(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 819 098**

(51) Int. CI.:

G06F 21/31 (2013.01)
G06F 21/34 (2013.01)
G06F 21/35 (2013.01)
G06F 21/57 (2013.01)
G06F 21/62 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **26.10.2018 E 18202756 (5)**

(97) Fecha y número de publicación de la concesión europea: **22.07.2020 EP 3477517**

(54) Título: **Procedimiento de control de acceso a una zona segura de un equipo, programa de ordenador, soporte informático y equipo asociados**

(30) Prioridad:

27.10.2017 FR 1760159

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.04.2021

(73) Titular/es:

ALSTOM TRANSPORT TECHNOLOGIES (100.0%)
48, rue Albert Dhalenne
93400 Saint-Ouen, FR

(72) Inventor/es:

DEGENEVE, XAVIER y
FOUQUES, BAPTISTE

(74) Agente/Representante:

ELZABURU, S.L.P

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).

DESCRIPCIÓN

Procedimiento de control de acceso a una zona segura de un equipo, programa de ordenador, soporte informático y equipo asociados

La presente invención concierne a un procedimiento de control de acceso a una zona segura de un equipo electrónico.

La invención concierne igualmente a un programa de ordenador y a un soporte informático asociados.

La invención concierne además a un equipo electrónico asociado.

En el ámbito ferroviario, es conocido equipar equipos electrónicos, integrados en vehículos ferroviarios o instalados en el suelo a lo largo de una línea ferroviaria, con una interfaz de usuario que permita especialmente la actualización o la configuración de tales equipos.

Para evitar que usuarios no habilitados tomen el control de tales equipos, se han establecido procedimientos de control de acceso. En particular, se conoce un procedimiento de control de acceso, en el cual cada equipo comprende un identificador común para varios usuarios y un autenticador, tal como una contraseña, asociado al identificador común. Para tener acceso a una zona segura del equipo, el usuario comunica al equipo, el identificador común y el autenticador asociado.

Sin embargo, tal procedimiento no permite adaptar, y especialmente restringir, los derechos de acceso asociados a una configuración para usuarios específicos. Además, tal procedimiento no está adaptado para dar derechos de acceso temporales a un usuario, lo que plantea problemas de seguridad. Para que un usuario no pueda acceder al equipo, conviene modificar el identificador y el autenticador memorizados en el equipo, lo que es obligatorio para poner en práctica.

Se conoce igualmente un procedimiento de control de acceso en el cual los datos de autenticación de los usuarios habilitados son memorizados en un servidor central conectado a los equipos. Cualquier persona que desee conectarse al equipo comunica al citado equipo su identificador y su autenticador. El equipo comunica entonces estos datos al servidor central, el cual envía en retorno una autorización o una prohibición de acceso al equipo.

Sin embargo, tal procedimiento requiere un servidor central y por tanto no está adaptado para los equipos aislados o situados en zonas sin red, lo que es el caso en la mayoría de los equipos ferroviarios.

Se conoce también por el documento WO 2009/034018 A un procedimiento de acceso por un usuario a un dispositivo de control industrial. El acceso es controlado por medio de una memoria móvil o medios de almacenamiento de tiques de acceso.

Existe por tanto una necesidad de un procedimiento de control de acceso a equipos aislados o situados en zonas sin red que sea adaptable y simple de poner en práctica al tiempo que confiera un buen nivel de seguridad.

A tal efecto, la invención tiene por objeto un procedimiento de control de acceso a una zona segura de un equipo electrónico a partir de un archivo informático, comprendiendo el equipo electrónico una memoria que comprende al menos una zona segura, siendo el archivo informático específico de un usuario y estando memorizado en un soporte informático, comprendiendo el archivo informático un autenticador de referencia y un derecho de acceso al equipo electrónico para al menos una zona segura correspondiente, comprendiendo la memoria al menos un derecho de acceso de referencia al equipo electrónico, siendo puesto en práctica el procedimiento por el equipo electrónico y compendiando:

- la adquisición del autenticador de referencia a través del archivo informático a continuación de una conexión del soporte informático al equipo electrónico,

- la adquisición de un autenticador proveniente del usuario,

- la autenticación del usuario por comparación del autenticador proveniente del usuario con el autenticador de referencia,

- la adquisición del derecho de acceso a través del archivo informático cuando al final de la autenticación, el autenticador proveniente del usuario es conforme con el autenticador de referencia, y

- la apertura de una sesión de acceso a la citada al menos una zona segura correspondiente, cuando el derecho de acceso adquirido corresponde al derecho de acceso de referencia comprendido en la memoria.

