



19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA

11 Número de publicación: **2 328 708**

51 Int. Cl.:  
**H04W 12/08** (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Número de solicitud europea: **05109197 .3**

96 Fecha de presentación : **04.10.2005**

97 Número de publicación de la solicitud: **1773078**

97 Fecha de publicación de la solicitud: **11.04.2007**

54 Título: **Procedimiento para adaptar los reglajes de seguridad de una estación de comunicaciones y estación de comunicaciones.**

45 Fecha de publicación de la mención BOPI:  
**17.11.2009**

45 Fecha de la publicación del folleto de la patente:  
**17.11.2009**

73 Titular/es: **Swisscom AG.**  
**Alte Tiefenastrasse 6**  
**3050 Bern, CH**

72 Inventor/es: **Cantini, Renato y**  
**Aebi, Paul**

74 Agente: **Sugrañes Moliné, Pedro**

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 para adaptar los reglajes de seguridad de una estación de comunicaciones y estación de comunicaciones.

### **Campo técnico de la invención**

La presente invención se refiere a un procedimiento para adaptar los parámetros de seguridad de una estación de comunicaciones que comprende un puesto de trabajo y un terminal móvil provisto de un módulo de identificación, y a una estación de comunicaciones de acuerdo con las reivindicaciones independientes.

### **Descripción de la técnica relacionada**

En la técnica anterior, se describen diferentes mecanismos de control de acceso para, por ejemplo, regular el control de acceso de una aplicación a unos datos o a un dispositivo, en los documentos WO-A1-00/67212, US-A-5.517.014 o US-B1-6.216.014.

Además, el documento US-A1-2004/172370 se refiere a reglas de acceso de cumplimiento de sujetos con objetos con una política de seguridad predeterminada en una tarjeta inteligente. Cada regla de acceso define el derecho de un sujeto a llevar a cabo una acción sobre un objeto. La política de seguridad define las reglas de seguridad para el acceso de los sujetos a los objetos. Para una operación relacionada con un objeto dado, se compara con las reglas de seguridad al menos una regla de acceso relacionada con el objeto dado para aceptar la operación cuando la regla de acceso cumpla con todas las reglas de seguridad; en caso contrario, no se acepta la operación. Una operación puede ser la carga de un objeto tal como una aplicación, una modificación de las reglas de acceso, la supresión o adición de un sujeto, o una solicitud de acceso a un objeto dado por parte de un sujeto o grupo de sujetos.

En el documento EP-A1-11475978, se describen los detalles de un aparato y un procedimiento para gestionar procesos simultáneos de control de recursos de radio de la red de acceso a radio terrestre universal (UTRAN) que cambian la configuración de seguridad en el equipo de un usuario del sistema universal de telecomunicaciones móviles (UMTS). De acuerdo con un aspecto de la descripción, se proporciona un aparato que constituye un equipo de usuario que posee un gestor de mensajes, un procesador secuencial, una memoria de instrucciones, y un detector de cambios en la configuración de seguridad. Dicho gestor de mensajes está conectado con dicha memoria de instrucciones, con dicho procesador secuencial, y con dicho detector de cambios en la configuración de seguridad para guardar, procesar y detectar respectivamente los cambios en la configuración en instrucciones, y para determinar si existe alguna instrucción en el equipo del usuario, de tal modo que, para la UTRAN, parezca que el equipo del usuario procesa instrucciones de forma simultánea. De acuerdo con otro aspecto, se proporciona un procedimiento para procesar instrucciones simultáneas en el equipo de un usuario que posea una configuración de seguridad, que incluye las siguientes etapas: determinación de si existe alguna instrucción en el equipo del usuario; tras recibir una instrucción recibida: suspensión del procesamiento de instrucciones existente; determinación de si las instrucciones contienen algún cambio en la configuración de seguridad; y rechazo de la instrucción recibida o conservación de la instrucción recibida antes de retomar la instrucción existente; de tal modo que, para la UTRAN, parezca que el equipo del usuario procesa instrucciones de forma simultánea.

El documento EP-A1-1478196 se refiere a un módulo y un procedimiento para detectar al menos un evento en un equipo de abonado de telefonía celular móvil, que se basa en detectar el momento en que una tarjeta se pone en contacto operativo con el terminal de teléfono móvil, si el código que identifica al terminal o la tarjeta es el mismo que el código correspondiente leído en una ocasión anterior. Si no es el mismo, se entiende que se ha producido un cambio de terminal o un cambio de tarjeta, o que el terminal o la tarjeta han sido usados por primera vez, y se genera y envía un mensaje correspondiente. El código que identifica el terminal puede ser el IMEI, y el código que identifica la tarjeta puede ser el IMSI y/o el ICC-ID.

El documento WO-A1-01/08435 se refiere a un procedimiento y unos dispositivos, relacionados con el mismo, para configurar el nivel de seguridad de las funciones de cifrado usadas en los terminales de comunicaciones. En un teléfono móvil, se reciben de forma segura parámetros de situación tales como el código de identificación de un país en el que se encuentre situado temporalmente el terminal de telecomunicaciones, desde una fuente segura y a través de una red de telefonía móvil. Además, en dicha red de telecomunicaciones se determinan parámetros de seguridad tales como la máxima longitud aceptable (en bits) de las claves de cifrado, basándose en los parámetros de situación recibidos; y dichos parámetros de seguridad son usados por las funciones de cifrado y determinan el nivel de seguridad.

En la técnica anterior, en condiciones normales, la tarjeta SIM de una estación móvil no detecta que se produzca cambio alguno en el hardware o el software del terminal móvil o de un ordenador conectado al terminal móvil. Pueden producirse cambios en la conectividad de la red o en el estado de bloqueo del ordenador sin que la tarjeta SIM reciba la información. Por lo tanto, el terminal móvil y/o el ordenador asociado suele implantar sus propios mecanismos de seguridad, que son totalmente independientes de la tarjeta SIM. Esto puede ser perjudicial, ya que las aplicaciones ejecutadas en la tarjeta SIM pueden exponer las credenciales confidenciales a un entorno de ejecución externa. Por lo tanto, podría ser conveniente disponer de una tarjeta SIM capaz de imponer una política de seguridad. Además, es posible que el operador de red que expide la tarjeta SIM desee que sus abonados se vean obligados a respetar ciertos mecanismos de seguridad, o que ofrezca a los usuarios una manera más sencilla de utilizar su estación de comunicaciones de forma segura.

## Breve resumen de la invención

Un objetivo de la presente invención es crear un procedimiento para adaptar los parámetros de seguridad de una estación de comunicaciones que comprende un terminal móvil provisto de un módulo de identificación y crear una estación de comunicaciones y un módulo de identificación correspondientes.

Otro objetivo de la invención es adaptar los parámetros de seguridad de un módulo de identificación, tal como una tarjeta SIM, a eventos externos, es decir, eventos que se producen fuera de la tarjeta SIM.

De acuerdo con la invención, estos objetivos se logran mediante un procedimiento para adaptar los parámetros de seguridad de una estación de comunicaciones dependiendo de un evento que afecta a la seguridad de acuerdo con el preámbulo de la reivindicación 1, en la que dichos parámetros de seguridad, que se definen en el registro de seguridad, se usan para limitar el derecho o los derechos de una sola aplicación, un grupo de aplicaciones o todas las aplicaciones ejecutadas por dicha estación de comunicaciones o terminal móvil, incluida la restricción de acceso a aplicaciones incluidas en dicho módulo de identificación por parte de otros componentes de dicha estación de comunicaciones.

De acuerdo con la invención, estos objetivos también se logran mediante una estación de comunicaciones que comprende un terminal móvil provisto de un módulo de identificación de acuerdo con el preámbulo de la reivindicación 25, en el que dichos parámetros de seguridad, que se definen en el registro de seguridad, se usan para limitar el derecho o los derechos de una aplicación, un grupo de aplicaciones o todas las aplicaciones ejecutadas por dicha estación de comunicaciones o terminal móvil, incluida la restricción de acceso a aplicaciones en dicho módulo de identificación por parte de otros componentes de dicha estación de comunicaciones.

