(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 384 446**

(51) Int. CI.:
G08B 25/08 (2006.01)
G06F 21/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08759068 .3**
(96) Fecha de presentación: **06.06.2008**
(97) Número de publicación de la solicitud: **2220625**
(97) Fecha de publicación de la solicitud: **25.08.2010**

(54) Título: **Procedimiento para la supresión segura y selectiva de alarmas en una central de vigilancia y control**

(30) Prioridad:
17.12.2007 DE 102007061163

(45) Fecha de publicación de la mención BOPI:
05.07.2012

(45) Fecha de la publicación del folleto de la patente:
05.07.2012

(73) Titular/es:
DEUTSCHE TELEKOM AG
FRIEDRICH-EBERT-ALLEE 140
53113 BONN, DE

(72) Inventor/es:
SCHRÖDER, Stefan y
WEBER, Jens

(74) Agente/Representante:
de Elzaburu Márquez, Alberto

DESCRIPCIÓN

Procedimiento para la supresión segura y selectiva de alarmas en una central de vigilancia y control

La presente invención se refiere a un procedimiento para la supresión selectiva de una alarma a través de la determinación de un acceso y/o entrada permitido o no permitido a una instalación de acceso de una red de telecomunicaciones, en particular de una red de telefonía móvil, en una central de supervisión y control que supervisa la instalación de acceso sobre la base de mensajes de alarma, que son depositados a través de la apertura de la instalación de acceso. Además, la invención se refiere a un sistema para la aplicación del procedimiento.

El documento US 4.090.182 publica un procedimiento para la determinación de una apertura permitida no permitida de una instalación de acceso. En el caso de apertura no permitida, se activa en este caso una alarma. Antes de la apertura se puede transmitir por una persona autorizada un mensaje en forma de una señal codificada por medio de un aparato de radio a una instalación de supervisión local. La recepción del mensaje conduce a una supresión de una alarma, de tal manera que no se emite ninguna alarma. De esta manera, la instalación de supervisión se conmuta de forma indeterminada.

Las instalaciones de acceso necesarias para el funcionamiento de una red de telefonía móvil, como por ejemplo estaciones de base, estaciones amplificadoras o estaciones repetidoras representan instalaciones especialmente sensibles, que pueden ser puntos de ataque de accesos no autorizados a la red de telefonía móvil y a la telecomunicación que se está desarrollando en ella, que en las redes de telefonía móvil de la segunda y tercera generación (redes 2G y 3G) no es sólo ya desde hace mucho tiempo lenguaje con intercambio general de datos discrecionales. Un acceso representa un ataque inminente, que se puede manifestar, por ejemplo, en una escucha de la comunicación, una inserción o desviación de paquetes de datos o una falsificación de los datos. Mientras que una escucha de la telecomunicación a través de la obtención de informaciones personales representa una entrada en la esfera privada, de las manipulaciones de datos resulta un potencial de peligro considerablemente más elevado, en particular en lo que se refiere al desarrollo de procesos de encargo y de pago, que se realizan actualmente cada vez en mayor medida con terminales móviles para la telefonía móvil, y a la escucha de palabras de paso a través de phishing Website (páginas Web falsificadas).

Debido a la transmisión cada vez más creciente de informaciones sensibles a través de redes de telefonía móvil, se plantean requerimientos elevados a la seguridad de los puntos de acceso a la red de telefonía móvil. Tanto más amenazante es el hecho de que la codificación de datos útiles en algunas tecnologías de radio se realiza en las estaciones de base y, por lo tanto, se registra aquella criptografía de datos asociados en las estaciones de base. Las estaciones de base apenas presentan seguridad técnica interna para impedir una ingerencia. En primer término están protegidas por medidas de seguridad mecánicas comparativamente débiles (por ejemplo, puertas cerradas). Por lo tanto, no se garantiza la protección de los datos sensibles y los intrusos pueden obtener acceso de manera fácil a las estaciones y a la red de telefonía móvil cuando han superado la protección mecánica. Una ingerencia puede afectar en esta caso a los datos útiles, pero también a otros parámetros y en este caso pueden provocan daños graves dentro de la red o en otras estaciones de base. Por lo tanto, la supervisión de los puntos de acceso hacia una red de telefonía móvil ha adquirido una importancia enorme.

La especificación y normalización de las medidas de seguridad, entre otras, mecánicas no es el objetivo de la 3GPP (3rd Generation Partnership Project, una cooperación a nivel mundial de gremios de normalización, en particular para la normalización de redes de la segunda generación (GSM, Sistema Global para Comunicación Móvil) y de la tercera generación (UMTS, Sistema Universal de Telecomunicación Móvil). Por lo tanto, los fabricantes de elementos de la red han tomado con frecuencia medidas propias, que se basan en una supervisión de la apertura de la puerta en la instalación de acceso en los llamados OMCs (Centro de Mantenimiento de Operaciones). Son soluciones relacionadas con software, que solamente prestan una contribución a la seguridad de las instalaciones de acceso a la red de telefonía móvil.