Según otros aspectos ventajosos de la invención, el procedimiento de control de acceso comprende una o varias de las características siguientes, tomadas aisladamente o según todas las combinaciones técnicamente posibles:

- el archivo informático está firmado con una clave de firma, estando la clave de firma asociada a un certificado de una autoridad de certificación, estando memorizado en la memoria el certificado de la autoridad de certificación asociado

a la clave de firma, comprendiendo el procedimiento además, previamente a la adquisición del derecho de acceso, la verificación de la firma del archivo informático con el certificado de la autoridad de certificación memorizado en la memoria.

- el soporte informático es un soporte físico desmontable, tal como un soporte de memoria FLASH, por ejemplo una llave USB.

- el soporte informático es un soporte desmaterializado, tal como un archivo informático memorizado en un servidor de red.

- el archivo informático comprende una fecha de validez, comprendiendo el equipo electrónico un reloj, y en el cual la apertura de la sesión de acceso comprende además la comparación de la citada fecha de validez con una fecha corriente facilitada por el reloj, siendo abierta la sesión únicamente cuando la fecha de validez es posterior a la citada fecha corriente.

- el archivo informático comprende al menos una configuración que tiene como objetivo modificar el equipo, comprendiendo el procedimiento la ejecución de la configuración en el equipo electrónico después de la apertura de la sesión.

La invención concierne igualmente a un programa de ordenador que comprende instrucciones informáticas, las cuales cuando son ejecutadas por un ordenador ponen en práctica un procedimiento de control de acceso tal como el definido anteriormente.

Según otro aspecto ventajoso de la invención, el equipo tal como se describió anteriormente es un equipo ferroviario configurado para ser integrado a bordo de un vehículo ferroviario, tal como un motor, un sistema de visualización, un sistema de climatización, un equipo de red, un equipo de seguridad, un equipo de señalización o un equipo de control ferroviario, o bien para ser instalado en el suelo a lo largo de una línea ferroviaria, tal como una semáforo, un cambio de vías o un paso a nivel.

La invención tiene igualmente por objeto un procedimiento de control de acceso según la reivindicación 1.

Según otros aspectos ventajosos de la invención, el procedimiento de control de acceso comprende una o varias de las características de las reivindicaciones 2 a 7, tomadas aisladamente o según todas las combinaciones técnicamente posibles.

La invención concierne también a un equipo electrónico según la reivindicación 8.

Según otro aspecto ventajoso de la invención, el equipo presenta también las características de la reivindicación 9.

Otras características y ventajas de la invención se pondrán de manifiesto en la lectura de la descripción que sigue, dada únicamente a modo de ejemplo no limitativo, y hecha en referencia a los dibujos anejos, en los cuales:

- la figura 1 es una representación esquemática de un equipo electrónico y de un soporte según la invención, y

- la figura 2 es un organigrama de un procedimiento de control puesto en práctica por el equipo electrónico de la figura 1.

En la figura 1 están ilustrados un soporte informático 10 y un equipo electrónico 12.

El soporte informático 10 está configurado para ser conectado al equipo electrónico 12.

En el ejemplo ilustrado en la figura 1, el soporte 10 es un soporte físico desmontable. Se entiende por el término « desmontable » que dicho soporte es apto para ser separado del equipo electrónico 12. En el ejemplo de la figura 1, el soporte 10 está destinado a ser poseído por un usuario del equipo electrónico 12. Preferentemente, el soporte 10 es apropiado para ser transportado sin esfuerzo por tal usuario. Ventajosamente, la masa del soporte 10 es inferior o igual a 500 gramos (g), preferentemente inferior o igual a 300 g, preferentemente todavía inferior o igual a 100 g.