De acuerdo con la presente invención, un “evento que afecta a la seguridad” comprende una o una pluralidad de las siguientes acciones, llevadas a cabo por el usuario o por cualquier aplicación: cambio en la configuración del hardware de dicha estación de comunicaciones o terminal móvil, conexión de dicha estación de comunicaciones o terminal móvil a una red o sistema externo, evento generado por una aplicación ejecutada por dicha estación de comunicaciones o terminal móvil y evento transmitido de forma inalámbrica a dicha estación de comunicaciones. Éstas son algunas de las posibles acciones: creación, liberación, pérdida y cierre de canales de acceso desde y hacia la estación de comunicaciones, bloqueo o desbloqueo del estado de la estación de trabajo, retirada o instalación de componentes de hardware o software, inicio automático desde un dispositivo y detección de contenidos, tráfico, modificaciones, etc., malintencionados o que resulten sospechosos. Por supuesto, esta lista no incluye todos los eventos posibles; se presenta simplemente con fines ilustrativos y la invención no se limita en modo alguno a estos ejemplos. Se podría usar cualquier otro evento que pudiera resultar dañino o de relevancia para el usuario, la estación de comunicaciones o el terminal móvil. También se podría tener en cuenta un acceso a Internet adicional o acceso WLAN en un punto de acceso inalámbrico (*hot spot*), tal como se menciona anteriormente. Dicho evento podría incluir la actividad de un software antivirus, un firewall existente y/o una puerta de enlace IPSec. También se podrían tener en cuenta el estado de la sesión del usuario y/o el estado de un canal de conexión que implica dicho estado de comunicación.

Un evento se identifica mediante un gestor de eventos, que podría incorporarse en la estación de comunicaciones y/o el terminal móvil. La etapa de identificación de un evento que afecta a la seguridad se lleva a cabo preferentemente con uno o una pluralidad de los campos obligatorios tales como: identificador de evento, tipo de evento, fecha y hora y/o número de secuencia y campos opcionales tales como nivel crítico del evento o información adicional específica para el tipo de evento. Después de haberse identificado un evento y almacenado el evento en un registro de eventos, también se actualiza preferentemente un registro de seguridad. El registro de seguridad define todos los parámetros de seguridad de la estación de comunicaciones y para el terminal móvil. Los parámetros de seguridad también determinan preferentemente los requisitos de autenticación para una aplicación ejecutada por dicho módulo de identificación y/o dicho terminal móvil. Dichos parámetros de seguridad, que se definen en el registro de seguridad, se usan para limitar el derecho o los derechos de una sola o de la totalidad de las aplicaciones ejecutadas por dicha estación de comunicaciones o terminal móvil.

En una forma de realización ventajosa, la estación de comunicaciones comprende un ordenador y una estación móvil. La estación móvil comprende a su vez un terminal móvil, por ejemplo un teléfono celular o una tarjeta de acceso a una red celular, y un módulo de identificación, por ejemplo una tarjeta SIM. De este modo, el procedimiento de la invención comprende una etapa de adaptación de los mecanismos de seguridad usados por el ordenador y/o por el terminal móvil mediante la consulta de un registro de seguridad existente en el módulo de identificación, con el fin de determinar el nivel de seguridad que corresponda.

El módulo de identificación (por ejemplo, una tarjeta SIM) puede estar provisto de un gestor de eventos, registro de eventos y registro de seguridad compartidos, pero también es posible proporcionar un gestor de eventos y un registro de eventos compartidos y destinar un único registro de seguridad para una aplicación o un grupo de aplicaciones. La invención también es factible con un gestor de eventos compartido y un único registro de eventos y registro de seguridad para una aplicación o grupo de aplicaciones y con un único gestor de eventos, registro de eventos y registro de seguridad para una aplicación o grupo de aplicaciones.

La ventaja obtenida con la presente invención reside en que proporciona un equilibrio aceptable entre los requisitos de seguridad y la facilidad de uso y ausencia de interrupciones que se exige. Por ejemplo, la obtención de un acceso adecuado a credenciales y funciones confidenciales en el módulo de identificación y de un uso adecuado de las mismas

podría depender de que se produzcan eventos específicos en el entorno de ejecución externa. Los mecanismos de control de acceso del módulo de identificación se adaptarán a estos eventos específicos siguiendo una política de seguridad pertinente definida y almacenada en el módulo de identificación y recuperada desde el mismo.

- 5 De este modo, el procedimiento de la invención limita el acceso a aplicaciones del módulo de identificación por parte del entorno externo, dependiendo del registro de seguridad.

## Breve descripción de los dibujos

- 10 La invención se entenderá mejor con la ayuda de la descripción de una forma de realización, incluida a modo de ejemplo e ilustrada por las figuras, en las que:

la fig. 1a muestra una primera forma de realización de un sistema integral de comunicaciones, que ilustra una forma de realización de la presente invención;

15 la fig. 1b muestra una segunda forma de realización de un sistema integral de comunicaciones, que ilustra una forma de realización de la presente invención;

20 la fig. 1c muestra una tercera forma de realización de un sistema integral de comunicaciones, que ilustra una forma de realización de la presente invención;

la fig. 2 muestra la estructura de un módulo de identificación de acuerdo con la presente invención;

25 la fig. 3 ilustra un ejemplo de la invención de la autenticación para túneles VPN;

la fig. 4 ilustra una primera forma de realización de la invención con un gestor de eventos, registro de eventos y registro de seguridad compartidos dentro de la tarjeta SIM para todas las aplicaciones de la tarjeta SIM;

30 la fig. 5 ilustra una segunda forma de realización de la invención con un gestor de eventos y registro de eventos compartidos y un único registro de seguridad para una aplicación de la tarjeta SIM;

la fig. 6 ilustra una tercera forma de realización de la invención con un gestor de eventos compartido y un único registro de seguridad y registro de eventos para una aplicación de la tarjeta SIM; y

35 la fig. 7 ilustra una cuarta forma de realización de la invención con un único gestor de eventos, registro de seguridad y registro de eventos para una aplicación de la tarjeta SIM.

## Descripción detallada de posibles formas de realización de la invención

- 40 Haciendo referencia en primer lugar a la fig. 1a, un sistema de comunicaciones, que se indica generalmente con el número 10, permite la comunicación de datos entre una estación de comunicaciones 12 y una red IP 14. En la solicitud de patente publicada WO-A1-01/60013 se da a conocer un sistema de comunicaciones de este tipo. La red IP 14 puede tratarse de una intranet privada a la cual se permite el acceso de forma selectiva, o cualquier otro tipo de red de comunicación de datos privados. Cuando la estación de comunicaciones 12 cuenta con el permiso para acceder a la red 14, se pueden comunicar datos entre las mismas. Además, entre la estación de comunicaciones 12 y la red 45 14, se puede establecer una red privada virtual como la que se da a conocer detalladamente en el documento WO-A1-01/60013.

En la forma de realización ejemplar que se ilustra en las figs. 1a a 1c, el sistema de comunicaciones 10 comprende una red de acceso inalámbrico, por ejemplo una red GSM (sistema global para comunicaciones móviles), a la cual está conectada la red IP 14. En otras formas de realización, el sistema de comunicaciones 10 puede comprender, como alternativa, otra estructura tal como una WLAN, UMTS, GPRS, EDGE o cualquier otra red de comunicaciones conocida.

- 55 La estación de comunicaciones 12 incluye un transceptor de radio, por ejemplo una estación móvil tal como un teléfono móvil convencional. La estación móvil comprende un terminal móvil 16, en este caso un equipo GSM, WLAN, GPRS, EDGE o UMTS, y un módulo de identificación 18, en este caso una tarjeta SIM (módulo de identidad del abonado), que se introduce en el terminal móvil 16 o se conecta al mismo de cualquier otro modo. Se puede usar otro tipo de módulos de identificación, incluido el USIM utilizado en las redes UMTS, o módulos de identificación 60 virtual, que comprenden únicamente componentes de software.

El módulo de identificación incluye una posición de almacenamiento 20 para almacenar información de autenticación del abonado para autenticar el módulo incorporado en el sistema de comunicación celular 22, de forma convencional. El módulo de identificación puede incluir además una posición de almacenamiento para almacenar la 65 dirección de la red IP privada 14.

