(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 786 758**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 4/42 (2008.01)
B61L 3/12 (2006.01)
B61L 15/00 (2006.01)
B61L 23/00 (2006.01)
B61L 27/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **06.07.2017 E 17180041 (0)**

(97) Fecha y número de publicación de la concesión europea: **18.03.2020 EP 3272618**

(54) Título: **Procedimiento y dispositivos para desactivar una medida de seguridad de un sistema de seguridad automático**

(30) Prioridad:

19.07.2016 DE 102016213189

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.10.2020

(73) Titular/es:

THALES MANAGEMENT & SERVICES DEUTSCHLAND GMBH (100.0%)
Thalesplatz 1
71254 Ditzingen, DE

(72) Inventor/es:

SCHÄFER, DR. MICHAEL

(74) Agente/Representante:

ISERN JARA, Nuria

DESCRIPCIÓN

Procedimiento y dispositivos para desactivar una medida de seguridad de un sistema de seguridad automático

Antecedentes de la invención

La invención se refiere a un procedimiento para el funcionamiento de un sistema de seguridad automático dentro de un sistema de seguridad de tren crítico para la seguridad, estando configurado el sistema de seguridad para intervenir a través de una medida de seguridad en el funcionamiento del sistema de seguridad de tren crítico para la seguridad, pudiendo ser desactiva la medida de seguridad por parte de un usuario. La invención se refiere también a un dispositivo para desactivar una medida de seguridad de un sistema de seguridad automático dentro de un sistema de seguridad de tren crítico para la seguridad, estando configurado el sistema de seguridad para intervenir a través de una medida de seguridad en el funcionamiento del sistema de seguridad de tren crítico para la seguridad.

Un procedimiento de este tipo se conoce por ejemplo de [1] y [2].

En sistemas de seguridad automáticos conocidos, como por ejemplo el PZB (del alemán punktförmige Zugbeeinflussung, control puntual de tren), puede transmitirse a menudo solo una cantidad limitada de informaciones al conductor del vehículo motor. De este modo puede ocurrir que el conductor del vehículo motor no pueda reconocer de forma segura la razón por la cual ha intervenido en el proceso el sistema de seguridad de tren automático. Para decidir, si la medida de seguridad adoptada por el sistema de seguridad tenía sentido, está prescrito que el conductor del vehículo motor se ponga en contacto con el responsable de tráfico ferroviario y esclarezca las circunstancias inmediatas. En caso de comprobarse que la medida de seguridad adoptada por el sistema de seguridad fue provocada por un fallo técnico y de funcionamiento o entre tanto está obsoleta, el conductor del vehículo motor puede eludir la medida de seguridad.

Ha podido verse no obstante, que la consulta prescrita con el responsable de tráfico ferroviario no siempre se cumple, lo cual ha conducido al accidente descrito en [1]. En [1] se propone por lo tanto prever un bloqueo de nuevo arranque delimitado temporalmente tras producirse la medida de seguridad PZB, que tiene como objetivo en primer lugar, dar al conductor del vehículo motor el tiempo necesario para reflexionar sobre la situación y para llevar a cabo una conversación de radiocomunicación. Esto daría lugar no obstante, a demoras adicionales en el funcionamiento ferroviario. Se propone además de ello en [1], prever un establecimiento de conexión automática, condicionado por el sistema, con el responsable de tráfico ferroviario tras una medida de seguridad PZB, lo cual podría realizarse no obstante solo con un esfuerzo técnico alto.

De [3] se conoce un procedimiento para la autenticación de un usuario de una aplicación en un servidor, que genera un código secreto, el cual ha de transmitir un usuario a un aparato personal. Para la autorización se genera una contraseña de un solo uso, que se calcula a partir de la hora actual y el código secreto. Al registrarse el usuario ha de introducir ahora además de la contraseña normal, también la contraseña de un solo uso generada. El secreto necesario para la generación de la contraseña de un solo uso ya no se transmite y de este modo ya no puede ser escuchado. El usuario ha de poseer a este respecto tanto la contraseña, como también poseer el aparato personal. De este modo bien es cierto que puede asegurarse que solo tengan acceso al servidor usuarios autorizados, pero de este modo no puede evitarse sin embargo un uso no autorizado de una medida de seguridad provocada por el sistema de seguridad automático.