Por ejemplo, el soporte 10 es un soporte de memoria FLASH, tal como una llave USB. En variante, el soporte 10 es un disquete o disco flexible (de la denominación inglesa floppy disk), un disco óptico, un CD-ROM, un DVD, un disco magneto-óptico, una memoria ROM, una memoria RAM, una memoria EPROM, una memoria EEPROM, una tarjeta magnética o una tarjeta óptica.

En variante, el soporte 10 es un soporte desmaterializado o virtual. Por ejemplo, el soporte 10 es un archivo informático memorizado en un servidor de red o en cualquier otro órgano informático o electrónico. En este caso, el equipo electrónico 12 está en interacción con el citado órgano informático o electrónico. En otro ejemplo, el soporte 10 es un archivo adjunto a un correo electrónico.

El soporte 10 comprende un archivo informático específico de un usuario. Por « específico », se entiende que el archivo contiene informaciones propias únicamente de un usuario dado. A cualquier otro usuario del equipo 12 se le atribuirá entonces otro archivo informático.

En complemento facultativo, el soporte 10 comprende varios archivos informáticos específicos de usuarios, eventualmente diferentes uno de otro.

Preferentemente, el archivo informático está firmado con una clave de firma, denominada también « clave privada ». La verificación de validez de la firma del archivo se hace entonces con una clave denominada « certificado de una autoridad de certificación » denominada también « clave pública » o una cadena de certificados asociada a una autoridad de certificación. Tal verificación permite garantizar la integridad y la autenticidad de los datos contenidos en el archivo informático. Se entiende por el término « autenticidad » que los datos provienen de una entidad debidamente autorizada para generar el archivo informático. Se entiende por el término « integridad » que los datos no están alterados o modificados.

Ventajosamente, los datos contenidos en el archivo informático están cifrados, y esto especialmente cuando tales datos son confidenciales.

El archivo informático comprende un autenticador de referencia y al menos un derecho de acceso al equipo electrónico 12 para al menos una zona segura correspondiente del citado equipo 12.

El derecho de acceso es, por ejemplo, una autorización de abrir una sesión que dé acceso a una zona segura del citado equipo 12. Dicha autorización es, por ejemplo, otorgada durante un tiempo determinado. Tal autorización permite, por ejemplo, la utilización de datos descritos en el archivo informático para modificar una configuración del equipo 12.

En otro ejemplo, el derecho de acceso es común para varios equipos 12, incluso para equipos 12 diferentes. Por ejemplo, el derecho de acceso autoriza el acceso a todos los sistemas de climatización de una red de vehículos ferroviarios. En variante, el derecho de acceso autoriza el acceso a los sistemas de climatización de solamente un vehículo ferroviario dado.

El autenticador de referencia es específico del usuario destinado a mantener o a tener acceso al soporte 10.

El autenticador de referencia es, por ejemplo un elemento de conocimiento secreto tal como una contraseña o un dato de identificación física, especialmente un dato biométrico, tal como una imagen de una huella digital del usuario o una imagen de un iris del usuario. En variante, el autenticador de referencia es un elemento físico en posesión del usuario, tal como una ficha física o una tarjeta inteligente.

Preferentemente, el archivo informático comprende una fecha de validez, más allá de la cual los datos contenidos en el archivo informático han expirado y por tanto ya no son válidos.

El equipo electrónico 12 es un equipo autónomo. Se entiende por el término « autónomo » que el equipo 12 no está conectado a un servidor, local o centralizado, para funcionar.

En variante, el equipo electrónico 12 es un equipo conectado a una red informática.

El equipo 12, es, por ejemplo, un equipo ferroviario configurado para ser integrado a bordo de un vehículo ferroviario, tal como un motor, un sistema de visualización, un sistema de climatización, un equipo de red, un equipo de seguridad, un equipo de señalización, un equipo de control ferroviario, o bien para ser instalado en el suelo a lo largo de una línea ferroviaria, al como un semáforo, un cambio de agujas o un paso a nivel.

El equipo 12 comprende una entrada 13, una memoria 14, un procesador 16 y una interfaz hombre-máquina 18. Como complemento facultativo, cuando el archivo informático comprende una fecha de validez, el equipo 12 comprende también un reloj, no representado, que visualiza una fecha corriente.

