(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 393 568**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04M 1/725 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **05405398 .8**
(96) Fecha de presentación: **23.06.2005**
(97) Número de publicación de la solicitud: **1737181**
(97) Fecha de publicación de la solicitud: **27.12.2006**

(54) Título: **Dispositivo con procedimiento y producto de programa informático para controlar la posibilidad de utilización de un módulo de aplicación mediante un módulo de seguridad**

(45) Fecha de publicación de la mención BOPI:

26.12.2012

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

26.12.2012

(73) Titular/es:

SWISSCOM AG (100.0%)
ALTE TIEFENAUSTRASSE 6
3050 BERN, CH

(72) Inventor/es:

CANTINI, RENATO y
AEBI, PAUL

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Dispositivo con procedimiento y producto de programa informático para controlar la posibilidad de utilización de un módulo de aplicación mediante un módulo de seguridad

Aspecto técnico

La presente invención se refiere a un módulo de seguridad y a un procedimiento para controlar la posibilidad de utilización de un módulo de aplicación. La presente invención se refiere en particular a un módulo de seguridad adecuado para un equipo terminal de comunicaciones que esté preparado para autentificar una red de telecomunicaciones y que comprende por lo menos un módulo de aplicación utilizable así como un procedimiento para controlar la posibilidad de utilización del módulo de aplicación.

Estado de la técnica

Los módulos de seguridad son especialmente conocidos para equipos terminales de comunicación móviles, por ejemplo radioteléfonos móviles, en forma de tarjetas chip como las denominadas tarjetas SIM (Suscriber Identity Module). Estos módulos de seguridad tienen también amplia aplicación en equipos terminales de comunicación en las redes fijas. Además de para la identificación del abonado, los módulos de seguridad sirven especialmente también para la autentificación de las redes de telecomunicación. Los protocolos para la autentificación de las redes de extremo a extremo por medio del módulo de seguridad se describen en diversas publicaciones de normalización. La autentificación del acceso a la red a redes móviles basado en 3GPP AKA (3GPP:Third Generation Partnership Project (Proyecto de Asociación de Tercera Generación); AKA: Authentication and Key Agreement Protocol (Protocolo de Autentificación y Acuerdo Clave) se define por ejemplo en las especificaciones técnicas (ETSI TS 133 102 V6.3.0 (2004-12); Universal Mobile TelecommunicationsSystem (UMTS), (Sistema Universal de Telecomunicaciones Móviles); 3G Security (Seguridad 3G); Security Architecture (Arquitectura de Seguridad) (3GPP TS 33.102 Versión 6.9.0, Edición 6) o ETSI TS 131 102 V6.9.0 (2005-03)Universal Mobile Telecommunications System (UMTS) (Sistema Universal de Telecomunicaciones Móviles); Characteristics of the US-IM Application (Características de la Aplicación US-IM) (3GPP TS 31.102 Versión 6.9.0 Edición 6). La autentificación del acceso al IMS (IP Multimedia Subsystem, Subsistema Multimedia IP) basado en 3GPP AKA se define por ejemplo en las especificaciones técnicas ETSI TS 131 103 V6.7.0 (2005-03): Digital CellularTelecommunications System (Sistema Digital de Telecomunicaciones Celulares) (Fase 2+); Universal Mobile Telecommunications Systems (UMTS); Characteristics of the IP Multimedia Services Identity Module (ISIM) (Características del Módulo de Identidad de los Servicios Multimedia IP), Application (3GPP TS 31.103 Versión 6.7.0 Edición 6). La autentificación del acceso a redes locales públicas inalámbricas (Public Wireless Local Area Network, WLAN) basado en EAP (Extensible Authentication Protocol, Protocolo de Autentificación Extensible) se describe por ejemplo en ETSI TS 102 310 V6.1.0 (2005-02); Smart Cards (Tarjetas Inteligentes); Extensible Authentication Protocol Support in the UICC (Soporte de Protocolo de Autentificación Extensible en el UICC (Edición 6). Otros mecanismos de autentificación se describen en ETSI TS 101 181 V8.8.0 (2001-12); Digital Cellular Telecommunications System (Fase 2+) (Sistema Digital de Telecomunicación Celular, Fase 2+); Security Mechanisms for SIM ApplicationToolkit (Mecanismo de Seguridad para el Conjunto de Herramientas de Aplicación SIM) Stage 2 (Fase 2) (3GPP TS 03.48 Versión 8.8.0 Edición 1999) y en ETSI TS123048 V5.8.0 (2003-12); Digital Cellular Telecommunications System (Phase 2+) (Sistema de Telecomunicaciones Digitales Celulares, Fase 2+); Universal Mobile Telecommunications System (UMTS), Sistema Universal de Telecomunicaciones Móviles); Security Mechanisms for the (U) SIM Apliccation Toolkit; Stage 2 (Mecanismo de Seguridad para el Juego de Herramientas de Aplicación (U) SIM (3GPP TS 23.048 Versión 5.8.0, Edición 5) para SMS (Short Messaging Services). Típicamente los módulos de seguridad comprenden también módulos de aplicación que en particular pueden utilizarse a menudo también con independencia de la red. Por ejemplo se puede utilizar un módulo de criptografía para la decodificación de datos codificados, sin que para ello sea necesario el acceso a una red de telecomunicaciones autentificada. De forma similar se puede utilizar un módulo de aplicación para pagos en línea a través de Internet, sin que para ello tenga que utilizarse necesariamente la red de telefonía móvil o la WLAN, que son explotados por el editor del módulo de seguridad que le ofrece a un usuario de una red de telecomunicaciones, en particular de una red de radiotelefonía móvil o WLAN, que le facilita a un abonado un módulo de seguridad o módulo de aplicación para utilización en la red de telecomunicaciones, por lo tanto sin que exista control para saber si el abonado emplea módulos de aplicación independientes de la red, sin utilizar tampoco la red de telecomunicaciones del usuario. Esto quiere decir que el módulo de seguridad no pide ningún enlace de la utilización de aplicaciones independientes de la red a la utilización de la red de telecomunicaciones del usuario.

