, un técnico de servicio 30 obtiene a través de un único anuncio en el sistema un acceso a datos de diagnóstico de los más diferentes edificios o complejos de edificios. De esta manera, un técnico de servicio puede consultar, por ejemplo, antes de su visita al lugar a través de una única aplicación el estado de determinados componentes del sistema en los diferentes edificios y tomar en el campo previo ya las medidas necesarias o bien encargar las piezas de repuesto necesarias. 35 En general, el sistema posibilita un acceso sencillo y unitario a los datos específicos de los edificios y una gestión sencilla de los derechos de acceso necesarios para varios edificios o complejos de edificios.

Una configuración ventajosa de la invención consiste en que el servicio de liberación de la comunicación se ejecuta en un servidor central y está previsto para la liberación de la comunicación de usuarios registrados para varios 40 edificios o complejos de edificios, disponiendo cada edificio o cada complejo de edificios de un servidor descentralizado propio para el servicio de autorización de edificios y estando prevista una conexión de comunicación entre el servidor central y el servidor descentralizado. Si un usuario del sistema se anuncia con su identidad en el servicio de liberación de la comunicación en el servidor central, entonces aquí sólo debe verificarse si existen, en general, derechos de acceso a uno o varios edificios o complejos de edificios. Si éste es el caso, entonces se emite 45 desde el servidor central un mensaje al servidor descentralizado, que dispone de los derechos de acceso específicos del usuario. Para que se pueda liberar para el usuario la comunicación con el edificio y si el usuario está registrado para varios edificios o complejos de edificios, se puede liberar la comunicación también para varios edificios o complejos de edificios. En el servidor central o en el servidor descentralizado solamente se determina entonces qué derecho de acceso especial existe para el usuario anunciado y liberado para la comunicación y 50 entonces se le liberan estos datos para la comunicación.

Otra configuración ventajosa consiste en que el servicio de liberación de la comunicación dispone de al menos una interfaz de datos para la recepción de identidades de los usuarios registrados en una base de datos de autorización de un servicio de autorización de edificios con derechos de acceso específicos de los usuarios. Esto es 55 especialmente favorable, puesto que los usuarios son depositados con sus derechos de acceso específicos de los usuarios en el servidor descentralizado o bien en la base de datos de autorización del servidor descentralizado. En este caso, los usuarios son depositados con su identidad, su papel y la extensión de datos, a los que pueden acceder. Después de realizar el registro de un usuario con sus derechos de acceso específicos del usuario se puede recibir ahora la identidad del usuario a través de la interfaz de datos del servicio de liberación de la comunicación desde el servicio de liberación de la comunicación, y se pueden registrar en la lista, en la que están depositadas las 60 identidades de los usuarios con derechos de acceso. De esta manera se asegura que la identidad del usuario registrada en el servicio de liberación de la comunicación sea idéntica con la identidad del usuario, que está registrada en la base de datos de autorización del edificio o del complejo de edificios para el usuario. Una identidad predeterminada una vez por el servicio de autorización del edificio es utilizada, por lo tanto, por el servicio de

liberación de la comunicación para la autenticación. La interfaz de datos puede estar configurada en este caso de tal manera que se puede recibir directamente un mensaje emitido por el servidor descentralizado con la identidad del usuario y el reconocimiento del edificio, por ejemplo a través de Internet. También es concebible que la interfaz de datos esté configurada de tal forma que, por ejemplo, se realiza una comunicación con un teléfono móvil, de manera que el teléfono móvil transmite su identidad y esta identidad se deposita al mismo tiempo como identidad del usuario en el sistema tanto en la base de datos de autorización como también en la base de datos de autenticación. El servicio de liberación de la comunicación puede disponer, naturalmente, de varias interfaces, que posibilitan la recepción de identidades emitidas de diferentes medios de comunicación. En general, se registran en la lista todas las identidades recibidas a través de las interfaces de este tipo.