El equipo 12 comprende, además, diferentes módulos memorizados en la memoria 14 del equipo 12 y apropiados para ser ejecutados por el procesador 16 del equipo 12. En particular, en el ejemplo ilustrado en la figura 1, el equipo 12 comprende, un módulo de verificación de firma 24, un primer módulo de adquisición 26, un segundo módulo de adquisición 28, un módulo de autenticación 30, un tercer módulo de adquisición 32, un módulo de apertura 34 y un módulo de ejecución 36.

La entrada 13 está configurada para ser conectada al soporte 10 y para permitir la extracción de los datos contenidos en el archivo informático del soporte 10.

Por ejemplo, cuando el soporte 10 es una llave USB, la entrada 13 es un puerto USB. Cuando el soporte 10 es un CD o un DVD, la entrada 13 es un lector de CD y/o de DVD. Cuando el soporte 10 es un disco óptico, la entrada 13 es un lector de disco óptico. Cundo el soporte 10 es un disquete, la entrada 13 es un lector de disquete. Cuando el soporte 10 es un archivo informático memorizado en un servidor de red, la entrada 13 es una entrada de red, tal como un entrada Ethernet / IP, Wifi, Radiomóvil, GSM, 3G o incluso ITE.

La memoria 14 comprende una zona libre de acceso 40 y al menos una zona segura 42. La zona libre de acceso 40 es accesible a cualquier usuario del equipo 12 sin autenticación, ni autorización de acceso. La zona segura 42 es accesible solamente a datos autenticados y/o a acciones efectuadas por usuarios autorizados del equipo 12, es decir usuarios que hayan sido autenticados y hayan sido autorizados al acceso al equipo 12 según el procedimiento de control de acceso según la invención.

La memoria 14 comprende, además, un derecho de acceso de referencia al equipo electrónico 12. El derecho de acceso de referencia autoriza el acceso al menos a una zona segura 42 del equipo 12.

Además, cuando el archivo informático del soporte 10 está firmado, la memoria 14 comprende el certificado de la autoridad de certificación.

Cuando el archivo informático del soporte 10 está cifrado, la memoria 14 comprende una clave de descifrado del archivo informático.

En variante, al menos una parte de la memoria 14 está comprendida en un servidor conectado al equipo electrónico 12.

La interfaz hombre-máquina 18 es, por ejemplo, un teclado, una pantalla, un ratón, una interfaz distante de red (terminal de red, página web) o incluso un micrófono.

El módulo de verificación de firma 24 es apropiado para verificar la firma del archivo informático con el certificado de la autoridad de certificación.

El primer módulo de adquisición 26 es apropiado para adquirir un autenticador de referencia a través del archivo informático, después de una conexión del equipo 12 al archivo informático. El autenticador de referencia adquirido es el autenticador de referencia memorizado en el archivo informático del soporte 10.

El segundo módulo de adquisición 28 es apropiado para adquirir un autenticador introducido por el usuario a través de la interfaz hombre-máquina 18.

El módulo de autenticación 30 es apropiado para autenticar al usuario por comparación del autenticador introducido con el autenticador de referencia.

Cuando el autenticador introducido es válido con respecto al autenticador de referencia, el usuario queda autenticado. Cuando el autenticador introducido no es válido, el usuario no queda autenticado.

El tercer módulo de autenticación 32 es apropiado para adquirir un derecho de acceso a través del archivo informático, y esto solamente cuando el módulo de autenticación 30 haya autenticado al usuario.

Como complemento facultativo, el tercer módulo de adquisición 32 es apropiado para adquirir varios o el conjunto de los derechos de acceso del archivo informático cuando el módulo de autenticación 30 ha autenticado al usuario.

Como complemento facultativo todavía, cuando el archivo informático comprende una fecha de validez, el cuarto módulo de adquisición 33 es apropiado para adquirir la fecha de validez del archivo informático.