No obstante, a demás de los accesos hostiles no autorizados mencionados anteriormente que son posibles en general a instalaciones de entrada de redes de telecomunicaciones, también son necesarios trabajos de instalación, reparación y mantenimiento necesarios para la autorización en las instalaciones de acceso, puesto que es necesario realizar a intervalos regulares la sustitución de componentes de hardware y, dado el caso, la copia de Firmware actual o trabajos de reparación en casos de averías. Tal entrada o acceso necesarios técnicamente a la instalación de entrada, que se designa, en general, también como apertura de la instalación de acceso, debe distinguirse en la práctica del acceso hostil no autorizado.

Se conoce equipar las estaciones de base de redes de telefonía móvil y otras instalaciones de entrada de redes de telecomunicaciones, por ejemplo DSLAMs (Digital Subscriber Line Access Multiplexer, puntos de conexión de abonados y puntos de conmutación DSL), que no están en lugares de instalación asegurados, con instalaciones de supervisión de la apertura. Estas instalaciones de entrada se designan, en general, también como Base-Station Access Net (BS-AN). La apertura de un BS-AN asegurada de forma correspondiente, es decir, la creación de un

acceso a los lugares que albergan el hardware sensible de la instalación de acceso o la creación de un acceso a través de la apertura de una carcasa, armario de distribución o a través de toma directa del hardware, tiene entonces como consecuencia que en el lugar de supervisión y control competente para la supervisión de la BS-AN (OMC, Centro de Mantenimiento de Operaciones) aparece un mensaje de alarma en la técnica del sistema. En virtud de los diferentes fabricantes de los componentes asegurados, pueden aparecer también diferentes mensajes de alarmas en diferentes OMCs.

Para la verificación y evaluación de si el mensaje de alarma se basa en un acceso permitido, éste debe ser evaluado por el personal de servicio de la OMC. Esto se realiza a través de la comparación con planes de servicio de las aplicaciones en el lugar. Si al mensaje de alarma no se puede asociar ninguna aplicación introducida en los planes de servicio y correlacionada con su aparición temporal en la BS-AN correspondiente, existe la sospecha de una entrada o acceso no autorizado, y deben tomarse medidas adecuadas y debe rechazarse el ataque potencial.

La creación de los planes de servicio y su comparación manual con mensajes de alarma aparecidos es costosa de tiempo y no se puede realizar con gasto de tiempo y de personal tolerable. Además, la comparación requiere tiempo, dentro del cual ya se ha podido producir un daño considerable a través del ataque. Una comparación electrónica en el marco de una solución protegida por procesamiento electrónico de datos EDV es igualmente inadecuada, puesto que debe crearse la gestión del plan de servicio en forma electrónica y debe proveerse con interfaces con muchos OMCs diferentes.

Además, en la práctica no es posible la creación de planes de servicio completos con antelación, puesto que pueden aparecer interferencias y fallos de manera repentina e inesperada, también en función de trabajos en otras BS-ANs o componentes de la red y pueden requerir trabajos de reparación y aplicaciones rápidos y flexibles.

Además, hay que tener en cuenta que incluso la comparación de planes de servicio con la aparición de una comunicación de alarma no representa una manifestación unívocamente segura sobre un acceso autorizado a una BS-AN, puesto que un plan de servicio solamente contiene la información sobre una apertura realizada “en el transcurso de un día” de una BS-AN determinada y, por lo tanto, solamente proporciona puntos de partida inexactos párale tiempo de apertura admisible. En particular, permanece sin aclarar cuándo se realiza una apertura. Puesto que una apertura no autorizada de una BS-AN se puede realizar, con la provocación de datos considerables con repercusiones a largo plazo, también solamente durante corto espacio de tiempo, en decir, en el transcurso del día en el que están previstos trabajos de mantenimiento y reparación en la BS-AN correspondiente, éstos no se tienen en cuenta y existe el peligro de que se suprima una alarma activada también durante la apertura no autorizada de la BS-AN. Si se tiene en cuenta que un técnico abre en un día de aplicación por término medio 10 BS-AN, si se encontrasen por término medio 50 técnicos trabajando en todo el país, sería posible que pasasen desapercibidos ataques a 500 estaciones de base. Esto representa un riesgo para la seguridad intolerable y que requiere reducción.