En la forma de realización de la fig. 1a, la estación móvil 16 está conectada a un ordenador 13 mediante un enlace por cable o inalámbrico, por ejemplo a través de un conector de infrarrojos, por medio de Bluetooth, ZigBee,

NFC, HomeRF o cualquier otro medio adecuado. El ordenador puede ser un ordenador personal portátil en el que se ejecute un cliente de Internet, por ejemplo un navegador web, el correo electrónico de un cliente, etc. En la forma de realización de la fig. 1b, el terminal móvil 16 consiste en una tarjeta extraíble, como por ejemplo una tarjeta PC Card, introducida en una ranura adecuada del ordenador 13, introduciéndose el propio módulo de identificación en la tarjeta extraíble.

En la forma de realización de acuerdo con la fig. 1c, el terminal móvil 16 y el ordenador 13 están integrados, formando un único aparato, por ejemplo un “teléfono inteligente” o una PDA con un interfaz para una red celular. El módulo de identificación se introducirá directamente en este equipo.

El ordenador 13 también se puede conectar directamente a Internet 15 a través de un enlace, que no se ilustra, por ejemplo un módem, una tarjeta de red, un “router”, etc., independiente de la estación móvil 16.

En la forma de realización en la que ciertas partes del sistema de comunicaciones 10 están formadas a partir de una estructura de un sistema de comunicaciones GSM, tal estructura, así como la interfaz aérea formada entre la estación de comunicaciones remota 12 y la red IP privada 14, están definidas por las normas del sistema GSM.

Cuando se encuentra en funcionamiento, en el momento en que un usuario del ordenador desee acceder a la red IP privada 14, se generan las instrucciones apropiadas para iniciar una solicitud de acceso a la red IP privada 14 a través de la red celular 22.

De acuerdo con la presente invención, la política de control de acceso, definida por los parámetros de seguridad, de la estación de comunicaciones 12 depende de los eventos que afectan a la seguridad que se hayan identificado, gestionado y/o recuperado en el módulo de identificación 18. En particular, el acceso mediante el ordenador 13 y/o el terminal móvil 16 a ciertos datos, tales como credenciales o aplicaciones del módulo de identificación 18, depende de dichos eventos que afectan a la seguridad, almacenados en un registro de seguridad del módulo de identificación.

En la fig. 2, se muestra de forma esquemática el módulo de identificación 18 de la invención, que comprende, además de los elementos convencionales, un gestor de eventos 26, un registro de eventos 28 y un registro de seguridad 30.

De acuerdo con la invención, el gestor de eventos 26 del módulo de identificación 18 reconoce los eventos que afectan a la seguridad. De acuerdo con la presente invención, un “evento que afecta a la seguridad” comprende una o una pluralidad de las siguientes acciones, llevadas a cabo por el usuario o cualquier aplicación: cambio en la configuración de hardware de dicha estación de comunicaciones 12 o terminal móvil 16, conexión de dicha estación de comunicaciones 12 o terminal móvil 16 a una red o sistema externo, evento generado por una aplicación ejecutada por dicha estación de comunicaciones 12 o terminal móvil 16 y evento transmitido de forma inalámbrica a dicha estación de comunicaciones 12. Algunas de las posibles acciones son: la creación, liberación, pérdida o cierre de canales de acceso desde y hacia la estación de comunicaciones 12 (por ejemplo, túnel VPN IPSec), bloqueo o desbloqueo del estado de la estación de trabajo 12, retirada o instalación de componentes de hardware o software (nuevas interfaces o periféricos de red/conectividad, nuevos controladores o aplicaciones de red/conectividad), inicio automático desde un dispositivo (CD-ROM, DVD, USB, etc.) y detección de contenidos (software antivirus), tráfico (el firewall existente), modificaciones (sistema de detección de intrusos HIDS), etc., malintencionados o que resulten sospechosos. Por supuesto, esta lista no incluye todos los eventos posibles; se presenta simplemente con fines ilustrativos y la invención no se limita en modo alguno a estos ejemplos. Se podría usar cualquier otro evento que pudiera resultar dañino o de relevancia para el usuario, la estación de comunicaciones 12 o el terminal móvil 16. También se podría tener en cuenta un acceso a Internet 15 adicional o acceso WLAN en un hot spot, tal como se menciona anteriormente. También se podrían tener en cuenta el estado de la sesión del usuario y/o el estado de un canal de conexión que implica dicho estado de comunicación.

El evento podría ser relevante para la estación de comunicaciones 12 y para el terminal móvil 16 o sólo para uno de dichos dispositivos. Además, se puede usar la política de seguridad para definir restricciones para aplicaciones de la estación de comunicaciones 12 y/o el terminal móvil 16.

El evento se podría identificar mediante un gestor de eventos 27 situado en el terminal móvil, que se podría proporcionar además del gestor de eventos 26 contenido en el módulo de identificación 18 de la estación de comunicaciones 12 (figura 4), o en su sustitución. En esta forma de realización, el gestor de eventos 27 de la estación de comunicaciones notificará el evento al gestor de eventos 26 del módulo de identificación. Los eventos que afectan a la seguridad se identifican preferentemente con uno o una pluralidad de los campos obligatorios tales como identificador de eventos, tipo de evento, fecha y hora y/o número de secuencia y campos opcionales tales como nivel crítico del evento o información adicional específica para el tipo de evento.

Después de haberse identificado un evento y almacenado el evento en un registro de eventos 28, también se actualiza preferentemente un registro de seguridad 30. El registro de seguridad 30 define todos los parámetros de seguridad de la estación de comunicaciones 12 y/o el terminal móvil 16. Los parámetros de seguridad también determinan preferentemente los requisitos de autenticación para aplicaciones ejecutadas por dicho módulo de identificación 18, por dicho terminal móvil 16 y/o por el ordenador 13. Dichos parámetros de seguridad, que se definen en el registro de seguridad 30, se usan para limitar el derecho o los derechos de una sola, un grupo o la totalidad de las aplicaciones ejecutadas

por dicha estación de comunicaciones 12 o terminal móvil 16, especialmente el derecho a acceder a alguna parte o funcionalidades del módulo de identificación. Cuando se desconecta la estación de comunicaciones 12, los parámetros de seguridad se pueden almacenar y se volverán a usar cuando se vuelva a conectar la estación de comunicaciones 12.

Para comprender mejor la presente invención, las figs. 3 a 7 ilustran diferentes ejemplos de la invención y diferentes formas de realización para materializar la presente invención.

A este respecto, la fig. 3 ilustra un procedimiento para establecer túneles de red privada virtual (VPN) simultáneos, al tiempo que se lleva a cabo una autenticación sólida y sin interrupciones, usando el procedimiento de la invención. En este ejemplo, un usuario inicia una aplicación de cliente (etapa 100) con el fin de establecer un canal de comunicación seguro, por una VPN a través de Internet, con una red remota.

Cuando se abre un primer túnel VPN, este evento es identificado (etapa 110) por el gestor de eventos 26 incorporado en el módulo de identificación (o posiblemente en el terminal móvil o en el ordenador). Después, el evento es almacenado en el registro de eventos 28 (etapa 120). De acuerdo con el procedimiento de la invención, el registro de seguridad 30 existente en el módulo de identificación 18 recibe la notificación (etapa 130) y se actualiza (etapa 140) de acuerdo con el evento identificado (inicio del primer túnel VPN). Los mecanismos de seguridad o parámetros de seguridad de toda la estación de comunicaciones 12 y/o el terminal móvil 16 dependerán del registro de seguridad 30 existente en el módulo de identificación 18. De este modo, la estación de comunicaciones consulta (etapa 150) y comprueba este nivel de seguridad (etapa 160).

En el presente ejemplo, el software usado para establecer una conexión VPN que está instalado en el ordenador 13 consulta (etapa 150) y comprueba este nivel de seguridad (etapa 160). La configuración existente en el registro requiere una autenticación de usuario, por ejemplo la introducción de un código PIN o la autenticación mediante características biométricas (etapa 170), para que se establezca un túnel VPN. Después de que se hayan presentado unas credenciales sólidas de autenticación de usuario (etapa 180), éstas se pueden almacenar en el módulo de identificación 18 y/o ser comprobadas por el mismo.