El módulo de apertura 34 es apropiado para abrir una sesión de acceso a la citada al menos una zona segura 42 correspondiente, cuando el derecho de acceso adquirido corresponde al derecho de acceso de referencia comprendido en la memoria 14 y, en su caso según el complemento facultativo antes citado, cuando la fecha de validez adquirida es posterior a la fecha facilitada por el reloj del equipo 12.

La sesión de acceso es, por ejemplo, una sesión que autoriza el acceso a la zona segura 42 durante una duración determinada. La sesión de acceso es, por ejemplo, una sesión que autoriza la modificación de la configuración del equipo 12, por ejemplo, la modificación de un software integrado en el equipo 12.

Preferentemente, cuando el archivo informático comprende al menos una configuración que tiene por objetivo modificar el equipo 12, el módulo de ejecución 36 es apropiado para ejecutar, tras la apertura de una sesión por el módulo de apertura 34, al menos una configuración que tiene por objetivo modificar el equipo 12.

Las configuraciones son, por ejemplo, configuraciones que tienen por objetivo actualizar el equipo 12. En variante, las configuraciones son comportamientos ajustables del equipo 12, tales como, direcciones de red, la identificación de entradas y de salidas, características físicas de los elementos controlados por el equipo 12 y la ejecución de módulos aplicativos.

Se va a describir ahora un procedimiento de control de acceso en referencia a la figura 2. El procedimiento de control de acceso es puesto en práctica por el equipo electrónico 12 en interacción con el soporte informático 10.

Inicialmente, el equipo electrónico 12 es conectado al archivo informático del soporte 10. Cuando el soporte 10 es un soporte físico desmontable, dicha conexión es realizada por el usuario a través de la entrada 13. Cuando el soporte

10 es un soporte desmaterializado, tal como un archivo informático memorizado en un servidor de red o en cualquier otro órgano informático o electrónico, el equipo electrónico 12 se conecta al soporte 10 eventualmente a través de una conexión inalámbrica.

Cuando el archivo informático del soporte 10 está firmado, el procedimiento de control comprende una etapa 100 de verificación de la firma del archivo informático por el módulo de verificación de firma 24, con la ayuda del certificado de la autoridad de certificación memorizada en la memoria 14.

Después, durante una etapa 110, el primer módulo de adquisición 26 adquiere el autenticador de referencia comprendido en el archivo informático.

A continuación, durante una etapa 120, el usuario introduce o comunica un autenticador a través de la interfaz hombre-máquina 18. El autenticador introducido o comunicado por el usuario es adquirido entones por el segundo módulo de adquisición 28.

Durante una etapa 130 siguiente, el módulo de autenticación 30 autentica al usuario por comparación del autenticador introducido con el autenticador de referencia. El usuario es autenticado solamente cuando el autenticador introducido es válido con respecto al autenticador de referencia.

Después, durante una etapa 140, cuando el módulo de autenticación 30 ha autenticado al usuario, el tercer módulo de adquisición 32 adquiere un derecho de acceso comprendido en el archivo informático.

Además, cuando el archivo informático comprende una fecha de validez según el complemento facultativo antes citado, el cuarto módulo de adquisición 33 adquiere, durante una etapa 150, la citada fecha de validez del archivo informático.

Durante una etapa 160 siguiente, el módulo de apertura 34 abre una sesión de acceso a la citada al menos una zona segura 42 correspondiente, cuando el derecho de acceso adquirido corresponde al derecho de acceso de referencia comprendido en la memoria 14, y en su caso, cuando la fecha de validez adquirida es posterior a la fecha corriente facilitada por el reloj del equipo 12.

Cuando el archivo informático comprende al menos una configuración que tiene por objetivo modificar el equipo 12, el módulo de ejecución 36 ejecuta, durante una etapa 170 siguiente, al menos una configuración que tiene por objetivo modificar el equipo 12.

Así, el procedimiento de control según la invención permite a un usuario acceder de manera segura a un equipo 12. En efecto, siendo el soporte 10 específico de un usuario dado, si un tercero toma posesión del soporte 10, el citado tercero no podrá servirse del mismo si no conoce el autenticador del usuario. Además, esto permite igualmente identificar unívocamente al usuario físico. Además, el archivo puede hacerse obsoleto por la adición de una fecha de validez al archivo, lo que resuelve el problema de los usuarios temporales,

El procedimiento de control no requiere redes centralizadas para funcionar. Dicho procedimiento es por tanto utilizable para equipos 12 aislados o situados en zonas sin red.