Las investigaciones de la seguridad en BS-ANs y OMCs actuales han mostrado que es forzosamente necesaria una elevación de la norma de seguridad y una reducción del riesgo para la seguridad.

Por lo tanto, la presente invención tiene el cometido de reducir en el tiempo y en el personal el gasto de trabajo para la determinación de si en la apertura de una instalación de acceso, que se basa en un mensaje de alarma recibido, se trata de un acceso autorizado o no autorizado, y de ahorrar de esta manera costes, así como reducir al mínimo el riesgo para la seguridad a través de la determinación rápida y segura de una apertura autorizada o no autorizada, incluyendo el riesgo de suprimir de forma inadvertida la alarma para una apertura no autorizada.

Este cometido se soluciona por medio de un procedimiento con las características de la reivindicación 1 así como con un sistema de acuerdo con la reivindicación 17 para la aplicación del procedimiento según la reivindicación 1.

De acuerdo con la invención, está previsto para la supresión selectiva de una alarma a través de la determinación de una entrada y/o acceso autorizado o no autorizado a una instalación de entada de una red de telecomunicaciones, en particular de una red de telefonía móvil o de una red fija, en una central de control que supervisa la instalación de entrada sobre la base de mensajes de alarma, que son depositados a través de la apertura de la instalación de entrada, que se transmita en primer lugar en cada caso ante de la apertura de la instalación de entrada por medio de un aparato de alarma un mensaje a un servidor de mensajes. De esta manera, el técnico indica a la central de supervisión y control (OMC) que supervisa la instalación de entrada, antes de la apertura, que quiere abrir una instalación de entrada determinada, es decir, que quiere crear y creará acceso o entrada a los puntos de ataque de la red de telecomunicaciones. La transmisión se puede realizar en este caso directamente al servidor de mensajes o indirectamente en primer lugar a una instalación de recepción, a la que está asociado el servidor de mensajes.

El mensaje comprende en este caso al menos informaciones sobre la identidad del emisor del mensaje y la identidad de la instalación de entrada. Como complemento de estas informaciones, el mensaje puede contener también otros datos, por ejemplo sobre el comienzo temporal exacto de los trabajos de mantenimiento o de reparación o la duración prevista o el final de los trabajos, de manera que se puede definir una ventana de tiempo, dentro de la cual debe realizarse un filtrado de la alarma.

El mensaje se puede realizar en forma de un mensaje corto electrónico (SMS), de una comunicación de voz o de un formulario de la Web. De manera alternativa, puede encontrar aplicación también un procedimiento con reconocimiento de palabra individual, por ejemplo IVR (Interactive Voice Response) para la interacción de voz. No obstante, también son posibles otros formatos de datos.

Como aparato de mensajes se puede utilizar un terminal móvil para la telefonía móvil, en particular un teléfono móvil, un Smartphone o una tarjeta de datos de telefonía móvil de un ordenador portátil. El aparato de mensajes corresponde en este caso con preferencia a la norma de seguridad 3GPP. De manera alternativa y/o complementaria, para el caso de un fallo local de la red de telefonía móvil se puede prever un aparato de mensajes en la instalación de entrada, a través del cual se puede informar a la central de control sobre la apertura de la instalación de entrada.

La transmisión del mensaje se puede realizar a través de una conexión segura, que es especialmente segura contra escucha y modificación del contenido, como también presenta una protección contra repetición (replay protection). De esta manera se consigue también durante la transmisión del mensaje una norma de seguridad alta. Con preferencia, como aparato de mensajes se puede utilizar un aparato de este tipo según la norma 3GPP, en la que se dan estas características de seguridad en una medida suficiente. De manera alternativa o adicional, se puede establecer una seguridad de extremo a extremo entre el aparato de mensajes y el servidor de mensajes.

De acuerdo con la invención, está previsto que el servidor de mensajes pueda generar una información de supresión de la alarma. Con preferencia, ésta se genera en función de los datos contenidos en el mensaje, en particular sólo cuando se ha realizado una verificación de los datos contenidos en el mensaje son resultado positivo. La verificación puede comprender en este caso la autentificación del emisor del mensaje y/o de la instalación de entrada. Se puede realizar una autentificación especialmente segura del emisor del mensaje con preferencia a través de la tarjeta SIM (Subscriber Identity Module) o UICC (Universal / UMTS Integrated Circuit Card) del aparato de mensajes, que sirven en cada caso para la identificación de un usuario de telefonía móvil en la red y/o se puede realizar a través del MSISDN (Mobile Subscriber USDN Number) del emisor del mensaje. El MSISDN representa un número de teléfono móvil unívoco en todo el mundo y se forma por el código del país (CC), el Código de Destino Nacional (NDC) y el número de abonado (SN). De manera alternativa o en combinación, para la autentificación se puede utilizar también un PIN asociado al emisor del mensaje. Además, de manera alternativa o en combinación con los procedimientos de autentificación mencionados son posibles también otros procedimientos, que se conocen en la técnica de seguridad, por ejemplo identificación de voz o verificación de la huella digital. Además, adicionalmente se puede realizar una autentificación de la instalación de entrada a través de un reconocimiento de la instalación de entrada asociada.