En el Wireless Application Protocol (WAP) Forum (Foro del Protocolo de Aplicación Inalámbrica (WAP) “Wireless Appplication Protocol (Protocolo de Aplicación Inalámbrica), WAP-182-ProvArch20010314-a, Provisioning Architecture Overview” (Resumen de Arquitectura de Facilitación) del 14 de Marzo de 2001 se exponen consideraciones de seguridad para la configuración de clientes WAP típicamente equipos terminales inalámbricos de clientes. La configuración protegida de un cliente WAP tiene lugar basándose en una relación de confianza entre un ofertante fiable (Trusted Provisioning Server, TPS) del contexto de configuración y del cliente WAP. En el establecimiento del contexto de configuración pueden emplearse por ejemplo también parámetros de seguridad tales como secretos o certificados compartidos.

En el documento US 2004/0123152 se describe una plataforma para marcas de seguridad basadas en hardware tales como tarjetas SIM o marcas USB (Universal Serial Bus). Las marcas de seguridad comprenden uno o varios dominios de seguridad para la instalación y ejecución de aplicaciones. Los dominios de seguridad están asignados cada uno a un ofertante de aplicación y comprenden unos mecanismos de seguridad internos. Los mecanismos de seguridad están basados en reglas de seguridad registradas, que incluyen en particular también reglas para bloquear y liberar justificantes de utilización de acceso (Credentials) y que tienen claves criptográficas.

Exposición de la invención

Uno de los objetivos de la presente invención es proponer un módulo de seguridad adecuado para un equipo terminal de comunicaciones así como un procedimiento para controlar la posibilidad de utilización de un módulo de aplicación de un módulo de seguridad, que no presente los inconvenientes del estado de la técnica. Es en particular un objetivo de la presente invención proponer un módulo de seguridad así como un procedimiento para controlar la posibilidad de utilización de un módulo de aplicación del módulo de seguridad, que permita por lo menos un cierto acoplamiento de la utilización de módulos de aplicación independientes de la red a la utilización de una determinada red de telecomunicaciones.

En este punto hay que recordar que con el concepto de posibilidad de utilización se describe la propiedad que tiene un módulo de aplicación de estar disponible (para un usuario) para su utilización. De forma correspondiente un módulo de aplicación con posibilidad de utilización suspendida (para el usuario) no está disponible para el uso puesto que el módulo de aplicación para el usuario por ejemplo no es visible, seleccionable, activable o ejecutable.

De acuerdo con la presente invención se alcanzan los objetivos antes indicados, en particular mediante los elementos de las reivindicaciones independientes. Otras formas de realización ventajosas se deducen además de las reivindicaciones dependientes y de la descripción.

El módulo de seguridad está previsto para un equipo terminal de comunicaciones y comprende por lo menos un módulo de aplicación utilizable. El módulo de seguridad está además preparado para autentificar una red de telecomunicaciones.

Los objetivos antes citados se alcanzan mediante la presente invención especialmente porque el módulo de seguridad está dotado de un módulo de bloqueo para anular la posibilidad de utilización del módulo de aplicación. Además de esto, el módulo de seguridad comprende un módulo de liberación para restablecer (respective establecer) la posibilidad de utilización del módulo de aplicación, así como un módulo de control para activar el módulo de liberación (respective para activar el restablecimiento de la posibilidad de utilización), dependiente de los datos recibidos que se puedan asignar de modo autentificable a una determinada red de telecomunicaciones. El módulo de seguridad comprende por ejemplo varios módulos de control cada uno de los cuales está asignado a un módulo de aplicación. El módulo de seguridad está realizado preferentemente como dispositivo, en particular como tarjeta chip, que se puede unir de modo liberable con el equipo terminal de comunicaciones. El especialista entenderá que el módulo de seguridad, también puede realizarse en una variante como producto de programa informático con medios de codificación del programa informático para el control de uno o varios procesadores del equipo terminal de comunicaciones. En una variante de realización el módulo de seguridad está realizado como módulo de identificación del abonado. El módulo de seguridad está realizado por ejemplo para un equipo terminal de comunicaciones móvil preparado para redes de radiotelefonía móvil. Por hecho de que la posibilidad de utilización de un módulo de aplicación dependiente de datos que se pueden asignar de modo autentificable a una determinada red de telecomunicaciones o se pueda suspender, se tiene la posibilidad de ligar la utilización de aplicaciones independientes de la red a la utilización de una determinada red de telecomunicaciones. Por ejemplo la posibilidad de utilización del módulo de aplicación puede estar ligado a la condición de que el usuario del equipo terminal de comunicaciones se dé de alta en la determinada red de telecomunicaciones y reciba entonces datos de autentificación de esta red de telecomunicaciones. La condición para la posibilidad de utilización se extiende preferentemente también a redes de telecomunicación que tengan un acuerdo Roaming con la determinada red de telecomunicaciones, es decir que la posibilidad de utilización se liga por lo tanto a su empleo en redes de telecomunicación del explotador de la red particular y el socio de Roaming del explotador de la red particular. Mediante la transmisión explícita de mensajes de autorización autentificados respective datos de autorización se puede ligar la posibilidad de utilización de un módulo de aplicación a determinadas condiciones del explotador de la red de telecomunicaciones, por ejemplo a un determinado importe de servicios que son obtenidos por el usuario del explotador de la red de telecomunicaciones.

En unas variantes de realización distintas o combinadas, el módulo de control está además preparado para activar el módulo de bloqueo, dependiendo del número de utilizaciones del módulo de aplicación, del número de selecciones del módulo de aplicación, del número de utilización de las funciones del módulo de aplicación, del número de sesiones establecidas a través de un canal lógico del módulo de comunicación, del número de ciclos de reposición del módulo de seguridad y/o de alcanzar un determinado tiempo. Mediante la vigilancia de diferentes parámetros se tiene la posibilidad de realizar un control dinámico de la posibilidad de utilización de un módulo de aplicación, adaptándolo de modo flexible a diferentes requisitos.