Otra configuración ventajosa consiste en que el servicio de liberación de la comunicación presenta una superficie de usuario para el anuncio a través de un usuario por medio una identidad. El usuario solamente tiene que utilizar aquí una identidad que le ha sido asignada por el servicio de autorización del edificio o bien que corresponde a la identidad de su teléfono móvil. El anuncio se realiza de una manera más ventajosa de forma centralizada a través de una aplicación, que es preparada por el servicio de liberación de la comunicación. De esta manera, el usuario siempre tiene el mismo "aspecto y tacto" y es posible una interacción sencilla con el sistema.

Otra configuración ventajosa consiste en que la superficie de usuario está prevista para la preparación de un entorno de usuario adaptado a los derechos de acceso específicos de usuario. Si se posibilita una vez una comunicación desde el servicio de liberación de la comunicación, entonces el servidor descentralizado o bien el servicio de autorización del edificio emite una información, en la que se indica qué entornos específicos del usuario proporcionados en el sistema son más adecuados para el manejo del sistema. Por ejemplo, en función del papel de un usuario se puede preparar una superficie, sobre la que se pueden leer sólo datos a través del usuario. La superficie puede ser estática, de manera que el usuario no tiene ninguna posibilidad de obtener otros conocimientos que los que son preparados por la gestión del edificio. No obstante, la superficie de usuario puede estar configurada también dinámicamente y puede posibilitar una interacción del usuario, de manera que puede navegar en diferentes jerarquías de la estructura de datos operativos. Además, la superficie de usuario puede estar configurada de tal manera que se posibilita al usuario una manipulación, o bien una intervención en los datos. Por ejemplo, es concebible que el usuario pueda modificar datos umbrales a través del sistema, pero también es concebible que el usuario pueda cargar software de actualizaciones. En este caso es ventajoso que el entorno de usuario específico del usuario sea preparado sólo cuando se ha liberación la comunicación para el usuario y se conoce en el sistema qué superficie de usuario es la superficie de usuario que se adapta para sus derechos de acceso.

Las diferentes superficies de usuarios propiamente dichas son preparadas exclusivamente por el servicio de liberación de la comunicación y sólo son registradas también allí. Desde el servicio de autorización del edificio sólo debe anunciarse qué superficie de usuario es adecuada para el papel o bien para el entorno, que el usuario solicita. Por lo tanto, el servicio de liberación de la comunicación no tiene que disponer tampoco, para la preparación de la superficie de usuario específica del usuario, de los datos confidenciales de los usuarios individuales. También a tal fin es suficiente solamente la identidad y la transmisión siguiente de la superficie preferida de usuario a través del servicio de autorización del edificio. De esta manera, también es posible una manipulación sencilla de la superficie de usuario a través del operador del servicio. Las superficies de usuario pueden ser configuradas y también pueden ser modificadas de forma centralizada.

Otra configuración ventajosa consiste en que la superficie de usuario está prevista ya, en el caso de anuncio a través de un usuario, para la preparación de una selección de papeles específicos de los usuarios. De esta manera, el usuario puede limitar igualmente cuál de las diferentes aplicaciones es útil o necesaria para él para la comunicación con los datos específicos de los usuarios. También se puede seleccionar ya en la superficie de usuario si éste necesita acceso a datos de control, si quiere modificar algo, por ejemplo, en una configuración de ascensor, si solamente quiere ser informado sobre el rendimiento del sistema por medio de una Score-Card (cuadro de mando integrado), en la que se registran las métricas. También puede indicar alternativamente si quiere realizar un mantenimiento remoto. En todas estas aplicaciones específicas, se proporcionan al usuario solamente datos que corresponden a su papel momentáneo seleccionado. Esto es especialmente ventajoso para un usuario, que dispone de derechos amplios y, por lo tanto, no tiene un papel específico en el sistema, de manera que sólo en virtud de su papel se le puede proporcionar por el sistema una superficie específica de usuario. El usuario pasa en este caso por sí mismo al papel correspondiente, de manera que los datos preparados son adaptados de manera correspondiente al papel seleccionado por él.

