



19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA

11 Número de publicación: **2 278 209**

51 Int. Cl.:
G08B 25/10 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Número de solicitud europea: **03778362 .8**

86 Fecha de presentación : **09.12.2003**

87 Número de publicación de la solicitud: **1579401**

87 Fecha de publicación de la solicitud: **28.09.2005**

54 Título: **Método para la vigilancia remota de ascensores y/o escaleras y/o pasarelas mecánicas.**

30 Prioridad: **02.01.2003 FI 20030008**

73 Titular/es: **Kone Corporation**
Kartanontie 1
00330 Helsinki, FI

45 Fecha de publicación de la mención BOPI:
01.08.2007

72 Inventor/es: **Rekinen, Tero**

45 Fecha de la publicación del folleto de la patente:
01.08.2007

74 Agente: **Lehmann Novo, María Isabel**

ES 2 278 209 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).

DESCRIPCIÓN

Método para la vigilancia remota de ascensores y/o escaleras y/o pasarelas mecánicas.

El presente invento se refiere a un método como se define en el preámbulo de la reivindicación 1 para tratar el código PIN (número de identificación personal) de la tarjeta SIM (módulo de identidad de abonado) de un terminal GSM (sistema global de comunicaciones entre móviles) de un dispositivo de vigilancia remota utilizado para vigilar a distancia ascensores y/o escaleras y/o pasarelas mecánicas.

Por vigilancia remota deben entenderse los procedimientos utilizados, en general, para vigilar la condición y el estado de reparación de un aparato midiendo parámetros cuyas variaciones reflejan cambios de la condición y del estado de reparación del aparato. En la vigilancia remota, la condición y el estado de reparación del aparato se vigilan, generalmente, de una manera regular. Cuando ocurre un cambio en la condición y el estado de reparación, puede realizarse un diagnóstico más preciso del fallo. Por diagnóstico de los fallos deberán entenderse los procedimientos utilizados para detectar e identificar un fallo y para encontrar la causa del mismo. La función más importante de un sistema de diagnóstico de fallos es detectar un fallo de forma fiable y positiva lo antes posible. Algunas veces, el sistema de diagnóstico ha sido programado para ofrecer una sugerencia acerca de cómo podría eliminarse el fallo detectado. De este modo, es posible llevar a la práctica la determinación de la necesidad del mantenimiento preventivo del equipo.

Por vigilancia remota de ascensores debe entenderse la vigilancia de la condición y el estado de reparación de los ascensores desde un lugar alejado empleando una conexión de telecomunicaciones. En la vigilancia remota del estado y de la condición de ascensores, los propios ascensores comunican avisos de las averías que son de esperar. Así, puede detectarse el desgaste de los componentes antes de que fallen por completo. Por tanto, puede establecerse de manera anticipada un valor objetivo fijo para la frecuencia con que se averían los ascensores, a fin de medir su fiabilidad y calidad.

En la técnica anterior, un dispositivo de vigilancia remota empleado en la actualidad para la vigilancia remota de ascensores y/o escaleras y/o pasarelas mecánicas, comprende un terminal GSM que se comunica, mediante una conexión de telecomunicaciones inalámbrica, con un centro de control de vigilancia remota, al cual transmite información sobre la condición y el estado de reparación de los ascensores y/o escaleras y/o pasarelas mecánicas. Para poder establecer una conexión de telecomunicaciones desde el terminal GSM al centro de control de vigilancia remota, el terminal GSM comprende una tarjeta SIM que es activada por un código denominado PIN.

La tarjeta SIM es una unidad de identificación de abonado empleada en comunicaciones inalámbricas. El código PIN es un número de identificación específico del terminal y del usuario, asignado a la tarjeta SIM.

En forma conocida, el código PIN se utiliza para impedir el uso no autorizado de la tarjeta SIM del terminal GSM de un dispositivo de vigilancia remota, ya que dicho uso genera costes indeseables para el propietario del terminal. El dispositivo de vigilancia remota ofrece el código PIN automáticamente cada vez

que la tarjeta SIM lo solicita, por ejemplo, en relación con la conexión de la alimentación.