[4] divulga un dispositivo para la autenticación de un usuario de una tarjeta IC, con la cual puede llevarse a cabo banca en línea. El dispositivo comprende una tarjeta IC para la memorización de una clave secreta para la generación de una contraseña de un solo uso y determinados números aleatorios, un terminal para la generación de una primera contraseña de un solo uso por parte de un primer generador de contraseñas y un servidor para la autenticación de la contraseña de un solo uso generada con el terminal. En el servidor se genera mediante un segundo generador de contraseña una segunda contraseña de un solo uso de acuerdo con el mismo procedimiento, tal como se usa en el terminal. La primera contraseña de un solo uso se transmite a través de una línea telefónica o una red al servidor. Mediante un verificador de contraseña se verifica, si la primera contraseña es idéntica a la segunda contraseña generada en el servidor.

Objetivo de la invención

Es por lo tanto el objetivo de la invención proponer un procedimiento para el funcionamiento de un sistema de seguridad automático, con el cual pueda evitarse de manera sencilla un uso no autorizado de una medida de seguridad provocada por el sistema de seguridad automático.

Descripción de la invención

Este objetivo se soluciona de acuerdo con la invención debido a que la medida de seguridad solo puede desactivarse, cuando se han llevado a cabo todos los siguientes pasos de procedimiento:

- establecimiento de contacto con una persona autorizada diferente del usuario;
- comprobación por parte de la persona autorizada, sobre si existe una perturbación, la cual hace necesaria la medida de seguridad;
- en caso de que la persona autorizada compruebe que no existe ninguna perturbación, la cual haga necesaria la medida de seguridad: generación de un número de transacción por parte de la persona autorizada;
- transmisión del número de transacción al usuario;
- introducción del número de transacción en un aparato de autenticación local, el cual tiene informaciones relativas al algoritmo, con el cual se generó el número de transacción;
- determinación de un número de comparación por parte del aparato de autenticación;
- comparación del número de transacción introducido con el número de comparación determinado por el aparato de autenticación;
- en caso de que el número de transacción y el número de comparación coincidan: aprobación de la posibilidad de elusión.

Con el procedimiento de acuerdo con la invención se fuerza una consulta y una comprobación de la situación, para poder eludir el sistema de seguridad. Debido a ello se asegura que la situación puede ser comprobada y evaluada por parte de la persona autorizada, que por regla general tiene acceso a más informaciones que el usuario. Tan pronto como se haya liberado la posibilidad de elusión, puede desactivarse la medida de seguridad. El procedimiento de acuerdo con la invención no requiere ninguna intervención en los aparatos del sistema de seguridad. De esta manera puede elevarse de manera sencilla y económica la seguridad.

De acuerdo con la invención se usan dos aparatos independientes entre sí, concretamente un aparato de identificación para la generación del número de transacción y un aparato de autenticación para la generación del número de comparación y para la comparación del número de comparación con el número de transacción.

Al establecerse el contacto se autentifica el usuario con la persona autorizada por ejemplo mediante indicación de un número de componente del sistema crítico para la seguridad (número de tren o similar). Este número de componente puede usarse entonces también para la generación del número de transacción. La generación del número de transacción por parte de la persona autorizada comprende también la generación por parte de otra persona por orden de la persona autorizada. La transmisión del número de transacción se produce preferentemente de modo telefónico o por SMS. El aparato de autenticación se encuentra en la zona de actuación del usuario (aparato de autenticación local), puede ser manejado por lo tanto por el usuario. La introducción del número de transacción se produce por regla general también por parte del usuario.

El número de transacción se genera preferentemente mediante un aparato de identificación, para el cual el usuario no está autorizado.

En una variante particularmente preferente del procedimiento de acuerdo con la invención se establece el número de comparación mediante el uso de informaciones referentes al algoritmo, con el cual se estableció el número de transacción, por parte del aparato de autenticación. El aparato de identificación y el aparato de autenticación usan por lo tanto preferentemente el mismo algoritmo, para generar el número de identificación o el número de comparación.

La aprobación de la posibilidad de elusión es otorgada preferentemente por el aparato de autenticación.