A continuación se describe y se explica en detalle la invención con la ayuda de la figura.

La figura 1 muestra una representación esquemática del sistema para la gestión de derechos de acceso.

El sistema 1 para la gestión de derechos de acceso a datos operativos y/o de control de edificios o de complejos de edificios 5 está constituido por un primer servidor 2, en el que se ejecuta un servicio de autorización de edificios. El servidor 2 dispone de una o varias bases de datos de autorización 20. En la o bien en las bases de datos de

autorización 20 se registran derechos de acceso específicos de los usuarios para determinados edificios o complejos de edificios 5. En este caso, por ejemplo, se deposita una identidad para un usuario 10 del sistema 1. Junto a la identidad del usuario 10 se deposita, además, qué papel tiene el usuario 10. Por ejemplo, el papel puede estar limitado y el usuario sólo tiene derechos para leer datos, que son generados o que están presentes en diferentes componentes del edificio o del complejo de edificios 5. No obstante, el papel puede consistir también en que el usuario puede manipular datos del complejo de edificios 5. Además, del papel, en la base de datos de autorización 20 se puede añadir a la identidad del usuario, además una entrada, en la que se define el alcance espacial de sus derechos de acceso. Por ejemplo, un usuario puede tener derechos de acceso sólo a determinados edificios de un complejo de edificios o dentro de un complejo de edificios puede tener derechos de acceso sólo a determinados componentes del sistema, por ejemplo exclusivamente a ascensores o exclusivamente a la automatización del edificio o exclusivamente a la instalación de calefacción.

El sistema 1 dispone, además, de un segundo servidor 3, en el que se ejecuta un servicio de liberación de la comunicación. El segundo servidor 3 presenta una base de datos de autenticación 30. En esta base de datos están depositados en una lista 4 todos los usuarios registrados en el sistema 1 con su identidad 4.1. A cada identidad de un usuario se añade en la lista 4, además, a qué edificios o complejos de edificios 5 puede acceder el usuario por medio de una comunicación a través de la conexión de comunicación 23. El segundo servidor 3 puede ser accionado en este caso de forma centralizada por un prestador de servicios, mientras que los primeros servidores 2 están dispuestos de forma descentralizada en el sistema 1. Los primeros servidores 2 pueden estar en este caso en lugares opcionales, seleccionados por un cliente del sistema. No obstante, los primeros servidores pueden estar alojados también directamente en los edificios o complejos de edificios.

Un usuario 10 puede acceder a través de la interfaz de usuario o bien la superficie de usuario 7, que está dispuesta sobre el segundo servidor 3 y que es preparada por el servicio de liberación de la comunicación, a los datos operativos o bien los datos de control de los edificios o de los complejos de edificios. A tal fin, el usuario 10 se anuncia en la superficie de usuario 7 con su identidad, que tiene en el sistema. El servicio de liberación de la comunicación verifica si la identidad coincide con una identidad depositada en la lista 4. Si éste es el caso, entonces se determina a partir de la columna 4.2 de la lista para qué edificios o complejos de edificios 5 el usuario tiene derechos de acceso. A continuación se libera para el usuario la comunicación con el edificio o bien o bien el complejo de edificios o bien con varios edificios o bien complejos de edificios depositados en la columna 4.2. A través de la conexión de comunicación 23 el usuario puede acceder ahora a los datos del edificio o del complejo de edificios. No obstante, en el lugar sólo se le conceden los derechos de acceso que están depositados en el primer servidor 2 en la base de datos de autorización. La posibilidad de comunicación básica se posibilita al usuario 10, por lo tanto, a través del servicio de autenticación con la ayuda de las informaciones depositadas en la base de datos de autenticación; el acceso especial a datos se concede al usuario 10 entonces con la ayuda del servicio de autorización del edificio en virtud de las informaciones depositadas en la base de datos de autorización 20. De esta manera se consigue una separación de la autenticación y de la autorización. A través de un servicio unitario, el servicio de autenticación se posibilita el acceso a diferentes edificios o complejos de edificios, sin que este servicio de autenticación disponga de datos confidenciales. Los papeles y los derechos de acceso específicos de los usuarios solamente están depositados en el primer servidor 2 en el servicio de autorización del edificio.