En la situación de la fig. 3, después se inicia un segundo túnel VPN. De nuevo, el gestor de eventos 26 identifica inmediatamente este evento (etapa 110), que se almacena en el registro de eventos 28 (etapa 120). Después, el registro de seguridad 30 recibe la notificación (etapa 130) y se actualiza (etapa 140). No obstante, en este caso, la configuración existente en el registro no requiere que continúe la autenticación, ya que ya se han presentado credenciales sólidas de autenticación. Esto da lugar al establecimiento de un túnel VPN sin interrupciones para el usuario.

Después de haber usado los canales de comunicación, se cierran ambos túneles VPN, uno después del otro. En todas las ocasiones, el gestor de eventos 26 identifica el evento (etapa 110), que se almacena en el registro de eventos 28 (etapa 120). El registro de seguridad 30 incorporado en el módulo de identificación 18 recibe la notificación y se adapta en consecuencia a cada momento (etapas 130, 140).

Cuando se inicia otro túnel VPN (es decir, el tercer túnel VPN de nuestro ejemplo), se realiza el mismo procedimiento descrito anteriormente para la primera VPN, es decir, identificación del evento mediante el gestor de eventos 26 (etapa 110), almacenar evento en el registro 28 (etapa 120), notificarlo al registro de seguridad y actualizarlo en consecuencia (etapas 130, 140).

Debido a que no quedó ningún túnel VPN y a que el registro de seguridad se adaptó en consecuencia, una vez más se requieren unas credenciales de autenticación sólidas como las mencionadas anteriormente (etapa 160), por ejemplo la introducción de un código PIN o la autenticación mediante características biométricas (etapa 170) tal como se describe anteriormente.

La fig. 4 ilustra una primera forma de realización de la invención con un gestor de eventos 26, registro de eventos 28 y registro de seguridad 30 compartidos para todas las aplicaciones 60 contenidas en el módulo de identificación 18. Tras haber iniciado una aplicación de cliente 40 (etapa 100), el evento se identifica a través del entorno de ejecución del cliente 50 mediante el gestor de eventos 27 de la estación de comunicaciones (etapa 110), se transmite al entorno de ejecución del módulo de identificación 70 y al gestor de eventos del módulo de identificación 26<sub>1</sub> y se almacena en el registro de eventos 28 de este módulo de identificación 18 (etapa 120). El nivel de seguridad de la estación de comunicaciones 12 se actualiza dentro del registro de seguridad 30 del módulo de identificación 18 de acuerdo con el evento o eventos almacenados (etapas 130, 140). Los mecanismos de seguridad se usan de acuerdo con el nivel de seguridad aplicable mediante la comunicación entre la aplicación de cliente 40 y la aplicación de tarjeta SIM 60 y la consulta del nivel de seguridad dentro de un registro de seguridad 30 compartido (etapas 150, 160).

La fig. 5 ilustra una segunda forma de realización de la invención con un gestor de eventos 26<sub>1</sub> y registro de eventos 28 compartidos y un único registro de seguridad 30<sub>1</sub>, 30<sub>2</sub> para una o para un grupo de aplicaciones 60<sub>1</sub>, 60<sub>2</sub>. La primera etapa de la forma de realización de la fig. 5 corresponde con la primera etapa de la forma de realización de la fig. 4, en la que, tras haber iniciado una aplicación de cliente 40 (etapa 100), el evento se identifica a través del entorno de ejecución del cliente 50 mediante el gestor de eventos 27 de la estación de comunicaciones (etapa 110), se transmite al entorno de ejecución de la tarjeta SIM 70 y al gestor de eventos 26<sub>1</sub> y se almacena en el registro de eventos 28 de dicho módulo de identificación 18. De nuevo, el nivel de seguridad de la estación de comunicaciones 12 se actualiza dentro

## ES 2 328 708 T3

de un registro de seguridad 30<sub>1</sub>, 30<sub>2</sub> de una aplicación o un grupo de aplicaciones 60<sub>1</sub>, 60<sub>2</sub> del módulo de identificación 18 de acuerdo con el evento o eventos almacenados (etapas 150, 160).

5 La fig. 6 ilustra una tercera forma de realización de la invención con un gestor de eventos 26<sub>1</sub> compartido para todas las aplicaciones 60<sub>1</sub>, 60<sub>2</sub> con el módulo de identificación 18. El procedimiento es básicamente el mismo que el que se explica en la fig. 4 y 5 de acuerdo con los principios básicos de la presente invención, con las etapas 100 a 160 que se describen anteriormente. No obstante, en la fig. 6, se proporciona un único registro de eventos 28<sub>1</sub>, 28<sub>2</sub> y registro de seguridad 30<sub>1</sub>, 30<sub>2</sub> para una aplicación o un grupo de aplicaciones 60<sub>1</sub>, 60<sub>2</sub>.

10 La fig. 7 ilustra una cuarta forma de realización de la invención, similar a las formas de realización que se han mostrado de acuerdo con las figs. 4, 5 y 6. En esta forma de realización, una aplicación o un grupo de aplicaciones 60<sub>1</sub>, 60<sub>2</sub> poseen un único gestor de eventos 26<sub>1</sub>, 26<sub>2</sub>, registro de eventos 28<sub>1</sub>, 28<sub>2</sub> y registro de seguridad 30<sub>1</sub>, 30<sub>2</sub>.

15 La ventaja obtenida con la presente invención reside en que proporciona un equilibrio aceptable entre los requisitos de seguridad y la facilidad de uso y ausencia de interrupciones que se exige. La obtención de un acceso adecuado a credenciales y funciones confidenciales en la tarjeta SIM y de un uso adecuado de las mismas podría depender de que se produzcan eventos específicos en el entorno de ejecución externa. Los mecanismos de control de acceso de la tarjeta SIM se adaptarán a estos eventos específicos.

### 20 **Números de referencia**

|                                          |                                                                                                                     |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| 10                                       | Sistema de comunicaciones                                                                                           |
| 12                                       | Estación de comunicaciones                                                                                          |
| 25 13                                    | Estación de trabajo                                                                                                 |
| 14                                       | Red IP                                                                                                              |
| 30 15                                    | Internet                                                                                                            |
| 16                                       | Terminal móvil                                                                                                      |
| 18                                       | Módulo de identificación del terminal móvil 16                                                                      |
| 35 20                                    | Posición de almacenamiento                                                                                          |
| 22                                       | Sistema de comunicación celular                                                                                     |
| 40 24                                    | Línea de comunicación                                                                                               |
| 26                                       | Gestor de eventos de la tarjeta SIM                                                                                 |
| 26 <sub>1</sub> , 26 <sub>2</sub>        | Gestor de eventos de la tarjeta SIM para aplicación o aplicaciones de tarjeta SIM 60 <sub>1</sub> , 60 <sub>2</sub> |
| 45 27                                    | Gestor de eventos de la estación de comunicaciones                                                                  |
| 28, 28 <sub>1</sub> , 28 <sub>2</sub>    | Registro de eventos                                                                                                 |
| 50 30, 30 <sub>1</sub> , 30 <sub>2</sub> | Registro de seguridad                                                                                               |
| 40                                       | Aplicación de cliente                                                                                               |
| 50                                       | Entorno de ejecución de cliente                                                                                     |
| 55 60, 60 <sub>1</sub> , 60 <sub>2</sub> | Aplicación de tarjeta SIM                                                                                           |
| 70                                       | Entorno de ejecución de tarjeta SIM                                                                                 |
| 60 100 a 170                             | Diferentes etapas del procedimiento de la invención                                                                 |
| 100                                      | Inicio de la aplicación de cliente                                                                                  |
| 110                                      | Identificación del evento mediante el gestor de eventos 26                                                          |
| 65 120                                   | Almacenamiento del evento en el registro de eventos 28                                                              |