En una variante espacial se genera el número de transacción mediante un número de componente de un componente a controlar mediante el sistema crítico para la seguridad, en particular el número de tren de un tren, y un sello de fecha. Es posible también un sello temporal preciso en minutos, con el cual se genera el número de transacción. El aparato de autenticación y el aparato de identificación deberían estar equipados por lo tanto con un equipo de medición de tiempo sincronizado (por ejemplo, GNSS, GPS). La generación del número de transacción puede producirse por ejemplo mediante un algoritmo flash.

Para delimitar temporalmente la aprobación de la posibilidad de elusión, puede estar previsto que al número de transacción se le asigne una ventana temporal, dentro de la cual puede usarse el número de transacción para la aprobación de la posibilidad de elusión.

La invención se refiere también a un dispositivo para desactivar una medida de seguridad de un sistema de seguridad automático dentro de un sistema de seguridad de tren crítico para la seguridad, estando configurado el sistema de seguridad para intervenir a través de una medida de seguridad en el funcionamiento del sistema de

seguridad de tren crítico para la seguridad, comprendiendo: un aparato de identificación para generar un número de transacción; un aparato de autenticación para comparar un número introducido con un número de comparación, el cual comprende informaciones relativas al algoritmo, con el cual se estableció el número de transacción.

El aparato de autenticación es de acuerdo con la invención independiente del aparato de identificación. Esto quiere decir que no es posible ninguna influencia en el aparato de autenticación por parte del aparato de identificación, en particular no existe ninguna conexión de datos.

En una forma de realización particularmente preferente el aparato de identificación es parte de un sistema de manejo central.

La invención se refiere también a un sistema de seguridad de tren crítico para la seguridad con un sistema de seguridad automático, a un acceso manejable por parte del usuario al sistema de seguridad y a un dispositivo descrito anteriormente.

El aparato de identificación está dispuesto preferentemente alejado del componente a ser manejado por el usuario. De este modo se evita que el usuario mismo genere el número de transacción.

En una forma de realización especial se trata en el caso del acceso de una tecla de aprobación en el vehículo de motor conductor de un tren. La persona autorizada puede ser en este caso por ejemplo el responsable de tráfico ferroviario. El usuario es preferentemente el conductor del vehículo de motor de un tren. El aparato de autenticación está dispuesto entonces preferentemente en el vehículo de motor del tren. Mediante la tecla de aprobación (botón de anulación) puede eludirse una medida iniciada por el sistema de seguridad.

Otras zonas críticas para la seguridad, en las cuales puede usarse de manera ventajosa el procedimiento de acuerdo con la invención, son el tráfico aéreo, infraestructura crítica para la seguridad, como centrales de energía, suministro de energía y de agua, sistema crítico para la seguridad en tecnología de automatización y de conducción de procesos, sistemas de conducción en el tráfico vial.

Otras ventajas de la invención resultan de la descripción y del dibujo. Asimismo, las características mencionadas anteriormente y desarrolladas aún en mayor medida pueden utilizarse de acuerdo con la invención en cada caso en sí mismas por separado o varias de ellas en combinaciones cualquiera. Las formas de realización mostradas y descritas no han de entenderse como enumeración cerrada, sino que tienen más bien carácter a modo de ejemplo para la descripción de la invención.

Descripción detallada de la invención y dibujo

La Fig. 1 muestra un dispositivo de acuerdo con la invención para el uso en un sistema crítico para la seguridad con un sistema de seguridad automático.

La Fig. 2 muestra un esquema de desarrollo con los pasos de procedimiento del procedimiento de acuerdo con la invención.