El registro de un usuario nuevo para el acceso a un edificio o complejo de edificios 5 se puede realizar de diferentes maneras. El usuario 10 puede anunciarse, por ejemplo, en el servicio de autenticación a través de la superficie de usuario 7. No obstante, debe ser autorizado por la gestión del edificio, al que quiere tener acceso, para que el servicio de autenticación le libere para la comunicación a través de la conexión de comunicación 23. A tal fin, se asigna al usuario por la gestión del edificio una identidad, que corresponde a aquélla, con la que se ha anunciado en el servicio de autenticación. A esta identidad se asigna por la gestión del edificio un papel y el alcance. Los datos son depositados en el primer servidor 2 en la base de datos de autorización 20. Si el usuario 10 está registrado por la gestión del edificio y está depositado en la base de datos 20, entonces se emite por el servicio de autorización del edificio un mensaje al servicio de autenticación. El servicio de autenticación introduce la identidad del usuario en la lista 4 en la base de datos de autenticación 30. En la columna 4.2, el servicio de autenticación introduce la identificación del edificio o bien del complejo de edificios 5, desde el que se emite el mensaje. El usuario 10 está depositado ahora en el sistema 1 con su identidad y los edificios, a los que puede tener acceso.

Para la comunicación entre el primer servidor 2 y el segundo servidor 3 se puede utilizar cualquier comunicación estándar discrecional. Por ejemplo, es posible una comunicación a través de Internet, pero también es concebible que se realice la comunicación a través de una línea de telecomunicaciones o una línea fija. La comunicación se puede realizar en este caso por cables o también a través de radio.

El registro de un usuario 10 se puede realizar también a través de un aparato, que tiene una identidad y que es apto para la comunicación, es decir, para la emisión y la recepción de datos. En este caso, se puede tratar, por ejemplo, de un teléfono móvil un i-phone p i-pad. En este caso, a través del usuario 10 se puede realizar con la ayuda del aparato de comunicación 8 un registro en el primer servidor 2. El aparato de comunicación emite en este caso su identidad al primer servidor 2 a través de la conexión de comunicación 8.1. Esto se realiza junto con una consulta del

5 usuario de si se le conceden derechos de acceso. Desde la gestión de edificios se depositan ahora, como en el caso ya descrito, la identidad del usuario, en este caso la identidad de su aparato de comunicación y el papel asignado a esta identidad y su alcance. El registro se realiza en la base de datos de la autorización 20. El servicio de autorización del edificio transmite al aparato de comunicación 8 a continuación a través de la conexión de comunicación 8.1 un mensaje codificado, en el que está depositada la identidad. Además de la identidad, se indica en el mensaje codificado desde qué edificio procede este mensaje, es decir, que está depositada la identificación del edificio, que posibilita junto con la identidad a través del servicio de autenticación un acceso al edificio respectivo o bien al complejo de edificios 5. El aparato de comunicación 8 transmite ahora el mensaje codificado a una interfaz de datos 6 del servicio de autenticación que se ejecuta en el segundo servidor 3. En este caso, se utiliza otra conexión de comunicación. El servicio de autenticación envía al aparato de comunicación 8 después de la recepción del mensaje codificado una confirmación de que el mensaje ha llegado. La información codificada es descodificada por el servicio de autenticación y la identidad del usuario 10 depositada en ella se deposita junto con la identificación del edificio, para el que se ha permitido registrar, en la lista 4 en la base de datos de autenticación. En el mensaje codificado se puede tratar, por ejemplo, de un código de barras bidimensional, que se puede recibir y también emitir por el aparato móvil. No obstante, también son concebibles otras posibilidades de la codificación de mensajes. Si el usuario 10 está depositado ahora en el servicio de autenticación en la base de datos de autenticación, entonces puede realizar a través de la superficie de usuario 7 por medio del aparato móvil, cuya identidad está ahora en el sistema, un anuncio en el sistema 1 y en caso de coincidencia de la identidad depositada en la lista 4 del aparato móvil con la identidad en el anuncio, se posibilita al usuario a través de la conexión de comunicación 23 la comunicación con el edificio o bien con el complejo de edificios 5.