En unas variantes de realización distintas o combinadas, el módulo de control está además preparado para activar el módulo de liberación, con independencia de los mensajes de autorización recibidos, que se puedan asignar de modo autentificable a la determinada red de telecomunicaciones y/o sean dependientes de datos de autentificación recibidos que se puedan asignar a la determinada red de telecomunicaciones. El control de la posibilidad de utilización de un módulo de aplicación en función de los datos de autentificación recibidos tiene la ventaja de que la posibilidad de utilización se puede controlar sin otras modificaciones de la infraestructura de la red, únicamente en el módulo de seguridad.

En unas variantes de realización distintas o combinadas, el módulo de bloqueo está preparado para suspender la posibilidad de utilización del módulo de aplicación mediante la desactivación, el bloqueo, la ocultación, la liberación y/o la desinstalación del módulo de aplicación. El módulo de liberación está preparado correspondientemente para volver a establecer la posibilidad de utilización del modulo de aplicación por medio de la activación, desbloqueo, listado, despertado y/o instalación del módulo de aplicación.

En una variante de realización, el módulo de seguridad comprende por lo menos un registro de expiración que está asignado a uno o varios módulos de aplicación. El módulo de control está preparado para almacenar en el registro de expiración datos actuales relativos al número de utilizaciones del módulo de aplicación, al número de selecciones del módulo de aplicación, al número de utilizaciones de funciones del módulo de aplicación, al número de sesiones establecidas a través de un canal lógico del módulo de aplicación, al número de ciclos de reposición del módulo de seguridad y/o al tiempo de duración.

En una variante de realización, el módulo de seguridad comprende por lo menos un registro de autorización que está asignado a uno o varios módulos de aplicación. El módulo de control está preparado para almacenar en el registro de autorización datos relativos al número autorizado de utilizaciones del módulo de aplicación, al número autorizado de selecciones del módulo de aplicación, al número autorizado de utilizaciones de funciones del módulo de aplicación, al número autorizado de sesiones a través de un canal lógico de sesiones de aplicación, al número autorizado de ciclos de reposición del módulo de seguridad y/o al tiempo de duración autorizado.

Además del módulo de seguridad para equipos terminales de comunicación y del procedimiento para el control de la utilización de un módulo de aplicación, la presente invención se refiere también a un producto de programa informático con medios de codificación del programa informático para el control de uno o varios procesadores de un módulo de seguridad para un equipo terminal de comunicaciones, cuyo módulo de seguridad está preparado para autentificar una red de telecomunicaciones y cuyo módulo de seguridad comprende por lo menos un módulo de aplicación utilizable, comprendiendo el producto de programa informático en particular un medio legible por ordenador en el cual están almacenados los medios de codificación del programa informático.

Breve descripción de los dibujos

A continuación se describe una realización de la presente invención sirviéndose de un ejemplo. El ejemplo de realización está ilustrado por las siguientes figuras adjuntas:

La figura 1 muestra un diagrama de bloques que representa esquemáticamente un equipo terminal de comunicaciones con un módulo de seguridad, estando realizado el módulo de seguridad como dispositivo que está unido de modo liberable con el equipo terminal de comunicaciones.

La figura 2 muestra un diagrama de bloques que representa otro ejemplo de un equipo terminal de comunicaciones con un módulo de seguridad, estando realizado el módulo de seguridad como producto de programa informático con medios de codificación del programa informático para el control de uno o varios procesadores del equipo terminal de comunicaciones.

La figura 3 muestra un diagrama de bloques que ilustra de modo esquemático una posible realización del módulo de seguridad así como los desarrollos de proceso correspondientes.

La figura 4 muestra un diagrama de bloques que ilustra esquemáticamente otra posible realización del módulo de seguridad así como los respectivos desarrollos del proceso.

La figura 5 muestra un diagrama de bloques que ilustra esquemáticamente otra posible realización del módulo de seguridad así como los correspondientes desarrollos del proceso.

La figura 6 muestra un diagrama de bloques que ilustra esquemáticamente otra posible realización del módulo de seguridad así como los respectivos desarrollos del proceso.

Guías para la realización de una invención

En las figuras 1 a 6 los componentes que se correspondan entre sí están designados cada uno con el mismo signo de referencia.

En las figuras 1 a 6, la referencia 1 designa un módulo de seguridad que está preparado para autentificar una red de telecomunicaciones 2. Una autentificación de la red de telecomunicaciones 2 de extremo a extremo la realiza el