## ES 2 328 708 T3

|        |                                                                                                                           |
|--------|---------------------------------------------------------------------------------------------------------------------------|
| 130    | Notificación al registro de seguridad 30                                                                                  |
| 140    | Actualización del nivel de seguridad en el registro de seguridad 30                                                       |
| 5 150  | Aplicación de tarjeta SIM de dirección 60                                                                                 |
| 160    | Consulta o comprobación del nivel de seguridad en el registro de seguridad 30                                             |
| 170    | Autenticación del usuario                                                                                                 |
| 10 180 | Cumplimiento de las condiciones de uso especificadas por el registro de seguridad 30 para la aplicación de tarjeta SIM 60 |
| 15     |                                                                                                                           |
| 20     |                                                                                                                           |
| 25     |                                                                                                                           |
| 30     |                                                                                                                           |
| 35     |                                                                                                                           |
| 40     |                                                                                                                           |
| 45     |                                                                                                                           |
| 50     |                                                                                                                           |
| 55     |                                                                                                                           |
| 60     |                                                                                                                           |
| 65     |                                                                                                                           |

## REIVINDICACIONES

1. Un procedimiento para adaptar los parámetros de seguridad de una estación de comunicaciones (12) dependiendo de un evento que afecta a la seguridad, en el que la estación de comunicaciones (12) comprende un terminal móvil (16) con un módulo de identificación (18), y el procedimiento comprende las siguientes etapas de:

- (a) identificación del evento que afecta a la seguridad, que se produce en dicha estación de comunicaciones y/o dicho terminal móvil (16);
- (b) actualización de un registro de seguridad (30) existente en el módulo de identificación (18) de acuerdo con el evento que afecta a la seguridad; y
- (c) adaptación y refuerzo del nivel de seguridad de la estación de comunicaciones (12) de acuerdo con el registro de seguridad (30) del módulo de identificación (18),

**caracterizado** porque

dichos parámetros de seguridad, que se definen en el registro de seguridad (30), se usan para limitar el derecho o derechos de una aplicación, un grupo de aplicaciones o la totalidad de las aplicaciones (60, 60<sub>1</sub>, 60<sub>2</sub>) ejecutadas por dicha estación de comunicaciones (12) o terminal móvil (16), incluida la restricción de acceso a aplicaciones (60, 60<sub>1</sub>, 60<sub>2</sub>) existentes en dicho módulo de identificación (18) por parte de otros componentes de dicha estación de comunicaciones (12).

2. El procedimiento según la reivindicación 1, en el que dicho evento que afecta a la seguridad es identificado en dicho módulo de identificación (18) y/o en dicha estación de comunicaciones (12).

3. El procedimiento según cualquiera de las reivindicaciones 1 y 2, en el que dicho evento que afecta a la seguridad se almacena en dicho módulo de identificación (18).

4. El procedimiento según cualquiera de las reivindicaciones 1 a 3, en el que dicho evento que afecta a la seguridad se refiere a uno de los siguientes casos:

- cambio en la configuración de hardware de dicha estación de comunicaciones (12) o terminal móvil (16), y/o
- cambio en la configuración de software de dicha estación de comunicaciones (12) o terminal móvil, y/o
- conexión de dicha estación de comunicaciones (12) o terminal móvil (16) a una red o sistema externo, y/o
- evento generado por una aplicación ejecutada por dicha estación de comunicaciones (12) o terminal móvil (16), y/o
- evento transmitido de forma inalámbrica a dicha estación de comunicaciones (12).

5. El procedimiento según una cualquiera de las reivindicaciones 1 a 4, en el que dicho evento que afecta a la seguridad comprende uno o una pluralidad de los siguientes eventos: creación; liberación, pérdida o cierre de canales de acceso, bloqueo o desbloqueo del estado de la estación de trabajo, retirada o instalación de componentes de hardware o software, un inicio automático desde un dispositivo y detección de contenidos, tráfico o modificaciones que resulten maliciosos o sospechosos.

6. El procedimiento según una cualquiera de las reivindicaciones 1 a 4, en el que dicho evento que afecta a la seguridad se refiere a la actividad de un antivirus, un firewall y/o una puerta de acceso IPSec.

7. El procedimiento según una cualquiera de las reivindicaciones 1 a 6, en el que dicho evento que afecta a la seguridad se refiere al estado de la sesión del usuario y/o al estado de un canal de conexión que implica dicho estado de comunicación.

8. El procedimiento según una cualquiera de las reivindicaciones 1 a 7, en el que dicho evento que afecta a la seguridad se usa para limitar el derecho de una sola o de la totalidad de las aplicaciones ejecutadas por dicha estación de comunicaciones (12) o terminal móvil (16) de realizar algunas acciones.

9. El procedimiento según las reivindicaciones 1 a 8, en el que dichos parámetros de seguridad determinan el acceso a credenciales a partir de una señal de entrada del usuario.

10. El procedimiento según las reivindicaciones 1 a 8, en el que el acceso a credenciales contenidas en dicho módulo de identificación (18) depende de dicho nivel de seguridad.

## ES 2 328 708 T3

11. El procedimiento según la reivindicación 9 ó 10, en el que dichas credenciales comprenden características biométricas del usuario.

5 12. El procedimiento según las reivindicaciones 1 a 11, en el que dicho nivel de seguridad determina los requisitos de autenticación para una aplicación ejecutada por dicho módulo de identificación (18) y/o por dicho terminal móvil (16).

10 13. El procedimiento según cualquiera de las reivindicaciones 1 a 12, en el que la estación de comunicaciones (12) comprende una estación de trabajo (13) y un terminal móvil (16) con un módulo de identificación (18) y el procedimiento comprende la etapa de adaptación de los mecanismos de seguridad para la estación de trabajo (13) y/o el terminal móvil (16), de acuerdo con el nivel de seguridad aplicable mediante una consulta en el registro de seguridad (30) del módulo de identificación (18).

15 14. El procedimiento según cualquiera de las reivindicaciones 1 a 13, que comprende la etapa de identificación de un evento que afecta a la seguridad con uno o una pluralidad de los siguientes campos: identificador de evento, tipo de evento, fecha y hora, número de secuencia, nivel crítico del evento o información adicional específica para el tipo de evento.

20 15. El procedimiento según cualquiera de las reivindicaciones 1 a 14, que comprende la etapa de actualización del nivel de seguridad de la estación de comunicaciones (12) dentro de un registro de seguridad (30) compartido por todas las aplicaciones ejecutadas por dicho módulo de identificación (18) y/o terminal móvil (16).

25 16. El procedimiento según cualquiera de las reivindicaciones 1 a 14, que comprende la etapa de actualización del nivel de seguridad de la estación de comunicaciones (12) dentro de un registro de seguridad diferente (30) para cada aplicación o para un grupo de aplicaciones, ejecutadas por dicho módulo de identificación (18) y/o terminal móvil (16).

30 17. El procedimiento según cualquiera de las reivindicaciones 1 a 16, que comprende la etapa de notificación al módulo de identificación (18) del evento que afecta a la seguridad y almacenamiento del evento que afecta a la seguridad en un registro de eventos (28) existente en dicho módulo de identificación (18).

18. El procedimiento de la reivindicación 17, en el que todas las aplicaciones ejecutadas por dicho módulo de identificación (18) y/o terminal móvil (16) comparten dicho registro de eventos (28).

35 19. El procedimiento de la reivindicación 17, en el que se usa un registro de eventos (28) diferente para cada aplicación o para un grupo de aplicaciones ejecutadas por dicho módulo de identificación (18) y/o terminal móvil (16).

40 20. El procedimiento según cualquiera de las reivindicaciones 1 a 19, que comprende la etapa de identificación de un evento que afecta a la seguridad por medio de un gestor de eventos (26, 26<sub>1</sub>, 26<sub>2</sub>, 27) incluido en dicho módulo de identificación (18) y/o en dicha estación de comunicaciones (12).

45 21. El procedimiento de la reivindicación 20, en el se proporciona dicho gestor de eventos (26, 26<sub>1</sub>, 26<sub>2</sub>) en dicho módulo de identificación (18) y es compartido por todas las aplicaciones ejecutadas por dicho módulo de identificación (18) y/o terminal móvil (16).

50 22. El procedimiento de la reivindicación 21, en el se proporciona un gestor de eventos (26, 26<sub>1</sub>, 26<sub>2</sub>) diferente para cada aplicación o para un grupo de aplicaciones ejecutadas por dicho módulo de identificación (18) y/o terminal móvil (16).