Cuando ha de ponerse en uso el terminal GSM del dispositivo para la vigilancia remota de ascensores y/o escaleras y/o pasarelas mecánicas, el instalador de la conexión de telecomunicaciones debe tener en su poder la tarjeta SIM y conocer el código PIN de la tarjeta SIM a instalar. La tarjeta SIM requerida para la instalación es propiedad del cliente o de la compañía que instala y/o mantiene el ascensor y/o la escalera y/o la pasarela mecánicas. En relación con la instalación, o después de ella, existe la posibilidad de que a esta tarjeta SIM utilizada para la instalación y al código PIN exigido para su uso, se les de un uso incorrecto, o que se pierda la tarjeta SIM junto con el código PIN asociado a ella, lo que sería el origen de costes innecesarios para el propietario de la tarjeta SIM.

El problema principal que conllevan las soluciones de acuerdo con el presente estado de la técnica está relacionado con la seguridad de los datos del código PIN necesario cuando se pone en uso la tarjeta SIM del terminal GSM de un dispositivo de vigilancia remota y que ha de introducirse en ella.

El objeto del presente invento es superar los inconvenientes y solventar los problemas encontrados en las soluciones antes mencionadas de la técnica anterior.

En términos más definidos, el método del invento para tratar el código PIN de la tarjeta SIM del terminal GSM de un dispositivo de vigilancia remota empleado para vigilar a distancia ascensores y/o escaleras y/o pasarelas mecánicas, se caracteriza por lo que se describe en la parte caracterizadora de la reivindicación 1. Las características de ciertas realizaciones preferidas del invento se exponen en las reivindicaciones subordinadas.

Utilizando el método del invento, se logran varias ventajas significativas con respecto a la técnica anterior.

En una realización preferida, el presente invento mejora la seguridad con que se tratan los datos del código PIN de la tarjeta SIM del terminal GSM del dispositivo de vigilancia remota. La mejora de la seguridad de los datos es posible porque el código PIN creado en el centro de control de vigilancia remota por generación aleatoria, no es conocido para nadie ni se imprime en papel sino que se guarda en la memoria del dispositivo de vigilancia remota y en el centro de control de vigilancia remota.

Otra ventaja conseguida merced al presente invento es que el código PIN real, generado aleatoriamente, corrientemente en uso y facilitado posteriormente, nunca tiene que introducirse manualmente. Por tanto, la seguridad de los datos se ve mejorada de manera sustancial ya que, incluso ni el instalador, conoce el código en cuestión.

Otra ventaja conseguida por el presente invento es que hace posible sustituir el dispositivo de vigilancia remota, terminal GSM o tarjeta SIM, por ejemplo, por una pieza de repuesto sin que, por ello, se vea perjudicada la seguridad.

Una compañía que preste mantenimiento de ascensores y/o escaleras y/o pasarelas mecánicas utilizando vigilancia remota, puede aprovechar ventajosamente la seguridad de la transmisión de datos en la vigilancia a distancia de ascensores y/o escaleras y/o pasarelas mecánicas, como argumento comercial.

El presente invento se refiere, principalmente, a la

transmisión de datos en la vigilancia remota inalámbrica mediante telecomunicaciones. Igualmente, puede aplicarse en comunicaciones de datos en el caso de varias conexiones de red instaladas en ascensores, Tales conexiones de red son, por ejemplo, WLAN, LAN, Ethernet, etc.

El presente invento se refiere a un método de tratar el código PIN de la tarjeta SIM de un terminal GSM de un dispositivo de vigilancia remota utilizado para vigilar a distancia ascensores y/o escaleras y/o pasarelas mecánicas. De acuerdo con la realización más preferida del presente invento, cuando han de ponerse en uso el dispositivo de vigilancia remota y el terminal GSM, a la tarjeta SIM antes mencionada se le asignan un código PIN público, por defecto, y un código PIN generado aleatoriamente. El código PIN por defecto se utiliza, preferiblemente, cuando se ponen en uso, por vez primera, el dispositivo de vigilancia remota y su terminal GSM y su tarjeta SIM, para permitir la comunicación de datos funcionales entre el antes citado terminal GSM y el centro de control de vigilancia remota, después de lo cual, mediante una primera llamada de configuración, al dispositivo de vigilancia remota se le asigna el código generado aleatoriamente, que es puesto en uso de forma automática.