módulo de seguridad 1 basándose por ejemplo en los mecanismos de autentificación conocidos, citados inicialmente. El módulo de seguridad comprende varios módulos de aplicación 11, 11' que pueden ser utilizados por el usuario del módulo de seguridad 1 o por el entorno del tiempo de funcionamiento (Client Execution Environment) o por aplicaciones del equipo terminal de comunicaciones 10. Para los módulos de aplicación 11, 11' que requieren una interacción del usuario, el usuario puede introducir datos, por ejemplo a través de los elementos de introducción de datos 101, 101' (teclado, ratón) y que se le reproducen para el usuario a través de la pantalla 102 o de forma acústica. Además de los módulos de aplicación utilizables 11, 11' el módulo de seguridad 1 comprende otros módulos de función, en particular un módulo de bloqueo 12, un módulo de liberación 13 y un módulo de control 14 así como un registro de expiración así como un registro de autorización 16. El módulo de bloqueo 12 está preparado para suspender la utilización de uno o varios módulos de aplicación 11, 11', es decir bloquear la disponibilidad y/o el derecho a utilización del correspondiente módulo de aplicación 11, 11'. El módulo de liberación 13 está preparado para restablecer la utilización de uno o varios módulos de aplicación 11, 11', es decir para establecer y garantizar (de nuevo o eventualmente por primera vez) la disponibilidad y/o l autorización para la utilización de los módulos de aplicación respectivos 11, 11'. El módulo de control 14 está preparado para activar el módulo de liberación 13 respective restablecer la utilización, así como para activar el módulo de bloqueo 12 respective suspender la utilización, dependiendo de la utilización de uno o varios módulos de aplicación 11, 11', es decir dependiendo de unas condiciones definidas relativas a la utilización de los módulos de aplicación 11, 11'. Los módulos de función están realizados preferentemente como módulos de software programados. Los módulos de función comprenden códigos de programa informático para el control de uno o varios procesadores que se encuentren en el dispositivo sobre el cual está realizado el módulo de seguridad 1. Tal como está representado esquemáticamente en la figura 1, el módulo de seguridad 1 está realizado preferentemente como dispositivo que está unido de modo liberable con el equipo terminal de comunicaciones 10, preferentemente como tarjeta chip, en particular como módulo de identificación del abonado en forma de una tarjeta SIM. Tal como está representado esquemáticamente en la figura 2, en una de las variantes, el módulo de seguridad está organizado como producto de programa informático que está incorporado directamente en el equipo terminal de comunicaciones 10 y que controla uno o varios procesadores del equipo terminal de comunicaciones 10. El especialista entenderá que los módulos de función también pueden estar realizados en parte o en su totalidad en forma de hardware. El equipo terminal de comunicaciones 10 comprende por lo menos un módulo de comunicaciones para la comunicación de datos a través de redes de telecomunicación 2, 4. El equipo terminal de comunicaciones 10 está realizado por ejemplo como radioteléfono móvil, PDA (Personal Data Assistant), laptop o como ordenador personal. La red de telecomunicaciones 2 comprende preferentemente una red de telefonía móvil, por ejemplo una red GSM (Global System for Mobile Communication), una red UMTS (Universal Mobile Telephone System), otro sistema de radiotelefonía móvil, por ejemplo basado en satélites y/o una WLAN (pública). El especialista entenderá que la red de telecomunicaciones 2 también puede comprender una red fija, por ejemplo una ISDN (Red Digital de Servicios Integrados) o Internet. La red de telecomunicaciones 4 se corresponde tecnológicamente por ejemplo con la red de telecomunicaciones 2, pero presenta otra identificación de red diferente (por ejemplo otro código de red móvil MNC) y es explotado típicamente por otro explotador. En la figura 1, la referencia 3 se refiere a una central de autentificación, que por el lado de la red soporta la autentificación de la red de extremo a extremo por medio del módulo de seguridad 1. La referencia 5 se refiere a un módulo de control de autorización que no tiene no tiene por qué estar realizado en la central de autentificación 3, sino que puede estar asignado a otra unidad de red de la red de telecomunicaciones 2, por ejemplo a un servidor de control de autorización. El módulo de control de autorización 5 está realizado preferentemente como producto de programa informático, que incluye códigos del programa informático para el control de uno o varios procesadores de una unidad de red de la red de telecomunicaciones 2. Con respecto a la función del módulo de control de autorización 5 se tratará más adelante.

En los siguientes apartados se explica el funcionamiento del módulo de seguridad 1, haciendo para ello referencia a las figuras 3 a 6. En las figuras 3 a 6, las referencias 7, 7' se refieren a módulos de aplicación (Client Applications) del equipo terminal de comunicaciones 10; la referencia 8 se refiere al entorno del tiempo de funcionamiento (Client Execution Environment) del equipo terminal de comunicaciones 10. La referencia 9 se refiere a un módulo de control de incidentes (Client Event Handler) del equipo terminal de comunicaciones 10; la referencia 6 se refiere a una puerta de red, y la referencia 17 se refiere al entorno del tiempo de funcionamiento (Execution Environment) del módulo de seguridad 1. Las figuras 3 a 6 reproducen una presentación lógica/funcional. El flujo de datos y el flujo de control a nivel de aplicación entre un módulo de aplicación activo 11 del módulo de seguridad 1, y un módulo de aplicación 7 asignado al equipo terminal de comunicaciones 10 están indicados en las figuras 3 a 6 por medio del paso S7. Con el paso S7' se indica esquemáticamente en los eventos tales como la selección de una aplicación (por ejemplo módulo de aplicación 11 del módulo de seguridad 1) se activan por los módulos de aplicación 7 del equipo terminal de comunicaciones 10.

Tal como está representado en las figuras 3 a 6, en el entorno de tiempo de funcionamiento 17 del módulo de seguridad 1 se reciben en el paso S1' datos procedentes de la central de autentificación 3 o del módulo de control de autorización 5, que se conducen por ejemplo en el paso S1 a través del puerto de la red 6. Los datos de la central de autentificación 3 comprenden datos de autentificación que se transmitieron durante la autentificación de la red de telecomunicaciones 2 al módulo de seguridad 1 para señalar la autentificación de la red de telecomunicaciones 2. Los datos del módulo de autorización 5 comprenden por lo menos un mensaje de autorización que se transmite desde el módulo de control de autorización 5 al módulo de seguridad 1. El mensaje de autorización se puede autentificar y se puede retransmitir a la red de telecomunicaciones 2 respective al módulo de control de autorización

5, a un correspondiente servidor de control de autorización o a un prestador de servicios de confianza. El mensaje de autorización comprende por ejemplo datos de autorización con instrucciones para la liberación o restablecimiento del derecho de utilización de uno o varios módulos de aplicación 11, 11'. Los datos de autorización pueden generarse también implícitamente en el módulo de seguridad basándose en un mensaje de autorización recibido. En el entorno del tiempo de funcionamiento 17 del módulo de seguridad 1 se pueden recibir también de un servidor de tiempo de confianza sellos de tiempo autentificables a través de la red de telecomunicaciones 2, 4. Además, el entorno del tiempo de funcionamiento 17 del módulo de seguridad 1 se reciben en el paso S2' datos procedentes del entorno del tiempo de funcionamiento 8 del equipo terminal de comunicaciones 10, que se conducen por ejemplo en el paso S2 a través del módulo de control de eventos 9 del equipo terminal de comunicaciones 10. Los datos del entorno del tiempo de funcionamiento 8 comprenden instrucciones para la selección y activación de módulos de aplicación 11, 11', para la selección y activación de funciones de los módulos de aplicación 11, 11', así como para la reposición (reset) del módulo de seguridad 1.

Tal como está representado en las figuras 3 a 5, los datos recibidos del entorno de tiempo de funcionamiento 17 del módulo de seguridad 1 se retransmiten en el paso S3 al módulo de control 14.