25 La superficie de usuario 7 puede estar configurada de múltiples maneras. Por ejemplo, la superficie de usuario puede disponer de diferentes aplicaciones, a través de las cuales el usuario puede seleccionar ya durante el anuncio en el sistema 1 un papel específico del usuario y se le proporciona a continuación una superficie específica del usuario, que está adaptada de una manera óptima a sus necesidades. Por ejemplo, a alguien que no debe realizar ninguna manipulación, sino que solamente debe leer datos, se le proporciona una superficie, que no presenta posibilidades de entrada. Si alguien debe manipular datos, por ejemplo ajustar valores umbrales, entonces se le proporcionan superficies de usuario, a través de las cuales puede realizar una entrada de datos correspondiente. Los datos modificados son transmitidos entonces a través de la conexión de comunicación 23 al edificio o bien al complejo de edificios y allí de acuerdo con los derechos de acceso del usuario se realiza la modificación de los datos en los diferentes componentes, que están instalados en el edificio. En este caso, se puede preparar al usuario por el servicio de autorización una superficie de mando y de observación muy específica. En este caso, se dan al usuario también todas las posibilidades habituales de la visualización o bien del acceso. De esta manera, un usuario se puede conectar a través de Internet, a través de VPN, a través de Facebook, a través de Twitter o a través de una conexión de telecomunicación normal con el servicio de autenticación o bien con la superficie del servicio de autenticación y a través de la superficie, que se indica entonces en su entorno respectivo, se puede comunicar con el edificio o bien con el complejo de edificios.

40

REIVINDICACIONES

1.- Sistema (1) para la gestión de derechos de acceso de usuarios a datos operativos y/o datos de control de edificios o de complejos de edificios (5), en el que el sistema (1) presenta:

- un primer servidor (2) para un servicio de autorización de edificios con al menos una base de datos de autorización (20) para el registro de derechos de acceso específicos de los usuarios para determinados edificios o complejos de edificios (5),
- un segundo servidor (3) para un servicio de liberación de la comunicación con una base de datos de autorización (30) para el registro de usuarios registrados en el sistema (1), en el que la base de datos de autorización(30) presenta una lista (4) de todos los usuarios dotados con derechos de acceso específicos de los usuarios,

o en el que en la lista (4) están depositados para cada usuario dotado con derechos de acceso aquellos edificios o complejos de edificios (5), para los que el usuario dispone de derechos de usuario, en el que el servicio de liberación de la comunicación está previsto para la liberación de una comunicación de un usuario con los edificios o complejos de edificios (5) depositados para él en la lista (4) y en el que el servicio de autorización de edificios está previsto para la liberación de los derechos de acceso específicos para el usuario a datos operativos y/o de control del edificio o del complejo de edificios (5) sobre la base de los derechos de acceso depositados en la base de datos de autorización (20), **caracterizado** porque los derechos de acceso específicos para un usuario se definen a través de su identidad y de un papel asignado a su identidad, y el usuario puede acceder de acuerdo con su papel leyendo o manipulando a datos de componentes del edificio o del complejo de edificios.

2.- Sistema de acuerdo con la reivindicación 1, en el que

- el servicio de liberación de la comunicación se ejecuta en un servidor central (3) y está previsto para la liberación de la comunicación de usuarios registrados para varios edificios o complejos de edificios (5),
- cada edificio o cada complejo de edificios (5) dispone de un servidor (2) descentralizado propio para el servicio de autorización de edificios y
- entre el servidor central (3) y cada servidor descentralizado (2) está prevista una conexión de comunicación (23).