La autentificación puede conducir entonces a un resultado positivo, cuando la persona del emisor del mensaje puede ser identificada con un técnico conocido o cuando adicionalmente la identidad de la instalación de entrada coincide con una instalación de entrada realmente existente y supervisada por el OMC llamado.

Además, la verificación puede comprender, de manera alternativa o complementaria a la autentificación, una autorización del emisor del mensaje. En esta autorización se puede verificar, por ejemplo, si el emisor del mensaje posee la fase de seguridad necesaria para la apertura de la instalación de entrada anunciada o bien posee una autorización de entrada general. Además, adicionalmente se puede verificar si la identidad de la instalación de entrada pertenece a un grupo de identidades, que no están autorizadas para el mensaje o bien cuya apertura está, en principio, limitada o prohibida, de manera que en este caso no se realiza una autorización del emisor del mensaje.

Para completar, en la autentificación o autorización para la verificación de la factibilidad se pueden utilizar informaciones de planes de servicio. Así, por ejemplo, se puede verificar si el técnico, cuya autentificación se realiza, se encuentra también realmente en servicio en el día correspondiente y/o en la región, en la que se encuentra la instalación de entrada. De esta manera se eleva adicionalmente la seguridad.

La autorización puede conducir, por ejemplo, a un resultado positivo cuando el emisor del mensaje posee los derechos de entrada necesarios para la apertura de la instalación de entrada, en particular la fase de seguridad necesaria y/o la autorización de entrada y la instalación de entrada no pertenece a un grupo de instalaciones, que están bloqueadas, en principio, para cualquier apertura. Además, puede estar previsto que la autorización solamente conduzca a un resultado positivo cuando se ha realizado con éxito la verificación de la factibilidad. La autorización propiamente dicha se puede realizar, por ejemplo, introduciendo la identidad del emisor del mensaje, por ejemplo en forma del MSISDN, en una Tabla de emisores de mensajes autorizados.

Con preferencia, se puede realizar una verificación positiva cuando se ha realizado una autentificación positiva así como una autorización positiva. El servidor de mensajes genera en este caso una información de supresión de la alarma. Ésta puede estar limitada según la invención en su validez temporal.

Para la consecución de una medida alta de seguridad, se puede establecer el comienzo de la validez de la información de la supresión de la alarma temporalmente por el emisor del mensaje, de manera que la información de

supresión de la alarma no sea válida ya desde el comienzo de su generación, lo que implica el peligro de un acceso no autorizado no reconocible hasta que el técnico se ha presentado en el lugar. Por lo tanto, el emisor del mensaje puede indicar cuándo tiene intención de abrir la instalación de entrada, Además, el periodo de tiempo de validez puede estar limitado, en principio, por ejemplo por parte de la central de control para todos los mensaje a una longitud de tiempo determinada, por ejemplo de una a algunas horas. Además, el periodo de tiempo se puede establecer también a través del emisor del mensaje individualmente y para cada aplicación y con preferencia se puede comunicar al mismo tiempo con el mensaje a la central de control. En este caso, el emisor del mensaje puede seleccionar, por ejemplo, un periodo de tiempo de validez determinado a partir de un grupo de periodos de tiempo predeterminados fijamente, puede predeterminar un periodo de tiempo individualmente en función de la duración prevista de la aplicación o puede comunicar el instante del final esperado de los trabajos en la instalación de entrada. Con preferencia, el emisor del mensaje puede seleccionar a partir de una de las posibilidades mencionadas.

Como complemento a esta selección del emisor del mensaje se recomienda siempre prever una limitación temporal de la validez, para que e el caso de que el emisor del mensaje se olvide de seleccionar y comunicar el final del periodo de tiempo de la validez, no se produzca ningún fallo de la seguridad. En otra variante de realización de acuerdo con la invención, el final de la validez se puede comunicar también por el emisor del mensaje inmediatamente después de cerrar la instalación de entrada, para que se pueda conectar la alarma lo más rápidamente posible de nuevo nítidamente. De esta manera se anula precozmente la información de supresión de la alarma. Con la limitación de la duración de la validez se puede impedir que un intruso consiga entrada o acceso, después de la marcha del técnico, a la instalación de entrada.