De acuerdo con una realización del presente invento, el código PIN público, por defecto, es asignado antes que el código PIN generado aleatoriamente. De acuerdo con otra realización del presente invento, el código PIN generado aleatoriamente es asignado antes que el código PIN público, por defecto.

De acuerdo con una realización preferida del presente invento, el código PIN generado aleatoriamente es creado en forma automática en el centro de control de vigilancia remota, en donde se guarda el código PIN generado aleatoriamente y desde donde el código PIN generado aleatoriamente es enviado a la tarjeta del dispositivo de vigilancia remota. De acuerdo con otra realización del invento, el código PIN público, por defecto, y el código PIN generado aleatoriamente se guardan en la memoria de la tarjeta del dispositivo de vigilancia remota.

Además, de acuerdo con una realización del presente invento, el código PIN público, por defecto, es transmitido desde la tarjeta del dispositivo de vigilancia remota a la tarjeta SIM como código PIN generado aleatoriamente cuando se ponen en uso el dispositivo de vigilancia remota y el terminal GSM.

De acuerdo con el presente invento, cuando el código PIN es solicitado desde la tarjeta del dispositivo de vigilancia remota en relación con la conexión de la alimentación al terminal GSM, siempre se le asigna automáticamente un código PIN a la tarjeta SIM del terminal GSM. De acuerdo con una realización del presente invento, a la tarjeta SIM se le asignan tanto un código PIN público, por defecto, como un código PIN generado aleatoriamente, en cualquier orden, de modo que cuando el código PIN facilitado en primer lugar sea erróneo, se facilite el otro código PIN en forma automática.

De acuerdo con otra realización del invento, la alimentación es conectada al terminal GSM en relación con la instalación o la sustitución del antes citado terminal GSM o por un cambio de la batería de respaldo de la tarjeta SIM o del dispositivo de vigilancia remota, o cuando el sistema se recupera de una situación anormal. Además, cuando se está cambiando la tarjeta SIM del terminal GSM, se asignan tanto un código PIN público, por defecto, como un código PIN generado aleatoriamente.

De acuerdo con el presente invento, el código PIN público, por defecto, utilizado es, preferiblemente, cualquier código definido por un operador local y/o global, y/o acordado con él, para una nueva tarjeta SIM del terminal GSM.

En lo que sigue se describirá el invento con detalle haciendo referencia al dibujo adjunto, que ilustra el principio de funcionamiento del método del invento para tratar el código PIN de la tarjeta SIM de un terminal GSM de un dispositivo de vigilancia remota utilizado para vigilar a distancia ascensores y/o escaleras y/o pasarelas mecánicas.

De acuerdo con el presente invento, cuando ha de ponerse en uso la tarjeta del dispositivo de vigilancia remota para vigilar a distancia ascensores y/o escaleras y/o pasarelas mecánicas, a la tarjeta SIM del terminal GSM conectada a él mediante un cable se le ha de facilitar, primero, un denominado código PIN público, por defecto, "defecto", que puede ser cualquier número definido por un operador local y/o global y/o acordado con él. Después, se le facilita a la tarjeta SIM, a través de la tarjeta de vigilancia remota, un nuevo código PIN, "aleatorio", generado mediante un procedimiento totalmente aleatorio en el centro de control del sistema para la vigilancia remota de ascensores y/o escaleras y/o pasarelas mecánicas. Este código PIN generado al azar, "aleatorio", sólo se guarda, subsiguientemente, en el centro de control que controla la vigilancia remota de ascensores y/o escaleras y/o pasarelas mecánicas, y en la memoria de la tarjeta del dispositivo de vigilancia remota. El código PIN público, por defecto, "defecto", se guarda en la memoria del dispositivo de vigilancia remota.