De esta manera, dicho procedimiento de control permite el acceso a equipos aislados o situados en zonas sin red al tiempo que es adaptable y simple de poner en práctica y confiriendo un buen nivel de seguridad

REIVINDICACIONES

1. Procedimiento de control de acceso a una zona segura (42) de un equipo electrónico (12) a partir de un archivo informático, comprendiendo el equipo electrónico (12) una memoria (14) que comprende al menos una zona segura (42), siendo el archivo informático específico de un usuario y estando memorizado en un soporte informático (10), comprendiendo el archivo informático un autenticador de referencia y un derecho de acceso al equipo electrónico (12) para al menos una zona segura (42) correspondiente, comprendiendo la memoria (14) al menos un derecho de acceso de referencia al equipo electrónico (12), siendo puesto en práctica el procedimiento por el equipo electrónico (12) y comprendiendo:

- la adquisición (110) del autenticador de referencia a través del archivo informático a continuación de una conexión del soporte informático (10) al equipo electrónico (12),

- la adquisición (120) de un autenticador proveniente del usuario,

- la autenticación (130) del usuario por comparación del autenticador proveniente del usuario con el autenticador de referencia,

- la adquisición (140) del derecho de acceso a través del archivo informático cuando al final de la autenticación (130), el autenticador proveniente del usuario es conforme con el autenticador de referencia, y

- la apertura (160) de una sesión de acceso a la citada al menos una zona segura (42) correspondiente, cuando el derecho de acceso adquirido corresponde al derecho de acceso de referencia comprendido en la memoria (14).

2. Procedimiento según la reivindicación 1, en el cual el archivo informático está firmado con una clave de firma, estando la clave de firma asociada a un certificado de una autoridad de certificación, estando memorizado el certificado de la autoridad de certificación asociado a la clave de firma en la memoria (14), comprendiendo el procedimiento además, previamente a la adquisición (140) del derecho de acceso, la verificación (100) de la firma del archivo informático con el certificado de la autoridad de certificación memorizado en la memoria (14).

3. Procedimiento según las reivindicaciones 1 o 2, en el cual el soporte informático (10) es un soporte físico desmontable, tal como un soporte de memoria FLASH, por ejemplo una llave USB.

4. Procedimiento según las reivindicaciones 1 o 2, en el cual el soporte informático (10) es un soporte desmaterializado, tal como un archivo informático memorizado en un servidor de red.

5. Procedimiento según una cualquiera de las reivindicaciones 1 a 4, en el cual el archivo informático comprende una fecha de validez, comprendiendo el equipo electrónico (12) un reloj, y

en el cual la apertura de la sesión de acceso comprende además la comparación de la citada fecha de validez son una fecha corriente facilitada por el reloj, siendo abierta la sesión únicamente cuando la fecha de validez es posterior a la citada fecha corriente.

6. Procedimiento según una cualquiera de las reivindicaciones 1 a 5, en el cual el archivo informático comprende al menos una configuración que tiene por objetivo modificar el equipo (12), comprendiendo el procedimiento la ejecución (170) de la configuración en el equipo electrónico (12) después de la apertura de la sesión.

7. Programa de ordenador que comprende instrucciones informáticas, las cuales cuando son ejecutadas por un ordenador, ponen en práctica un procedimiento según una cualquiera de las reivindicaciones 1 a 6.