23. El procedimiento según una cualquiera de las reivindicaciones 1 a 22, que comprende las etapas de:

identificación de eventos que afectan a la seguridad con al menos un gestor de eventos (26, 26<sub>1</sub>, 26<sub>2</sub>, 27)

55 almacenamiento de los eventos que afectan a la seguridad en al menos un registro de eventos (28) del módulo de identificación (18),

actualización de un nivel de seguridad en al menos un registro de seguridad (30) de dicho módulo de identificación (18) de acuerdo con el evento almacenado,

60 comprobación de dicho nivel de seguridad.

65 24. El procedimiento según una cualquiera de las reivindicaciones 1 a 23, que comprende la etapa de almacenamiento de los parámetros de seguridad cuando se desconecta la estación de comunicaciones (12) y reutilización de los parámetros de seguridad cuando se vuelve a conectar la estación de comunicaciones (12).

## ES 2 328 708 T3

25. Estación de comunicaciones (12) que comprende un terminal móvil (16) provisto de un módulo de identificación (18), en la que el módulo de identificación (18) comprende:

al menos un registro de eventos (28) para almacenar eventos identificados por un gestor de eventos (26, 26<sub>1</sub>, 26<sub>2</sub>), y al menos un registro de seguridad (30), en el que se definen los parámetros de seguridad, para adaptar y reforzar el nivel de seguridad de la estación de comunicaciones (12) de acuerdo con los eventos almacenados en el registro de eventos (28),

**caracterizado** porque

dichos parámetros de seguridad, que se definen en el registro de seguridad (30), se usan para limitar el derecho o derechos de una aplicación, un grupo de aplicaciones o la totalidad de las aplicaciones (60, 60<sub>1</sub>, 60<sub>2</sub>) ejecutadas por dicha estación de comunicaciones (12) o terminal móvil (16), incluida la restricción del acceso a aplicaciones (60, 60<sub>1</sub>, 60<sub>2</sub>) contenidas en dicho módulo de identificación (18) por parte de otros componentes de dicha estación de comunicaciones (12).

26. Estación de comunicaciones (12) de acuerdo con la reivindicación precedente, que además comprende una estación de trabajo (13) y un terminal móvil (16), con al menos una unidad de dicho registro de seguridad (30) para actualizar el nivel de seguridad de la estación de trabajo (13) y/o el terminal móvil (16), de acuerdo con el evento almacenado en el registro de eventos (28).

27. Estación de comunicaciones (12) de acuerdo con la reivindicación precedente, en la que el terminal móvil (16) puede introducirse en la estación de trabajo (13) de forma que se pueda extraer.

28. Estación de comunicaciones (12) de acuerdo con cualquiera de las reivindicaciones 25 a 27, que además comprende varios registros de seguridad (30) para diferentes aplicaciones o para un grupo de aplicaciones.

29. Estación de comunicaciones (12) de acuerdo con la reivindicación precedente, que comprende varios registros de eventos (28) para diferentes aplicaciones o para un grupo de aplicaciones.

30. Estación de comunicaciones (12) de acuerdo con cualquiera de las reivindicaciones 25 a 29, que comprende al menos un gestor de eventos (26, 26<sub>1</sub>, 26<sub>2</sub>) para identificar los eventos que afectan a la seguridad en dicho módulo de identificación (18).

31. Estación de comunicaciones (12) de acuerdo con cualquiera de las reivindicaciones 25 a 30, que comprende diferentes gestores de eventos (26<sub>1</sub>, 26<sub>2</sub>) para diferentes aplicaciones o para un grupo de aplicaciones.