Después de que al terminal GSM del dispositivo de vigilancia remota para vigilar a distancia ascensores y/o escaleras y/o pasarelas mecánicas, se le ha asignado un código PIN generador al azar, "aleatorio", es posible establecer una conexión de comunicaciones para la transmisión de datos relacionados con la vigilancia remota desde el terminal GSM antes citado al centro de control que controla la vigilancia remota de ascensores y/o escaleras y/o pasarelas mecánicas, con el fin de garantizar la seguridad de los datos de la conexión.

Resulta muy evidente que, en el futuro, el método del presente invento será aplicable, incluso, en otros dispositivos de funcionamiento automático, vigilados a distancia merced a la utilización de comunicaciones de datos basadas en tecnología GSM.

REIVINDICACIONES

1. Método para tratar el código PIN de la tarjeta SIM de un terminal GSM de un dispositivo de vigilancia remota utilizado para vigilar a distancia ascensores y/o escaleras y/o pasarelas mecánicas, **caracterizado** porque, cuando han de ponerse en uso el dispositivo de vigilancia remota y el terminal GSM, a la antes citada tarjeta SIM se le asignan un código PIN público, por defecto, y un código PIN generado aleatoriamente.

2. Método de acuerdo con la reivindicación 1, **caracterizado** porque el antes mencionado código PIN público, por defecto, se asigna a la antes citada tarjeta SIM antes que el código generado aleatoriamente.

3. Método de acuerdo con la reivindicación 1, **caracterizado** porque el antes mencionado código PIN generado aleatoriamente, se asigna a la antes citada tarjeta SIM antes que el anteriormente mencionado código PIN público, por defecto.

4. Método de acuerdo con la reivindicación 1 o la reivindicación 2 o la reivindicación 3, **caracterizado** porque el antes citado código PIN generado aleatoriamente es creado de forma automática en el centro de control de vigilancia remota, donde se guarda el código PIN generado aleatoriamente, antes citado, y desde donde el mencionado código PIN generado aleatoriamente es enviado a la tarjeta del dispositivo de vigilancia remota.

5. Método de acuerdo con la reivindicación 1 o la reivindicación 2 o la reivindicación 3 o la reivindicación 4, **caracterizado** porqué antes citado código PIN público, por defecto, y el código PIN generado aleatoriamente, se guardan en la memoria de la tarjeta del dispositivo de vigilancia remota.

6. Método de acuerdo con la reivindicación 1 o

la reivindicación 2 o la reivindicación 3 o la reivindicación 4 o la reivindicación 5, **caracterizado** porque el antes citado código PIN público, por defecto, es transmitido desde la tarjeta del dispositivo de vigilancia remota a la tarjeta SIM como código PIN generado aleatoriamente cuando se ponen en uso el antes citado dispositivo de vigilancia remota y el terminal GSM.

7. Método de acuerdo con una cualquiera de las reivindicaciones precedentes, **caracterizado** porque, cuando el código PIN es solicitado desde la tarjeta del dispositivo de vigilancia remota en relación con la conexión de la alimentación al antes citado terminal GSM, siempre se asigna automáticamente un código PIN a la tarjeta SIM del terminal GSM.

8. Método de acuerdo con la reivindicación 1 o la reivindicación 2 o la reivindicación 3 o la reivindicación 7, **caracterizado** porque a la antes citada tarjeta SIM se le asignan tanto un código PIN público, por defecto, como un código PIN generado aleatoriamente, en cualquier orden y de tal manera que, cuando el código PIN facilitado en primer lugar sea erróneo, se facilite automáticamente el otro código PIN.

9. Método de acuerdo con la reivindicación 7, **caracterizado** porque la alimentación se conecta al antes citado terminal GSM en relación con la instalación o la sustitución del terminal GSM antes mencionado o con un cambio de la batería de respaldo de la tarjeta SIM o del dispositivo de vigilancia remota, o cuando el sistema se recupera de una situación anormal.

10. Método de acuerdo con una cualquiera de las reivindicaciones precedentes, **caracterizado** porque el código PIN público, por defecto, utilizado es cualquier código definido por un operador local y/o global y/o acordado con él, para una nueva tarjeta SIM del antes citado terminal GSM.