A través de la limitación temporal de la validez se consigue que la información de supresión de la alarma solamente tenga validez mientras es absolutamente necesario y se reduce al mínimo el riesgo de la supresión de un mensaje de alarma, que ha sido depositado en virtud de una apertura no autorizada de la instalación de entrada.

De manera alternativa o acumulativa, el técnico de servicio puede enviar al comienzo de los trabajos en el lugar una información de supresión de la alarma con validez ilimitada en el tiempo, y puede anularla de nuevo al término de los trabajos a través de un segundo mensaje, en particular puede anular la información de supresión de la alarma precozmente en el caso de que no se haya alcanzado todavía la limitación temporal de la validez de la información de supresión de la alarma, pero ya han ocluido los trabajos en el lugar.

De acuerdo con el procedimiento según la invención, la información de supresión de la alarma se puede evacuar a continuación en una instalación de supervisión de la apertura, que está dispuesta con preferencia dentro de la central de control (OMC). Esta evaluación se realiza en el caso de un mensaje de alarma depositado por una instalación de entrada Este mensaje se compara con las informaciones de supresión de la alarma que han aparecido hasta ahora desde el servidor de mensajes, realizando un filtrado del mensaje de alarma en el caso de una asociación positiva.

En la comparación de un mensaje de alarma con las informaciones de supresión de la alarma se verifica si para la instalación de entrada depositaria del mensaje de alarma existe hasta el instante de la deposición o de la entrada del mensaje de alarma en la central de control una información válida de supresión de la alarma, es decir, que el mensaje de alarma ha aparecido dentro de la ventana de tiempo para la que se solicita, antes de la apertura de la instalación de entrada, una autorización y ha sido conseguida. Si éste es el caso, se lleva a cabo una asociación positiva del mensaje de alarma a la información de supresión de la alarma correspondiente. Esto expresa que en el proceso de apertura de la instalación de entrada se trata con alta probabilidad de una entrada o bien un acceso permitido, de manera que se puede suprimir el mensaje de alarma depositado.

Además, se propone un sistema, que está instalado para la realización del procedimiento de acuerdo con la invención y permite una determinación de una entrada y/o acceso permitido o no permitido a una instalación de entrada de una red de telecomunicaciones, en particular de una red de telefonía móvil, en una central de control que supervisa la instalación de entrada sobre la base de mensajes de alarma, que son depositados a través de la apertura de la instalación de entrada,

El sistema presenta, además: una instalación de entrada de una red de telefonía móvil, que está instalada para depositar al menos un mensaje de alarma en el caso de su apertura, un aparato de mensajes para la transmisión de un mensaje a un servidor de mensajes, una conexión de comunicaciones para la transmisión del mensaje, un servidor de mensajes, que está instalado para generar una información de supresión de la alarma, en función del mensaje así como una supervisión de la apertura para la evaluación de mensajes de alarma y de informaciones de supresión de la alarma, que está instalada para comparar, en el caso de que se reciba un mensaje de alarma, este mensaje con las informaciones de supresión de la alarma y, en el caso de una asociación positiva, filtrar el mensaje de alarma depositado.

Puesto que el sistema está instalado para la realización del procedimiento de acuerdo con la invención, dispone de las mismas características que ya se han explicado con relación al procedimiento. Así, por ejemplo, el aparato de

mensajes puede ser un terminal móvil para la telefonía móvil, en particular un teléfono móvil, Smartphone o una tarjeta de datos de telefonía móvil de un ordenador portátil. Además, la conexión de comunicación entre el terminal de mensajes y el servidor de mensaje puede estar asegurada, es decir que puede estar protegida al menos contra escucha, modificación del contenido y repetición de los datos.

Hay que indicar que por un servidor de mensajes en el sentido de esta invención se entiende cualquier instalación técnica, que está instalada para recibir un mensaje y para generar una información de supresión de la alarma. El servidor de mensajes puede formar parte de la supervisión de la apertura de la central de control. No obstante, en una variante de realización alternativa, también puede estar configurado independiente de ésta, por ejemplo como servidor central, desde el que se emiten informaciones de supresión de la alarma, respectivamente, hacia una central de control que supervisa la instalación de entrada identificada en el mensaje.

El servidor de mensajes puede presentar una instalación para la verificación, en particular para la autentificación y/o autorización. Esta autentificación y/o autorización se pueden realizar de acuerdo con las etapas del procedimiento ya descritas.