3.- Sistema de acuerdo con la reivindicación 1 ó 2, en el que el servicio de liberación de la comunicación dispone de al menos una interfaz de datos (6) para la recepción de identidades de los usuarios registrados en una base de datos de autorización (20) de un servicio de autorización de edificios con derechos de acceso específicos de los usuarios.

4.- Sistema de acuerdo con una de las reivindicaciones anteriores, en el que el servicio de liberación de la comunicación presenta una interfaz de usuario (7) para el anuncio a través de un usuario por medio de la identidad.

5.- Sistema de acuerdo con la reivindicación 4, en el que la interfaz de usuario (7) está prevista para la preparación de un entorno de usuario adaptado a los derechos de acceso específicos del usuario.

6.- Sistema de acuerdo con la reivindicación 4 ó 5, en el que la superficie de usuario (7) está prevista durante el anuncio a través de un usuario ya para la preparación de una selección de papeles específicos de los usuarios.

7.- Procedimiento para el funcionamiento de un sistema para la gestión de un derechos acceso de usuarios a datos operativos y/o datos de control de edificios o de complejos de edificios de acuerdo con una de las reivindicaciones 1 a 6, en el que

- un servicio de liberación de la comunicación que se ejecuta en un primer servidor (3) libera una comunicación de un usuario anunciado con una identidad con los edificios o complejos de edificios (5) depositados para él en una lista (4), cuando su identidad coincide con una identidad depositada en la lista (4) y
- un servicio de autorización de edificios, que se ejecuta en un segundo servidor (2) después de realizar la liberación de la comunicación, concede derechos de acceso específicos para el usuario a datos operativos y/o de control del edificio o del complejo de edificios (5) sobre la base de datos depositados en una base de datos de autenticación (20),

caracterizado porque los derechos de acceso específicos para el usuario son definidos a través de su identidad y de un papel asociado a su identidad, y el usuario puede acceder leyendo o manipulando de acuerdo con su papel a datos de componentes del edificio o de complejos de edificios.

8.- Procedimiento de acuerdo con la reivindicación 7, en el que

- desde el servicio de liberación de la comunicación, que se ejecuta en un servidor central (3), se libera la comunicación de usuarios para varios edificios o complejos de edificios (5),
- a través de la conexión de comunicación (23) se transmite desde el servidor central (2) un mensaje sobre la liberación de la comunicación a un servidor descentralizado (2) del edificio o del complejo de edificios, en el que se ejecuta el servicio de autorización de edificios.

5

9.- Procedimiento de acuerdo con la reivindicación 7 u 8, en el que a través de una superficie de usuario (7) del servicio de liberación de la comunicación se prepara por medio de una identidad del usuario anunciado después de realizar la liberación de la comunicación un entorno del usuario adaptado a los derechos de acceso específicos del usuario.

10

10.- Procedimiento de acuerdo con la reivindicación 7 u 8, en el que a través de una interfaz de usuario (7) del servicio de liberación de la comunicación por medio de una identidad del usuario se prepara una selección de papeles específicos del usuario.

15

11.- Procedimiento de acuerdo con una de las reivindicaciones 7 a 10, en el que para el registro de un usuario nuevo

- se conceden derechos de acceso específicos de los usuarios para determinados edificios o complejos de edificios (5) a través del servicio de autorización de edificios,
- se registran los derechos de acceso específicos del usuario en al menos una base de datos de autorización (20), depositando para cada usuario dotado con derechos de acceso una identidad, un papel y un alcance de los derechos de acceso,
- las identidades de los usuarios, a los que se han concedido derechos de acceso específicos de los usuarios, son transmitidas a través de la interfaz de datos (6) al servicio de liberación de la comunicación, las identidades se depositan en la lista (4) de la base de datos de autenticación (30) del servicio de liberación de la comunicación junto con una identificación para el edificio determinado o el complejo de edificios (5), para el que o para los que los usuarios tienen derechos de acceso.

20

25