La Fig. 1 muestra un sistema 1 crítico para la seguridad con un sistema de seguridad 2 automático. El sistema de seguridad 2 automático interviene automáticamente en el funcionamiento del sistema 1 crítico para la seguridad, en cuanto que se inician medidas de seguridad relativas a un componente (por ejemplo un vehículo de motor) que ha de ser manejado por un usuario 3. En caso de considerar un usuario 3, que una medida de seguridad iniciada, la cual le afecta a él o a un componente a manejar por él, es innecesaria o fue desencadenada por error, existe la posibilidad, de eludir la medida de seguridad. El sistema de seguridad 1 de acuerdo con la invención comprende para ello un dispositivo 5 para desactivar la medida de seguridad. El correspondiente procedimiento se representa esquemáticamente en la Fig. 2. El usuario 3 se pone en contacto para ello en primer lugar con una persona 6 autorizada (por ejemplo, el responsable de tráfico ferroviario) y se identifica a sí mismo por ejemplo con un número de componente KN (por ejemplo, número del tren del tren afectado por la medida de seguridad) característico del componente a manejar por él, como usuario responsable. La persona 6 autorizada comprueba mediante la información 7 que se encuentra a su disposición, si la medida de seguridad es necesaria o no. En caso de concluir la persona 6 autorizada, que la medida de seguridad no era necesaria, genera con la ayuda de un aparato de identificación 8 un número de transacción ID, por ejemplo a partir del número de componente KN transmitido por el usuario y la hora actual. El número de transacción ID generado se transmite al usuario 3. Dentro del ámbito de actuación espacial del usuario 3 hay dispuesto un aparato de autenticación 9 (por ejemplo una tableta o un PC; en el caso de un tren el aparato de autenticación 9 puede estar integrado por ejemplo en una unidad de a bordo). El aparato de autenticación 9 genera (preferentemente como respuesta a solicitud o tras la introducción del número de transacción) un número de comparación REF usando el mismo algoritmo o un algoritmo parecido al algoritmo, con el cual se generó el número de identificación ID. Un algoritmo parecido sería por ejemplo, que se permitiese un desvío temporal determinado, en el cual los números de comparación REF se generasen para +/-5 minutos y que ha de coincidir con la ID. El aparato de autenticación 9 compara además de ello el número de identificación ID con el número de comparación REF. En caso de dar como resultado la comparación, que el número de identificación ID

coincide con el número de comparación REF, se aprueba una posibilidad de elusión de la medida de seguridad iniciada. El sistema crítico para la seguridad de acuerdo con la invención comprende por lo tanto un acceso 10 que puede ser activado, al sistema de seguridad 2 (representado en este caso como conmutador). El aparato de autenticación 9 puede acceder a este acceso al sistema de seguridad 2 y puede permitir una activación de la posibilidad de elusión (mediante activación del acceso 10) o evitarla. La activación se produce por lo tanto mediante el dispositivo 5. El conmutador 10 es preferentemente parte de un sistema de seguridad 2. Típicamente mediante el dispositivo 5 para la activación se aplica una tensión al conmutador 10 o se abre una tapa, para permitir el acceso al sistema de seguridad 2. El aparato de autenticación 9 no interviene en los aparatos del sistema de seguridad 2, sino que permite únicamente el acceso del usuario 3 a los aparatos del sistema de seguridad 2.

La situación, la cual ha conducido a la medida de seguridad, es evaluada de acuerdo con la invención por lo tanto de forma forzosa por dos personas 3, 6 diferentes (principio de los 4 ojos). Una aprobación de la elusión de la medida de seguridad puede producirse solo con el permiso de la persona 6 autorizada, de manera que sin modificación del sistema de seguridad 2 se asegura que se produce una comunicación con la persona 6 autorizada. De esta manera no se requieren por lo tanto interfaces nuevas. Debido a ello puede aumentarse de manera económica la seguridad y mantenerse reducidas las demoras en el funcionamiento del sistema 1 crítico para la seguridad.

Lista de referencias

1	Sistema crítico para la seguridad
2	Sistema de seguridad automático
3	Usuario
5	Dispositivo para desactivar la medida de seguridad
6	Persona autorizada
7	Información
8	Aparato de identificación
9	Aparato de autenticación
10	Acceso que puede ser activado al sistema de seguridad
ID	Número de transacción
REF	Número de comparación

Bibliografía

[1] http://www.eisenbahn-unfalluntersuchung.de/SharedDocs/Publikationen/EUB/DE/Untersuchungsberichte/2014/065 Mannheim Hbf.pdf? blob=publicationFile&v=3 Untersuchungszentrale der Eisenbahn-Unfalluntersuchungsstelle des Bundes: "Untersuchungsbericht Aktenzeichen: 60uu2014-08/002-3323" 23.09.2015

[2] https://en.wikipedia.org/wiki/Punktf%C3 %B6rmige Zugbeeinflussung

[3] https://play.google.com/store/apps/details?id=com.google.android. apps.authenticator2&hl=de