El procedimiento está previsto especialmente para la utilización para la protección de redes de telefonía móvil, de manera que las instalaciones de entrada representan en este caso especialmente estaciones de base de la red de telefonía móvil. No obstante, de manera alternativa, también se puede utilizar para cualquier red de telecomunicaciones discrecional, por ejemplo redes de datos de alta velocidad para DSL, que presentan puntos de acceso sensibles y que requieren protección, por ejemplo DSLAMs.

Opcionalmente, el sistema puede presentar también una base de datos, que está conectada con el servidor de mensajes o con la supervisión de la apertura y contiene planea de servicio sobre la entrada y/o acceso a las instalaciones de entrada. Estos planes de servicio se pueden tener en cuenta en la verificación.

Otras ventajas y configuraciones preferidas de la invención se pueden deducir de las reivindicaciones dependientes.

A continuación se explica la invención con la ayuda de un ejemplo de realización concreto.

En la práctica, es necesario realizar regularmente trabajos de mantenimiento y en casos de avería so en casos de fallos trabajos de reparación en instalaciones de entrada de una red de telecomunicaciones. En el ejemplo siguiente se hace referencia a una estación de base BS-AN (Base-Station Access Net) de una red de telefonía móvil y se describe el procedimiento con la ayuda de esta instalación de entrada ejemplar y de la red de telecomunicaciones ejemplar.

Si es necesario que un técnico deba crear acceso o entrada a una BS-AN, designado en general como apertura de la BS-AN, lo notifica a la central de supervisión y control competente para la supervisión d la BS-AN (plataforma OMC). Esto se puede realizar también a corto plano, es decir, mientras el técnico se encuentra ya en camino hacia un lugar de aplicación, no siendo posible en este caso una introducción de la aplicación en un plan de servicio.

El mensaje se realiza con preferencia en forma de un mensaje corto electrónico (SMS), un mensaje de voz o también en forma de un formulario de la Web, que el técnico deposita con la ayuda de un teléfono móvil o desde un ordenador portátil, que puede establecer por medio de tarjeta de datos de telefonía móvil una comunicación segura con una red de telefonía móvil.

El mensaje es transmitido codificado en este caso con preferencia a través de una conexión de comunicaciones segura hacia un servidor de mensajes, que puede generar una información de supresión de la alarma y contiene al menos informaciones sobre la identidad del técnico y de la BS-AN a abrir. Esta última se puede identificar, por ejemplo, de una manera unívoca a través de una identificación especial. Para la identificación del emisor del mensaje éste puede utilizar un PIN o MSISDN determinado, que es indicado especialmente en el mensaje. Tal número o tal código de identificación se puede enviar también de forma automática con el mensaje a través de la tarjeta SIM o UICC del Terminal de telefonía móvil como instalación de identificación, con lo que el terminal de telefonía móvil está identificado en la red de telefonía móvil y, por lo tanto, indirectamente el técnico es identificado de una manera unívoca.

Además, el técnico puede indicar adicionalmente cuándo comenzará con sus trabajos, es decir, cuándo debe ser válida una información de supresión de la alarma generada. Además, se puede indicar adicionalmente cuánto durarán sus trabajos, que pueden comprender eventualmente varias aperturas y cierres. Esto se puede realizar a través de la indicación de una duración de tiempo de los trabajos, por ejemplo 25 minutos o a través de la indicación de un instante concreto, en el que han concluido los trabajos, por ejemplo 15:15 horas. Además, se puede realizar también una selección desde un grupo de intervalos de tiempo fijos de validez, por ejemplo 30 minutos, 60 ó 90 minutos, etc., que el técnico indica en el mensaje. El mensaje se puede realizar, por ejemplo, desde una célula de telefonía cercada, cuando una BS-AN determinada está defectuosa o no existe en el lugar ningún suministro de telefonía móvil. Una información de supresión de la alarma generada por el servidor de mensajes es limitada en el

tiempo de esta manera en su validez.

El servidor de mensajes, que es con preferencia una unidad independiente de una supervisión de la apertura en el OMC, está conectado, sin embargo, para la actuación sobre ésta con la supervisión de la apertura, y lleva a cabo una verificación después de la recepción del mensaje. En otra variante de realización, el servidor de mensajes puede formar parte también de la supervisión de la apertura. La verificación comprende una autentificación del emisor del mensaje con la ayuda del número de identificación (PIN) transmitido o identificación de tarjetas SIM o bien identificación UICC y con la ayuda de la BS-AB a abrir con la ayuda de su identificación. Se determina si es posible una identificación del emisor del mensaje con un técnico. Si se puede asociar el número de identificación o la identificación de tarjetas SIM o bien la identificación UICC a un técnico, y se puede asociar, además, la identificación de la BS-AN a una estación de base existente, que es supervisada realmente por el OMC llamado, entonces el resultado de la autentificación es positivo.