Tal como está representado en la figura 6, el módulo de seguridad 1 comprende en una variante de realización varios módulos de control 14', 14'', que están asignados cada uno a uno de los módulos de aplicación 11, 11'. En la variante de realización según la figura 6 se retransmiten los datos del entorno del tiempo de funcionamiento 8 que se refieren al control de uno de los módulos de aplicación 11, 11', en el paso S3' respectivamente al módulo de control 14', 14'' correspondiente asignado. En la variante de realización según la figura 6 se retransmiten además los mensajes de autorización para uno o varios módulos de aplicación determinados en el paso S3' en cada caso al módulo de control 14', 14'' correspondiente asignado.

Tal como está representado en las figuras 3 y 4, el módulo de control 14 actualiza en el paso S4 el registro de autorización 16 basándose en los mensajes de autorización recibidos o en datos de autentificación que señalan la autentificación de la red de telecomunicaciones 2. Basándose en los mensajes de autorización recibidos o en los datos de autentificación, el módulo de control 14 activa el módulo de autorización 13 que en el paso S6 libera la utilización de uno, de varios o de todos los módulos de aplicación 11, 11' o la restablece. La liberación o el restablecimiento de la utilización de un módulo de aplicación 11, 11' se consigue por medio del módulo de liberación 13 porque se activa, se desbloquea, se despierta, se instala o se presenta en una lista el módulo de aplicación respectivo 11, 11'. También se puede borrar una marca de bloqueo que es leída por el módulo de aplicación 11, 11'. El registro de autorizaciones 16 comprende condiciones de autorización para uno o varios módulos de aplicación determinados 11, 11' o para la totalidad de los módulos de aplicación 11, 11' del módulo de seguridad 1. Las condiciones de autorización comprenden por ejemplo para uno o varios módulos de aplicación 11, 11' el número autorizado de utilizaciones del módulo de aplicación 11, 11', el número autorizado de selecciones del módulo de aplicación 11, 11', el número autorizado de utilizaciones de funciones del módulo de aplicación 11, 11', el número autorizado de sesiones a través de un canal lógico del módulo de aplicación 11, 11', el número autorizado de ciclos de reposición del módulo de seguridad 1 y/o el tiempo autorizado de utilización del módulo de aplicación 11, 11'. Las condiciones de autorización se establecen en el registro de autorizaciones 16, basándose por ejemplo en las instrucciones de restablecimiento recibidas o en los datos de autentificación, para lo cual las condiciones de autorización están contenidas en las instalaciones de restablecimiento o están almacenadas de forma oculta en el módulo de seguridad 1.

La liberación o el establecimiento de la utilización de un módulo de aplicación basándose en datos de autentificación recibidos está ligada en una variante a unas condiciones adicionales que especifican por ejemplo un número determinado de autentificaciones de la red de telecomunicaciones 2, dentro de un periodo de tiempo definido.

Tal como está representado en las figuras 5 y 6, el módulo de seguridad 1 comprende en una variante de realización varios registros de autorización 16, 16', que están asignados cada uno a uno de los módulos de aplicación 11, 11'. En la variante de realización según las figuras 5 y 6 el módulo de control 14 (respective 14', 14'') actualiza en el paso S4' cada vez el correspondiente registro de autorización 16, 16', basándose en los mensajes de autorización o datos de autentificación requeridos.

Con el fin de perseguir y reconducir autorizaciones que se modifiquen, el módulo de seguridad 1 dispone de uno o varios registros de expiración 15, 15'. La figura 3 ilustra una variante de realización en la que el módulo de seguridad 1 presenta un registro de expiración. Las figuras 4 a 6 ilustran variantes de realización preferentes en las que el módulo de seguridad 1 comprende varios registros de expiración 15, 15' que están asignados cada uno respectivamente a un módulo de aplicación 11, 11'. En el registro de expiración 15, 15' se almacenan indicaciones relativas a actividades realizadas o pendientes de realizar, relacionadas con uno o varios módulos de aplicación 11, 11'. Si el registro de expiración 15, 15' está preparado como registro incremental, los valores de tiempo o el numero de actividades (utilizaciones) se van contando en aumento partiendo de cero. Si el registro de expiración 15, 15' está preparado como registro decremental, los valores de tiempo o el número de actividades (utilizaciones) se van descontando partiendo de un valor límite inicial (condición de autorización). El registro de expiración 15, 15' comprende en particular datos relativos al número de utilizaciones del módulo de aplicación 11, 11', al número de selecciones del módulo de aplicación 11, 11', al número de utilizaciones de funciones del módulo de aplicación 11, 11', al número de sesiones establecidas a través de un canal lógico y el módulo de aplicación 11, 11', al número de

ciclos de reposición del módulo de seguridad 1 y/o a un periodo de tiempo, por ejemplo el tiempo transcurrido desde la concesión de la autorización. El especialista entenderá que el registro de expiración 15, 15' se puede corresponder con el registro de autorización 16, 16', en cuyo caso el armado del registro de autorización 16 equivale al armado de un valor de inicialización del registro de expiración 15, que a lo largo del tiempo o en función de su utilización se va decrementando.