[4] US 6 067 621 A

REIVINDICACIONES

1. Procedimiento para el funcionamiento de un sistema de seguridad (2) automático dentro de un sistema de seguridad de tren (1) crítico para la seguridad, estando configurado el sistema de seguridad (2) para intervenir a través de una medida de seguridad en el funcionamiento del sistema de seguridad de tren (1) crítico para la seguridad, pudiendo ser desactivada la medida de seguridad por parte de un usuario (3),
caracterizado por que,
la medida de seguridad puede desactivarse solo cuando se han llevado a cabo todos los siguientes pasos de procedimiento:

- establecimiento de contacto con una persona (6) autorizada diferente del usuario (3);
- comprobación por parte de la persona (6) autorizada, sobre si existe una perturbación, la cual hace necesaria la medida de seguridad;
- en caso de que la persona (6) autorizada compruebe que no existe ninguna perturbación, la cual haga necesaria la medida de seguridad: generación de un número de transacción (ID) mediante un aparato de identificación por parte de la persona (6) autorizada;
- transmisión del número de transacción (ID) al usuario;
- introducción del número de transacción (ID) en un aparato de autenticación (9) local, el cual tiene informaciones relativas al algoritmo, con el cual se estableció el número de transacción (ID), siendo el aparato de autenticación y el aparato de identificación independientes entre sí, de manera que no existe ninguna conexión de datos entre aparato de autenticación y el aparato de identificación;
- determinación de un número de comparación (REF) por parte del aparato de autenticación (9);
- comparación del número de transacción (ID) introducido con el número de comparación (REF) determinado por el aparato de autenticación (9) mediante el aparato de autenticación;
- en caso de que el número de transacción (ID) y el número de comparación (REF) coincidan: aprobación de la posibilidad de elusión.

2. Procedimiento de acuerdo con la reivindicación 1, caracterizado por que el número de transacción (ID) se genera mediante un aparato de identificación (8), para el cual el usuario (3) no está autorizado.

3. Procedimiento de acuerdo con una de las reivindicaciones anteriores, caracterizado por que el número de comparación (REF) se establece mediante el uso de las informaciones referentes al algoritmo, con el cual se estableció el número de transacción (ID), por parte del aparato de autenticación (9).

4. Procedimiento de acuerdo con una de las reivindicaciones anteriores, caracterizado por que la aprobación de la posibilidad de elusión es otorgada por el aparato de autenticación (9).

5. Procedimiento de acuerdo con una de las reivindicaciones anteriores, caracterizado por que el número de transacción (ID) se genera mediante un número de componente (KN) de un componente del sistema de seguridad de tren (1) crítico para la seguridad, en particular el número de tren de un tren, y un sello de fecha.

6. Procedimiento de acuerdo con una de las reivindicaciones anteriores, caracterizado por que al número de transacción (ID) se asigna una ventana temporal, dentro de la cual puede usarse el número de transacción (ID) para la aprobación de la posibilidad de elusión.

7. Dispositivo (5) para desactivar una medida de seguridad de un sistema de seguridad (2) automático dentro de un sistema de seguridad de tren (1) crítico para la seguridad, estando configurado el sistema de seguridad (2), para intervenir a través de una medida de seguridad en el funcionamiento del sistema de seguridad de tren (1) crítico para la seguridad, comprendiendo:

un aparato de identificación (8) para generar un número de transacción (ID);
medios para transmitir el número de transacción (ID) a un usuario;
un aparato de autenticación (9) para determinar un número de comparación (REF) y para comparar el número de transacción (ID) introducido con el número de comparación (REF), conteniendo el aparato de autenticación (9) informaciones relativas al algoritmo, con el cual se estableció el número de transacción (ID),
medios para la introducción del número de transacción (ID) en el aparato de autenticación (9),
siendo el aparato de autenticación y el aparato de identificación entre sí independientes, de manera que no existe ninguna conexión de datos entre aparato de autenticación y el aparato de identificación.

8. Dispositivo (5) de acuerdo con la reivindicación 7, caracterizado por que el aparato de autenticación (9) es independiente del aparato de identificación (8).

9. Dispositivo (5) de acuerdo con una de las reivindicaciones 7 u 8, caracterizado por que el aparato de identificación (8) es parte de un sistema de manejo central.

10. Sistema de seguridad de tren (1) crítico para la seguridad con un sistema de seguridad (2) automático, un

acceso (10) que puede ser controlado por el usuario, al sistema de seguridad, y un dispositivo (5) de acuerdo con una de las reivindicaciones 7 a 9.