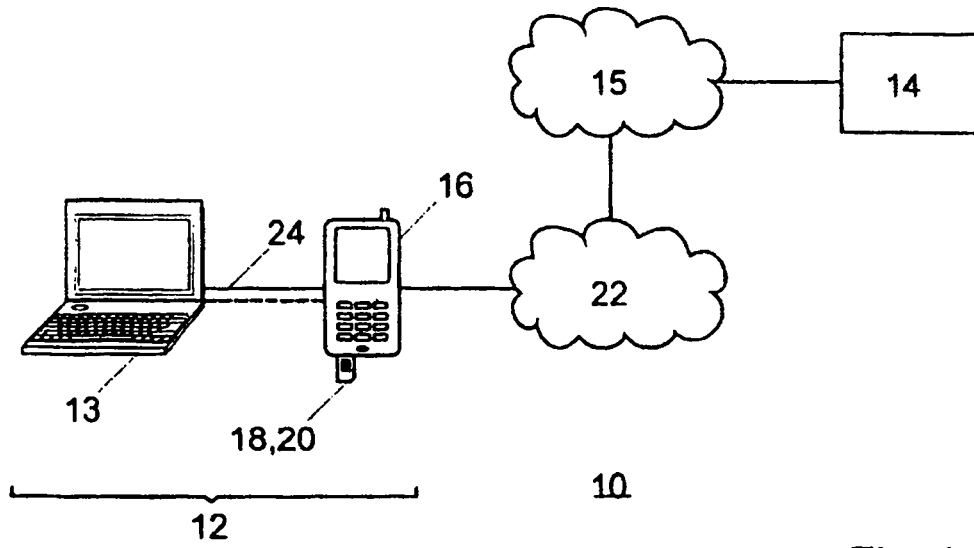


Fig. 1a

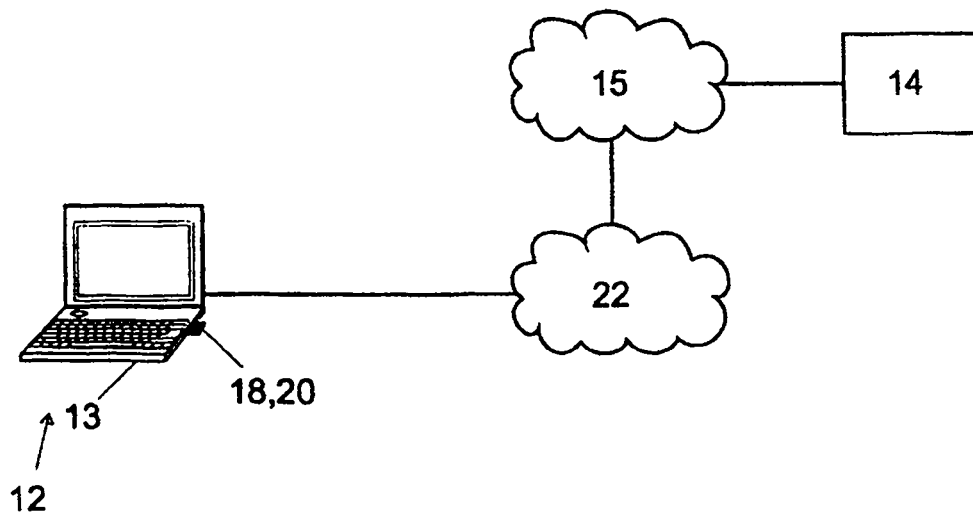


Fig. 1b

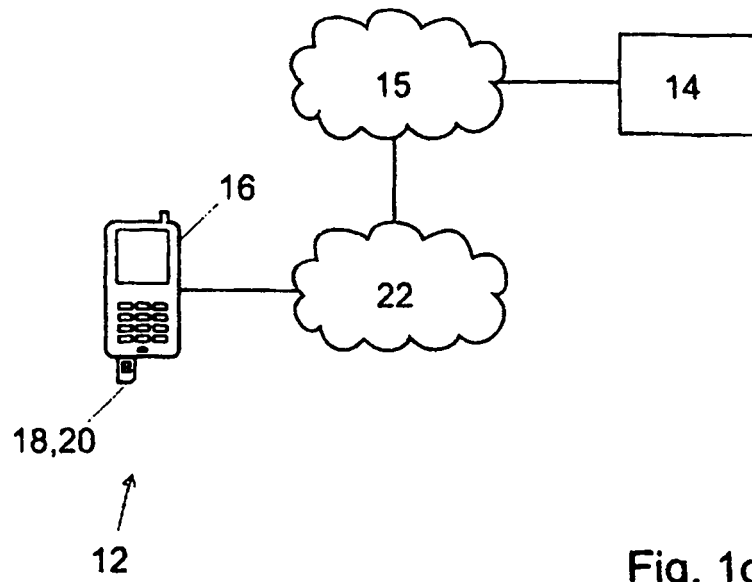


Fig. 1c

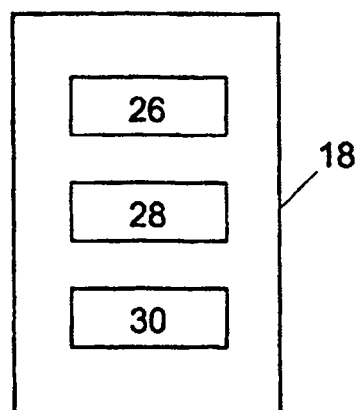


Fig. 2

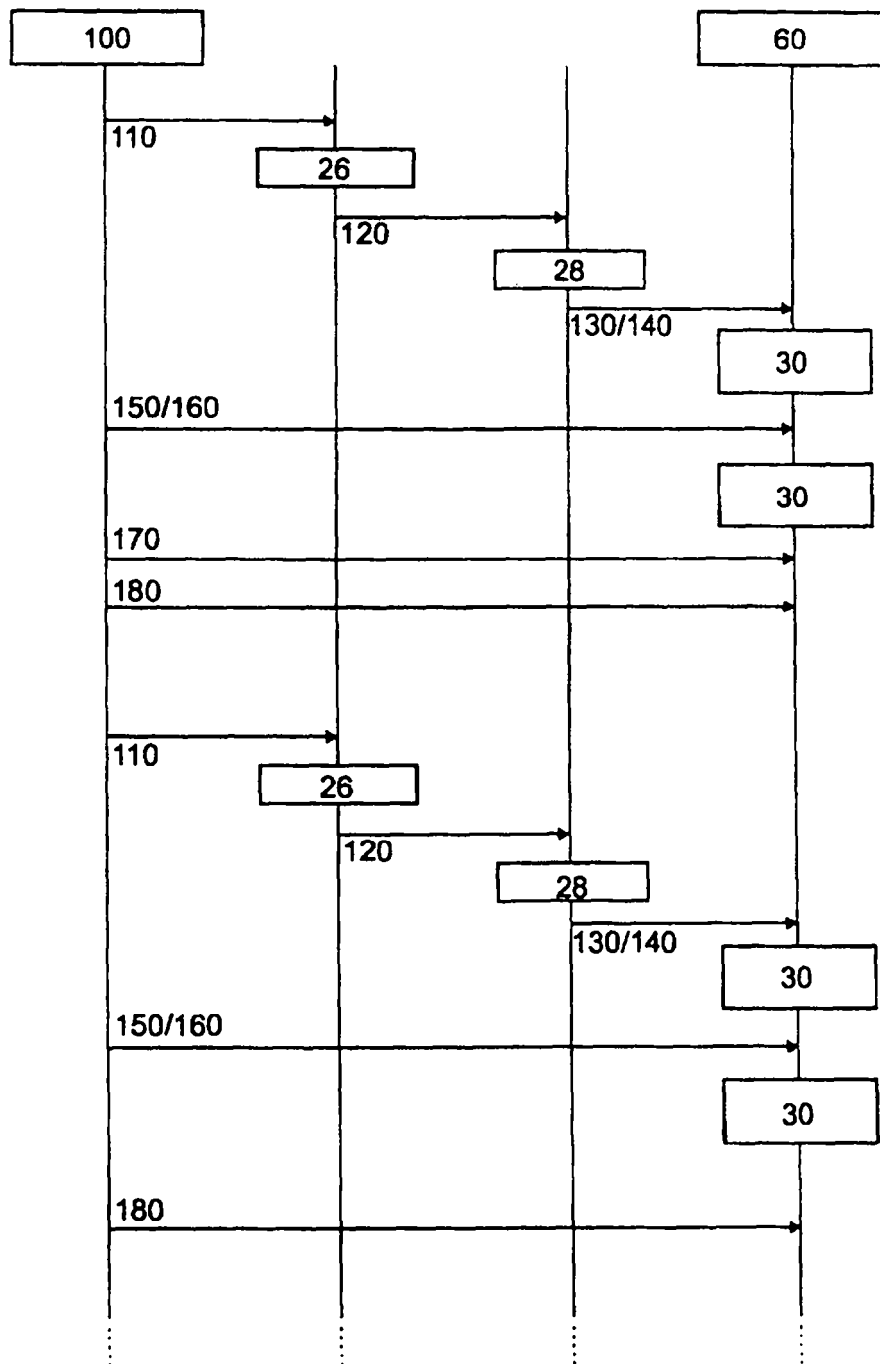


Fig. 3a