Si los datos recibidos comprenden una petición relativa a uno de los módulos de aplicación 11, 11' o una petición de reposición del módulo de seguridad 1, el módulo de control 14, 14' actualiza en el paso S5, S5' el correspondiente registro de expiración 15, 15' y comprueba la autorización para la selección o activación del módulo de aplicación afectado 11, 11' respective una función del módulo de aplicación afectado 11, 11'. La comprobación de la autorización se basa en el correspondiente registro de autorización 16, 16' y/o en el correspondiente registro de expiración 15, 15'. En el caso del registro de expiración 15, 15' incremental, deja de estar presente ninguna autorización cuando el valor incrementado alcanza o rebasa el correspondiente valor máximo admisible (el número de utilizaciones) en el registro de autorización 16, 16'. En el registro de expiración decremental 15, 15' deja de existir ninguna autorización cuando el valor decrementado, partiendo del valor máximo admisible original (por ejemplo el número de selecciones) del registro de autorización 16, 16' alcanza el valor cero. Si no existe ninguna autorización se genera por ejemplo un mensaje de confirmación de fallo a la unidad que hace la solicitud. Si la autorización queda anulada debido a la petición presente, el módulo de control 14 activa el módulo de bloqueo 12 que anula la posibilidad de utilización de uno, de varios o de todos los módulos de aplicación 11, 11'. La suspensión de la posibilidad de utilización de un módulo de aplicación 11, 11' se consigue mediante el módulo de bloqueo 11 porque se desactiva, bloquea, hiberna, o desinstala el módulo de aplicación afectado 11, 11' o porque al retirarlo se oculta de una lista. También se puede colocar una marca de bloqueo que al efectuar la aplicación por parte del módulo de aplicación 11, 11' se lee ella misma, a continuación de lo cual el módulo de aplicación 11, 11' da por terminada su actividad. En caso contrario, si existe una autorización, se selecciona y activa el módulo de activación correspondiente 11, 11', respective la función afectada. En una variante de realización alternativa se actualiza el registro de expiración 15, tal como está indicado en la figura 3, en el paso S8 por el respectivo módulo de aplicación 11. En la variante de realización con varios registros de expiración 15, 15' se actualiza en el paso S8' el registro de expiración 15, tal como está indicado en las figuras 4 a 6, que corresponda al respectivo módulo de aplicación 11, 11'.

En el módulo de seguridad 11 pueden estar previstos también varios registros de expiración 15, 15' y registros de autorización 16, 16' para los módulos de aplicación 11, 11' de distintas redes de telecomunicación 2 respective explotadores.

REIVINDICACIONES

1. Un módulo de seguridad (1) realizado como dispositivo para un equipo terminal de comunicaciones (10), cuyo módulo de seguridad (1) está preparado para autentificar una red de telecomunicación (2) y cuyo módulo de seguridad (1) comprende por lo menos un módulo de aplicación (11) utilizable, comprendiendo el módulo de aplicación (11) un código de programa informático para control de un procesador, **caracterizado por**

un módulo de bloqueo (12) para anular la posibilidad de utilización del módulo de aplicación (11),

un módulo de liberación (13) para restablecer la posibilidad de utilización del módulo de aplicación (11), y

un módulo de control (14) para activar el módulo de liberación (13) para restablecer la posibilidad de utilización del módulo de aplicación (11) dependiendo de un mensaje de autorización recibido que se pueda asignar de modo autentificable a una determinada red de telecomunicaciones (2), y de los datos de autentificación recibidos que se puedan designar a la red de telecomunicaciones (2).

2. Módulo de seguridad (1) según la reivindicación 1, **caracterizado porque** el módulo de control (14) está además preparado para activar el módulo de bloqueo (12) dependiendo de por lo menos de uno de entre: un número de utilizaciones del módulo de aplicación (11), un número de selecciones del módulo de aplicación (11), un número de utilización de las funciones del módulo de aplicación (11), un número de sesiones a través de un canal lógico del módulo de aplicación (11), un número de ciclos de reposición del módulo de seguridad (1) y de que se alcance un determinado periodo de tiempo transcurrido.

3. Módulo de seguridad (1) según una de las reivindicaciones 1 ó 2, **caracterizado porque** el módulo de bloqueo (12) está preparado para suspender la posibilidad de utilización del módulo de aplicación (11) por medio de uno de entre: desactivación, bloqueo, ocultación, hibernación y desinstalación del módulo de aplicación (11) y porque el módulo de liberación (13) está preparado para restablecer correspondientemente la posibilidad de utilización del módulo de aplicación (11) por medio de uno de entre: activación, desbloqueo, relación, despertar e instalación del módulo de aplicación (11).

4. Módulo de seguridad (1) según una de las reivindicaciones 1 a 3, **caracterizado porque** comprende por lo menos un registro de expiración (15) que está asignado a uno o a varios módulos de aplicación (11) y porque el módulo de control (14) está preparado para almacenar en el registro de expiración (15) datos actuales a través de por lo menos uno de entre: el número de utilizaciones del módulo de aplicación (11), el número de selecciones del módulo de aplicación (11), el número de utilizaciones de funciones del módulo de aplicación (11) el número de sesiones a través de un canal lógico del módulo de aplicación (11), el número de ciclos de reposición del módulo de seguridad (1) y el tiempo transcurrido.

5. Módulo de seguridad (1) según una de las reivindicaciones 1 a 4, **caracterizado porque** comprende por lo menos un registro de autorización (16) que está asignado a uno o a varios módulos de aplicación (11), y porque el módulo de control (14) está preparado para almacenar datos en el registro de autorización (16) relativos a por lo menos uno de entre: un número autorizado de utilizaciones del módulo de aplicación (11), un número autorizado de selecciones del módulo de aplicación (11), un número autorizado de utilizaciones de funciones del módulo de aplicación (11), un número autorizado de sesiones a través de un canal logístico del módulo de aplicación (11), un número autorizado de ciclos de reposición del módulo de seguridad (1) y de que se alcance el tiempo autorizado.

6. Módulo de seguridad (1) según una de las reivindicaciones 1 a 5, **caracterizado porque** está realizado como dispositivo, en particular como tarjeta chip que se puede unir de modo liberable con el equipo terminal de comunicaciones (10).

7. Módulo de seguridad (1) según una de las reivindicaciones 1 a 6, **caracterizado por** estar realizado como módulo de identificación del abonado y porque está realizado para un equipo terminal de comunicaciones (10) preparado para redes de radiotelefonía móvil.

8. Producto de programa informático comprendiendo: medios de codificación de un programa informático para control de uno o varios procesadores de un módulo de seguridad (1) realizado como dispositivo para un equipo terminal de comunicaciones (10), cuyo módulo de seguridad (1) está preparado para autentificar una red de telecomunicaciones (2), y cuyo módulo de seguridad (1) comprende por lo menos un módulo de aplicación (11) utilizable, comprendiendo el módulo de aplicación (11) un código de programa informático para el control de un procesador, de tal modo que,

el módulo de seguridad (1) realiza una suspensión de la posibilidad de utilización del módulo de aplicación (11),

porque el módulo de seguridad (1) realiza un restablecimiento de la posibilidad de utilización del módulo de aplicación (11), y

porque el módulo de seguridad (1) activa el restablecimiento de la posibilidad de utilización del módulo de aplicación (11), dependiendo de uno de entre: mensaje de autorización recibido que se pueda asignar de modo autentificable a

una determinada red de telecomunicaciones (2), y datos de autentificación recibidos, que son asignables a la red de telecomunicaciones (2).