8. Equipo electrónico (12) que comprende una memoria (14) que comprende al menos una zona segura (42), estando configurado el equipo electrónico (12) para interactuar con un archivo informático, siendo el archivo informático específico de un usuario y estando memorizado en un soporte informático (10), comprendiendo el archivo informático un autenticador de referencia y un derecho de acceso al equipo electrónico (12) para al menos una zona segura (42) correspondiente, comprendiendo la memoria (14) al menos un derecho de acceso de referencia al equipo electrónico (12), comprendiendo el equipo (12):

- un primer módulo (26) de adquisición de un autenticador de referencia a través del archivo informático después de una conexión del soporte informático (10) al equipo electrónico (12),

- un segundo módulo (28) de adquisición de un autenticador proveniente del usuario,

- un módulo (30) de autenticación del usuario por comparación del autenticador proveniente del usuario con el autenticador de referencia,

- un tercer módulo (32) de adquisición del derecho de acceso a través del archivo informático cuando el módulo (30) de autenticación ha autenticado al usuario, y

- un módulo (34) de apertura de una sesión de acceso a la citada al menos una zona segura (42) correspondiente, cuando el derecho de acceso adquirido corresponde al derecho de referencia comprendido en la memoria (14).

9. Equipo (12) según la reivindicación 8, en el cual el equipo (12) es un equipo ferroviario configurado para ser integrado a bordo de un vehículo ferroviario, tal como un motor, un sistema de visualización, un sistema de climatización, un equipo de red, un equipo de seguridad, un equipo de señalización o un equipo de control ferroviario, o bien para ser instalado en el suelo a lo largo de una línea ferroviaria, tal como un semáforo, un cambio de agujas o un paso a nivel.