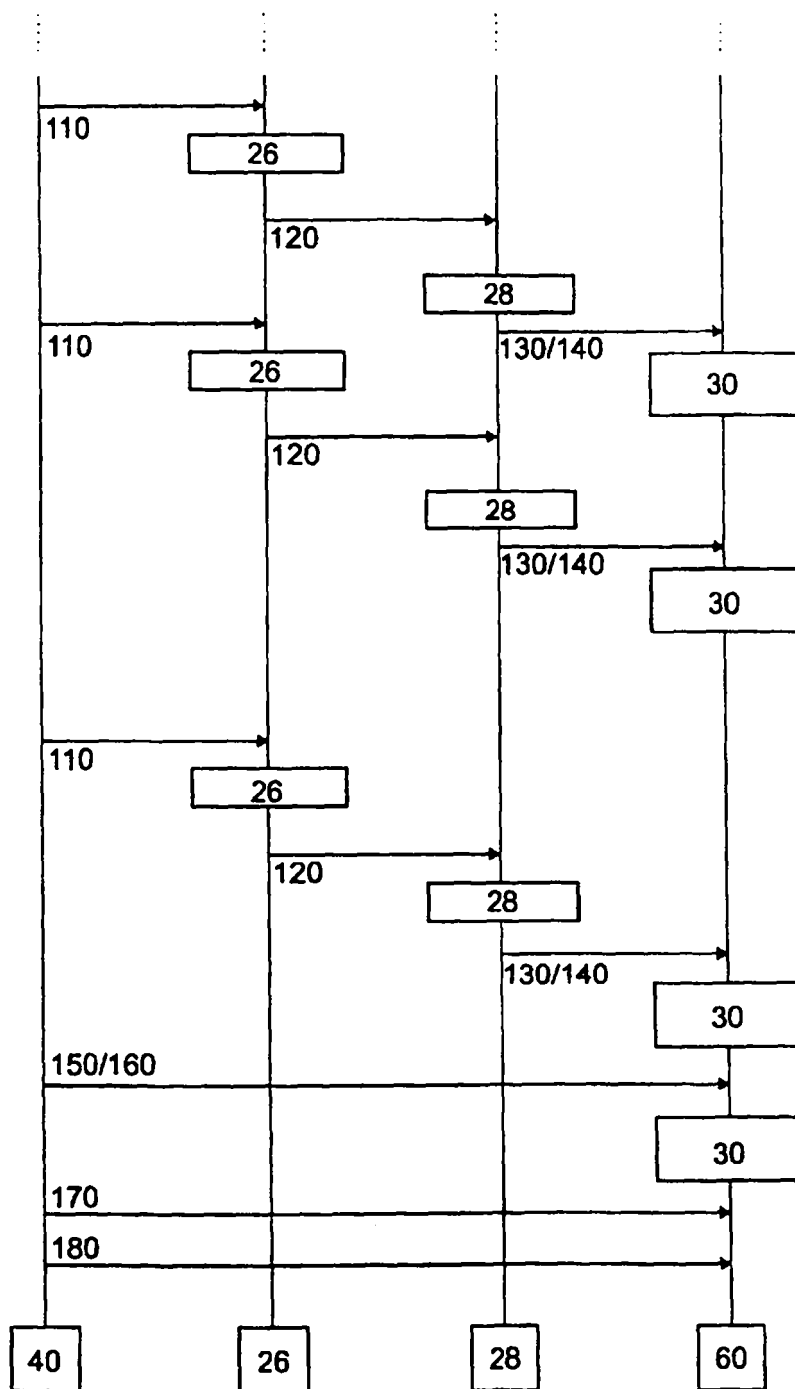


Fig. 3b

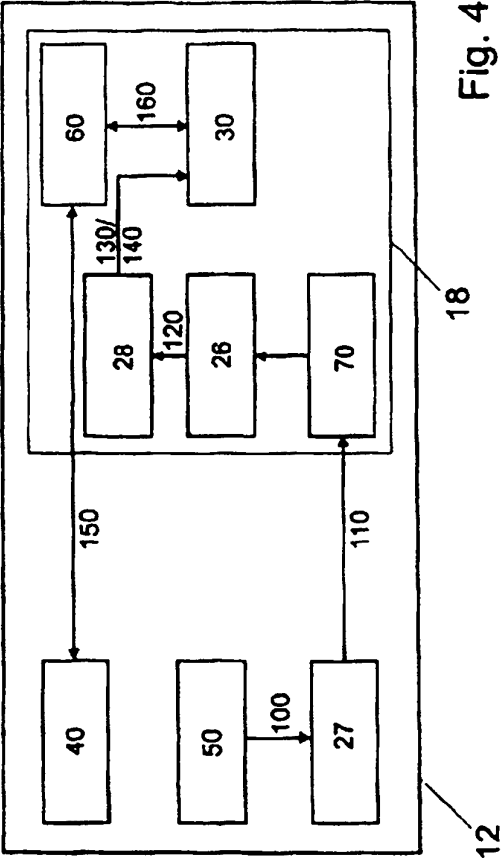


Fig. 4

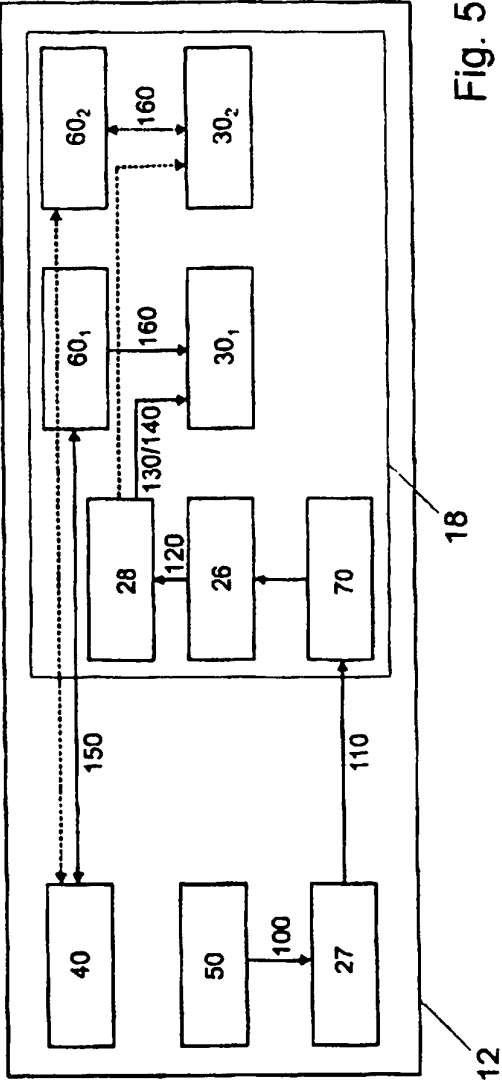


Fig. 5

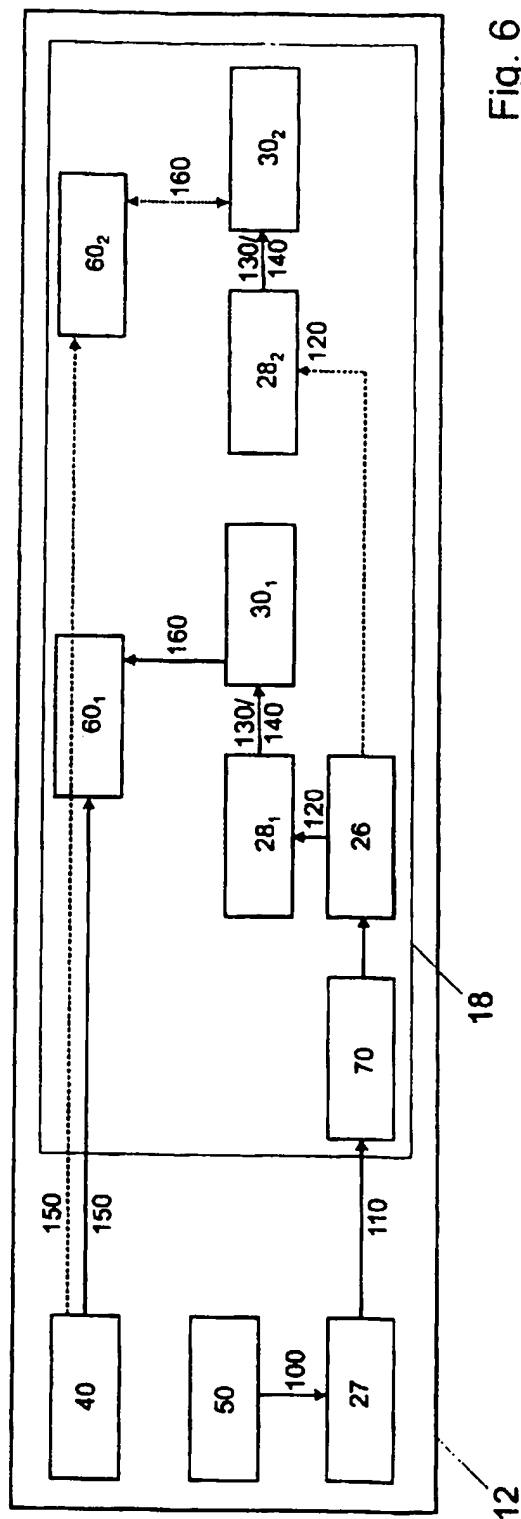


Fig. 6

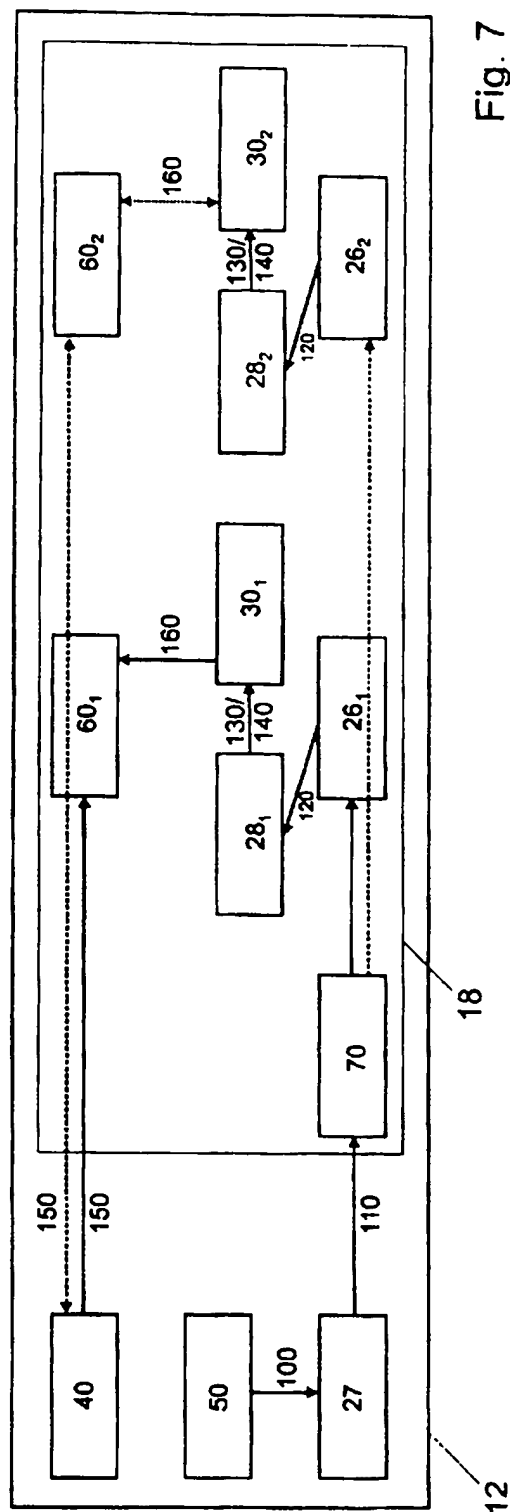


Fig. 7