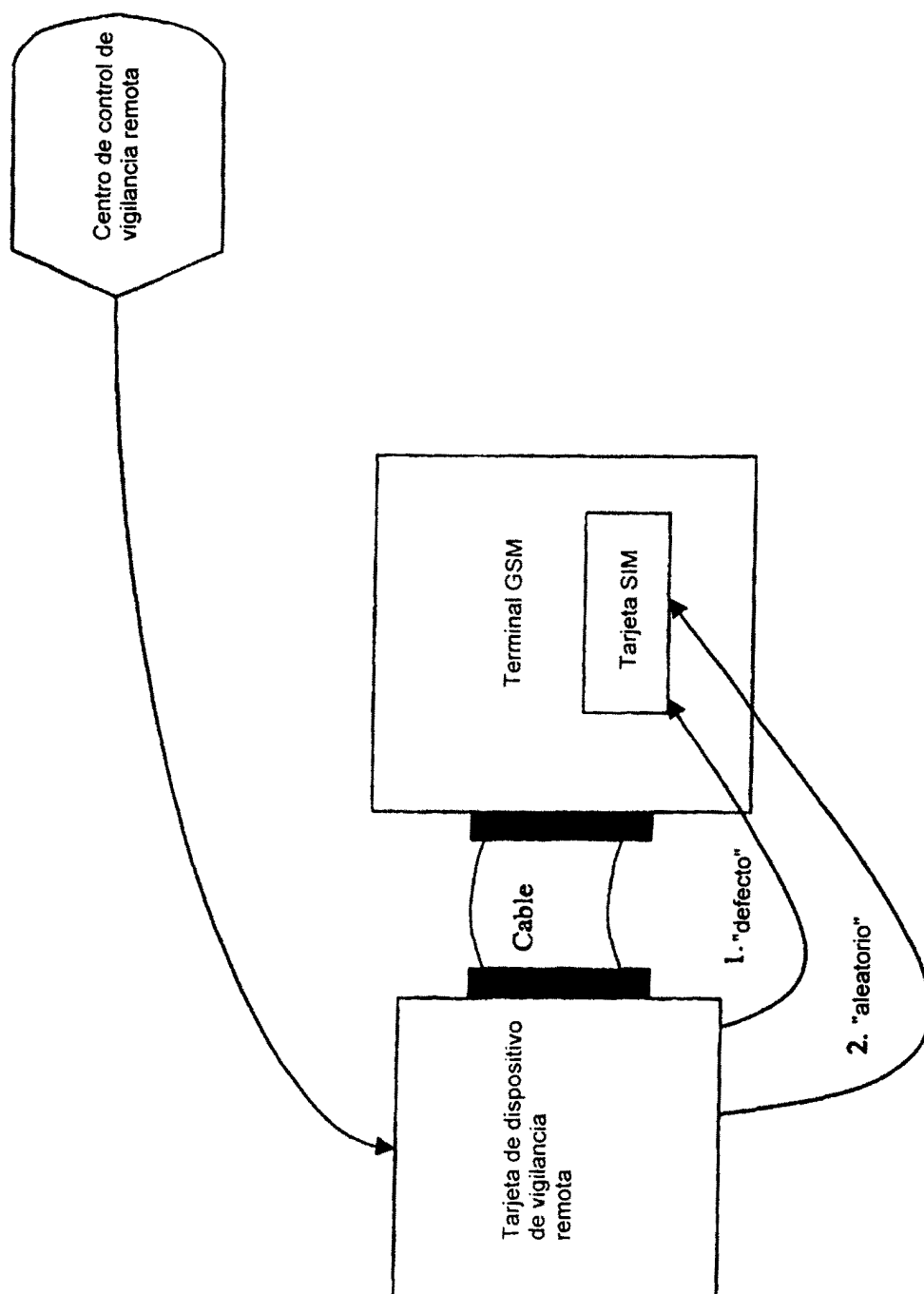


Fig. 1