A la autentificación se conecta como etapa siguiente del procedimiento una autorización, que se representa en la entrada de la identidad del emisor del mensaje, por ejemplo en forma de su MSISDN y, por lo tanto, del acceso autorizado en una Tabla. En el marco de la autorización se puede verificar adicionalmente si el técnico posee la autorización de entrada o la fase de seguridad necesarias para la apertura de la BS-AN deseada y/o si la BS-AN está liberada, en principio, para una apertura.

Para completar, en la verificación, es decir, en la autentificación o autorización para la verificación de la factibilidad e puede realizar una comparación del mensaje con planes de servicio sobre las aplicaciones del técnico, que son proporcionadas por una base de dato conectada con el servidor de servicios o en el caso de que el servidor de servicios forme parte de la supervisión de la apertura, con la supervisión de la apertura. De esta manera se puede verificar si el técnico, que quiere abrir una BS-AN, estará en servicio realmente en el instante correspondiente o si existe en el mensaje un intento de engaño.

Si la verificación es positiva, es decir, si se ha podido realizar tanto una asociación de la identidad anunciada del emisor del mensaje a un técnico, como también una asociación de la identificación de la BS-AN a una estación de base supervisada por el OMC competente, así como e ha podido llevar a cabo una autorización, dado el caso, después de la consideración de la verificación de la factibilidad, el servidor de mensajes genera una información de supresión de la alarga, que posee validez en la ventana de tiempo indicada por el técnico, seleccionada o establecida en las condiciones de sistema.

Cada información de supresión de la alarma es conducida a una supervisión de apertura del OMC competente para la supervisión de la BS-AN. Esta supervisión de la apertura recibe mensajes desde todas las BS-AN supervisadas en el caso de su apertura y los evalúa teniendo en cuenta las informaciones de supresión de la alarma existentes. Esta evaluación se realiza comparando un mensaje de alarma entrante con la información de supresión de la alarma que está presente para la BS-AN, que ha depositado el mensaje de alarma. Si existe una información de supresión de la alarma, que está correlacionada con el instante de la deposición o de la recepción del mensaje de alarma y ésta posee ya o todavía validez en el instante mencionado, entonces existe en la BS-AN un proceso de apertura autorizado y se puede suprimir o bien ignorar el mensaje de alarma.

Por lo tanto, si la verificación de si en el instante de un mensaje de alarma de una BS-AN existe una información de supresión de la alarma válida, conduce al resultado de que se puede asociar al mensaje de alarma una información de supresión de la alarma válida, lo que se designa en el sentido de la invención como asociación positiva, entonces se puede suprimir o filtrar el mensaje de alarma desde la supervisión de la apertura, puesto que se establece con suficiente seguridad que existe una apertura autorizada de la BS-AN. Por lo tanto, la supervisión de la apertura se puede designar también como filtro de alarma.

En otra variante de realización, la supervisión de la apertura puede enviar también informaciones, por ejemplo, sobre mensajes de alarma o informaciones de supresión de la alarma entrantes a un OMC central. De manera alternativa, el servidor de mensajes puede transmitir las informaciones de supresión de la alarma también al OMC central, que las gestiona de forma centralizada e informa a la plataforma OMC competente.

REIVINDICACIONES

1.- Procedimiento para la determinación de una apertura permitida o no permitida de una instalación de entrada de una red de telecomunicaciones, en particular de una red de telefonía móvil o de una red fija, en una central de control que supervisa la instalación de entrada sobre la base de mensajes de alarma, que son depositados a través de la apertura de la instalación de entrada, caracterizado porque en cada caso antes de la apertura de la instalación de entrada se transmite por medio de un aparato de alarma un mensaje a un servidor de mensajes, que puede generar una información de supresión de la alarma, que puede ser evaluada en la central de control, comparando en el caso de que se recibe un mensaje de alarma, este mensaje con las informaciones de supresión de la alarma y llevando a cabo, en el caso de una asociación positiva, un filtrado del mensaje de alarma.

2.- Procedimiento de acuerdo con la reivindicación 1, caracterizado porque como aparato de mensajes se utiliza un terminal móvil para la telefonía móvil, en particular un teléfono móvil, Smartphone o una tarjeta de datos de telefonía móvil de un ordenador portátil.

3.- Procedimiento de acuerdo con la reivindicación 1 ó 2, caracterizado porque la instalación de entrada es una estación de base de una red de telefonía móvil.

4.- Procedimiento de acuerdo con la reivindicación 1, 2 ó 3, caracterizado porque la transmisión del mensaje se realiza a través de una conexión segura.

5.- Procedimiento de acuerdo con una de las reivindicaciones anteriores, caracterizado porque el mensaje contiene al menos informaciones sobre la identidad del emisor del mensaje y la identidad de la instalación de entrada.