9. Procedimiento para controlar la posibilidad de utilización de un módulo de aplicación (11), comprendiendo el módulo de aplicación (11) un código de programa informático para controlar un procesador, y que está dispuesto en un módulo de seguridad (1) realizado como dispositivo para un equipo terminal de comunicaciones (10), comprendiendo el módulo de seguridad (1) un módulo de bloqueo (12), un módulo de autorización (13) y un módulo de control (14), estando preparado para autentificar una red de telecomunicaciones (2), **caracterizado por**

poder suspender la posibilidad de utilización del módulo de aplicación (11) por el módulo de bloqueo (12) del módulo de seguridad (1),

poder restablecer la posibilidad de utilización de un módulo de aplicación (11) por el módulo de liberación (13) del módulo de seguridad (1), y

poder activar el restablecimiento de la posibilidad de utilización del módulo de aplicación (11) por el módulo de control (14) del módulo de seguridad (1) dependiendo de uno de entre: mensaje de autorización recibido que se pueda asignar de modo autentificable a una determinada red de telecomunicaciones (2), y datos de autentificación recibidos que son asignables a la red de telecomunicaciones (2).

10. Procedimiento según la reivindicación 9, **caracterizado porque** la suspensión de la posibilidad de utilización del módulo de aplicación (11) se activa dependiendo de por lo menos de uno de entre: número de utilizaciones del módulo de aplicación (11), número de selecciones del módulo de aplicación (11), número de utilizaciones de las funciones del módulo de aplicación (11), número de sesiones a través de un canal lógico del módulo de aplicación (11), número de ciclos de reposición del módulo de seguridad (1) y llegar a alcanzar un determinado tiempo.