11. Sistema de seguridad de tren (1) crítico para la seguridad de acuerdo con la reivindicación 10, caracterizado por que el aparato de identificación (8) está dispuesto alejado del componente a ser manejado por el usuario (3).

12. Sistema de seguridad de tren crítico para la seguridad de acuerdo con la reivindicación 10 u 11, caracterizado por que se trata en el caso del componente de una tecla de aprobación en el vehículo de motor conductor de un tren.

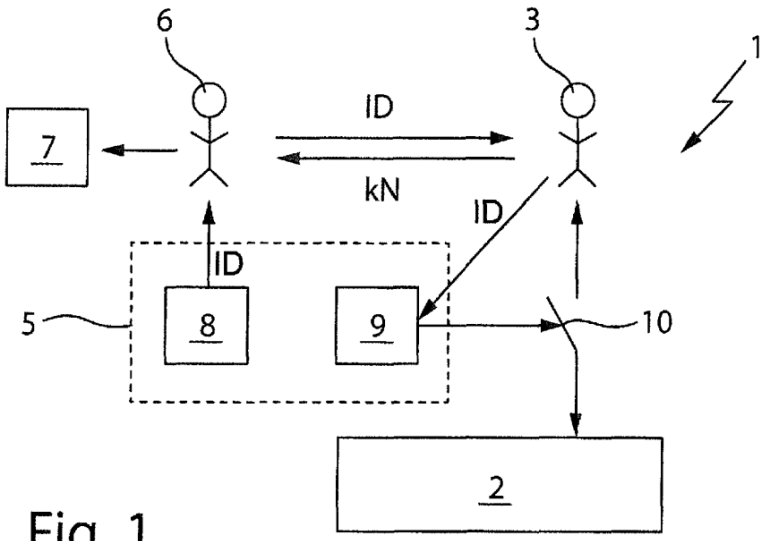
6
3
1
7
ID
kN
ID
ID
5
8
9
10
2

Fig. 1

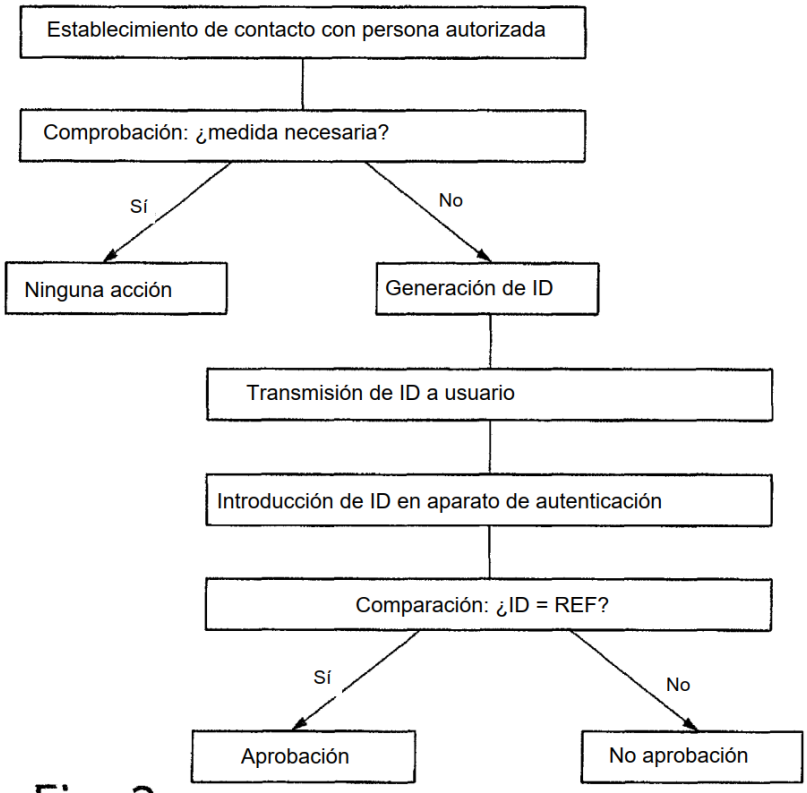
Establecimiento de contacto con persona autorizada
Comprobación: ¿medida necesaria?
Sí
No
Ninguna acción
Generación de ID
Transmisión de ID a usuario
Introducción de ID en aparato de autenticación
Comparación: ¿ID = REF?
Sí
No
Aprobación
No aprobación

Fig. 2