6.- Procedimiento de acuerdo con una de las reivindicaciones anteriores, caracterizado porque el mensaje se realiza el forma de n mensaje electrónico, en particular Email, o en forma de una mensaje corto electrónico (SMS), de una comunicación de voz o de un formulario de la Web.

7.- Procedimiento de acuerdo con una de las reivindicaciones anteriores, caracterizado porque la información de supresión de la alarma se genera en función del mensaje, en particular solamente después de la verificación positiva del mensaje.

8.- Procedimiento de acuerdo con la reivindicación 7, caracterizado porque la verificación comprende una autentificación del emisor del mensaje y/o de la instalación de acceso.

9.- Procedimiento de acuerdo con una de las reivindicaciones 7 u 8, caracterizado porque la verificación comprende una autorización del emisor del mensaje.

10.- Procedimiento de acuerdo con una de las reivindicaciones anteriores, caracterizado porque en la autorización para la verificación de la factibilidad se tienen en cuenta informaciones del plan de servicio.

11.- Procedimiento de acuerdo con una de las reivindicaciones anteriores, caracterizado porque la información de supresión de la alarma posee una validez limitada en el tiempo.

12.- Procedimiento de acuerdo con la reivindicación 11, caracterizado porque el comienzo de la validez se puede determinar por el emisor del mensaje.

13.- Procedimiento de acuerdo con la reivindicación 11 ó 12, caracterizado porque el final de la validez está fijada o se puede establecer por el emisor del mensaje.

14.- Procedimiento de acuerdo con la reivindicación 13, caracterizado porque el final de la validez se puede establecer individualmente a través de la indicación de su duración temporal y/o a través de la indicación del instante de la terminación de la validez por el emisor del mensaje y se comunica con el mensaje y/o porque el final de la validez se comunica por el emisor del mensaje inmediatamente después del cierre de la instalación de entrada.

15.- Procedimiento de acuerdo con la reivindicación 14, caracterizado porque se puede seleccionar al menos entre la indicación del instante de la terminación de la validez y la indicación de una duración temporal de la validez.

16.- Procedimiento de acuerdo con una de las reivindicaciones anteriores, caracterizado porque durante la comparación de un mensaje de alarma con las informaciones transmitidas de supresión de la alarma se verifica si existe para la instalación de entrada, en el instante de la deposición o de la recepción del mensaje de alarma una información válida para la supresión de la alarma, realizando, en el caso de la presencia de una información válida de la supresión de la alarma, una asociación positiva del mensaje de alarma a la información de supresión de la alarma.

17.- Sistema para la determinación de una apertura permitida o no permitida de una instalación de entrada de una red de telecomunicaciones, en particular de una red de telefonía móvil, en una central de control que supervisa la

instalación de entrada sobre la base de mensajes de alarma, que son depositados a través de la apertura de la instalación de entrada, caracterizado por

- una instalación de entrada de una red de telefonía móvil, que está instalada para depositar al menos un mensaje de alarma en el caso de su apertura,

- un aparato de mensajes para la transmisión de un mensaje a un servidor de mensajes,

- una conexión de comunicaciones para la transmisión del mensaje,

- un servidor de mensajes, que está instalado para generar una información de supresión de la alarma,

- una supervisión de la apertura para la evaluación de mensajes de alarma y de informaciones de supresión de la alarma, que está instalada para comparar, en el caso de que se reciba un mensaje de alarma, este mensaje con las informaciones de supresión de la alarma y, en el caso de una asociación positiva, filtrar el mensaje de alarma depositado.

18.- Sistema de acuerdo con la reivindicación 17, caracterizado porque el aparato de mensajes es un terminal móvil para telefonía móvil, en particular un teléfono móvil, Smartphone o una tarjeta de datos de telefonía móvil de un ordenador portátil.

19.- Sistema de acuerdo con la reivindicación 17 ó 18, caracterizado porque el servidor de mensajes forma parte de la supervisión de la apertura.

20.- Sistema de acuerdo con una de las reivindicaciones 17 a 19, caracterizado porque el servidor de mensajes presenta una instalación para la autentificación y/o autorización del emisor del mensaje.

21.- Sistema de acuerdo con una de las reivindicaciones 17 a 20, caracterizado porque la instalación de entrada es una estación de base de una red de telefonía móvil.

22.- Sistema de acuerdo con una de las reivindicaciones 17 a 21, caracterizado por una base de datos, que está conectada con el servidor de mensajes o con la supervisión de apertura y que contiene planes de servicio sobre la entrada y/o acceso a las instalaciones de entrada.