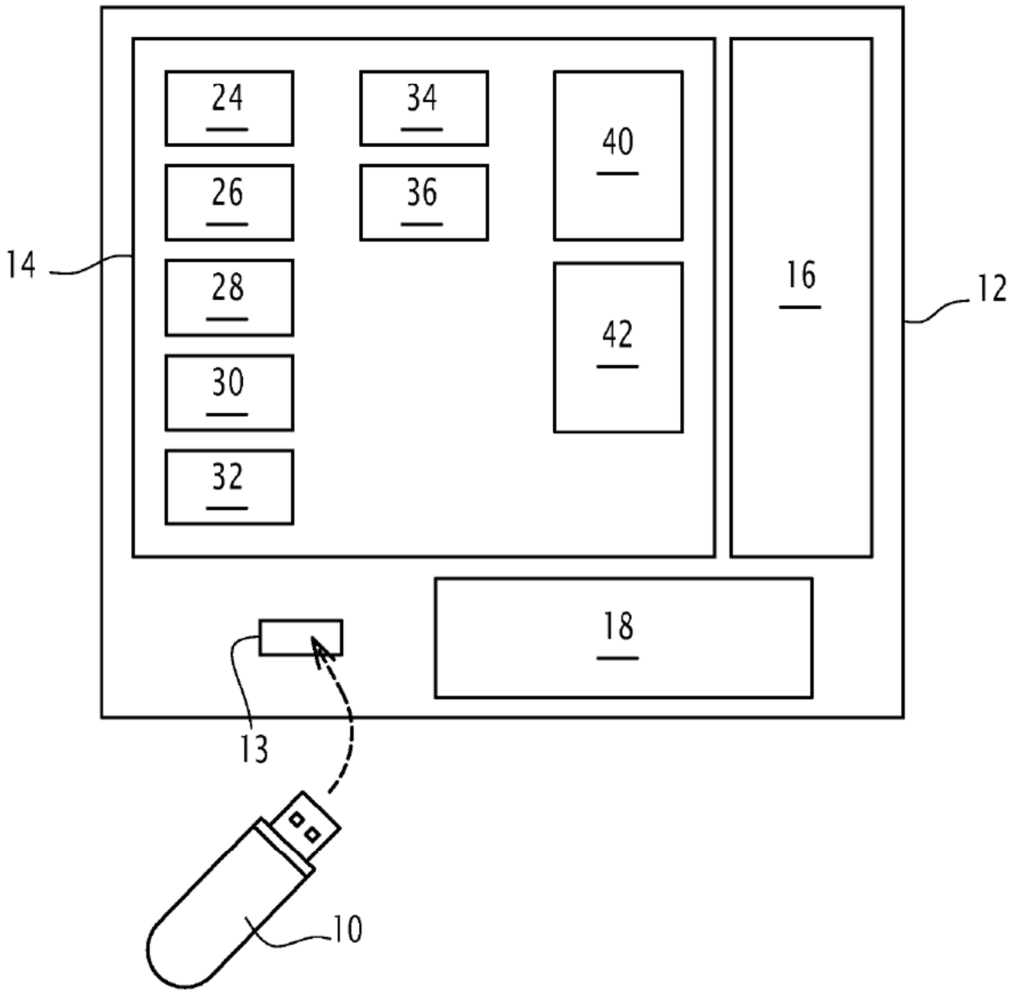

FIG.1

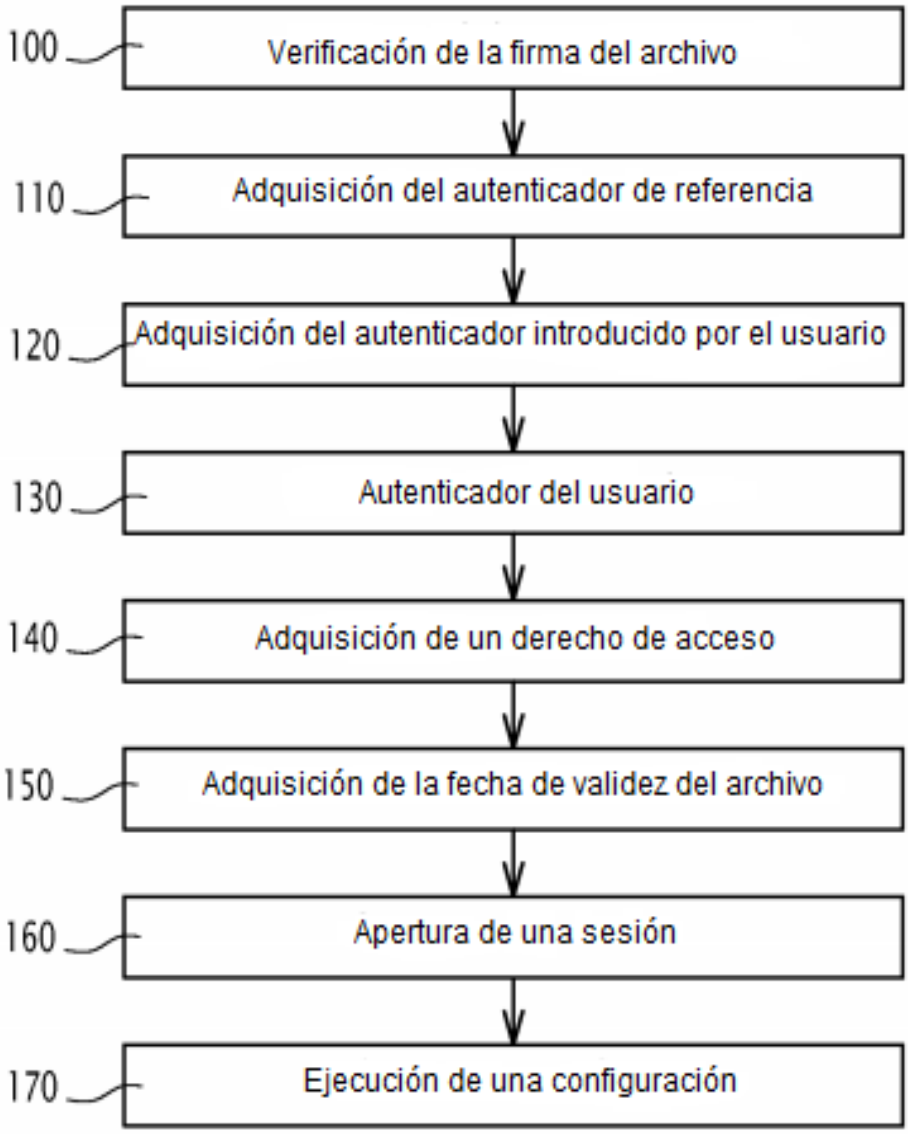
100
Verificación de la firma del archivo
110
Adquisición del autenticador de referencia
120
Adquisición del autenticador introducido por el usuario
130
Autenticador del usuario
140
Adquisición de un derecho de acceso
150
Adquisición de la fecha de validez del archivo
160
Apertura de una sesión
170
Ejecución de una configuración

FIG.2