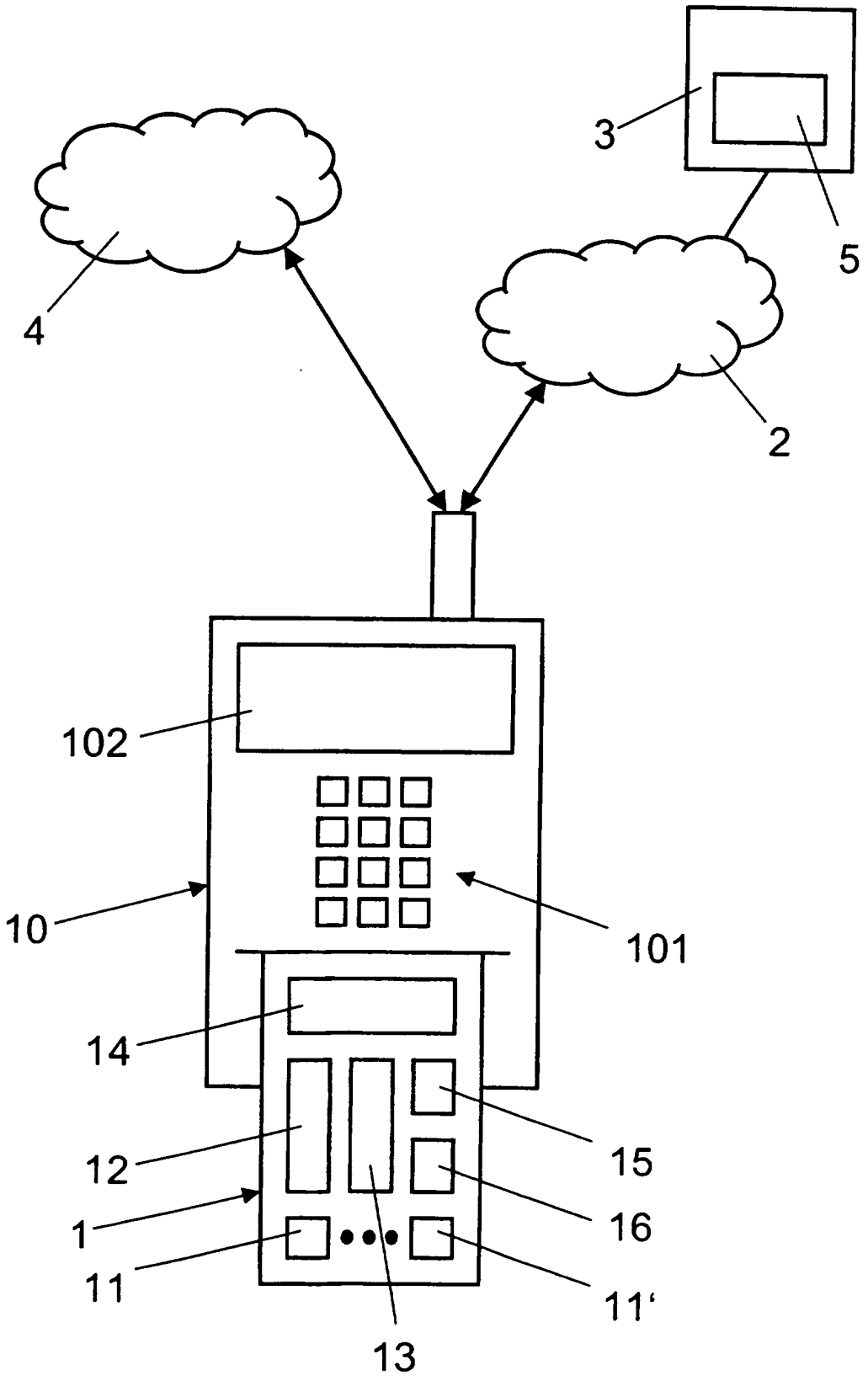

Fig. 1

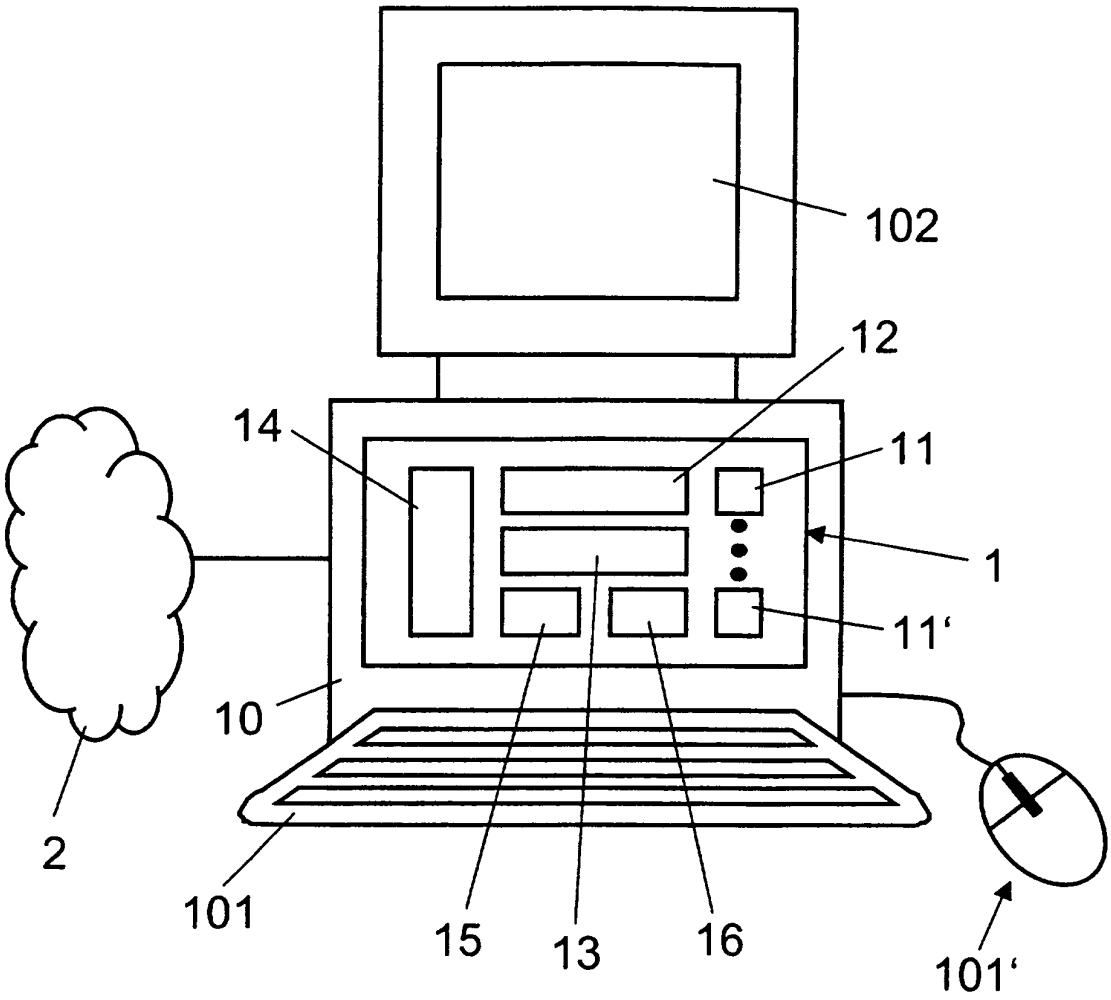

Fig. 2

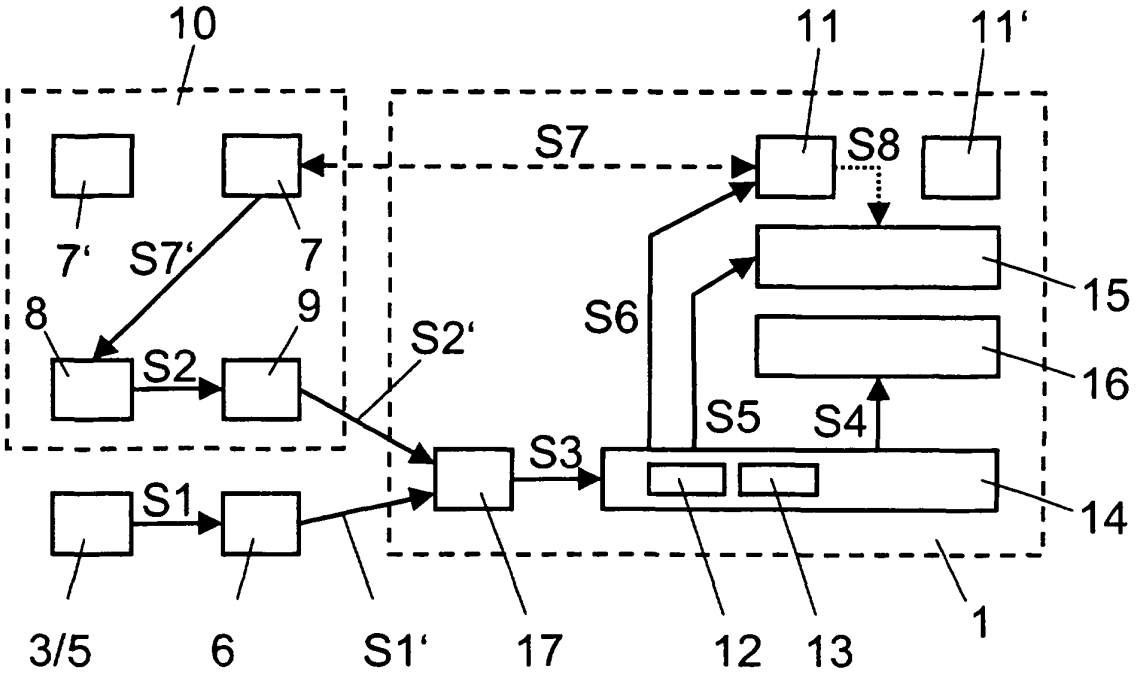
10
11
11‘
S7
S8
7‘
S7‘
7
8
9
S2
S2‘
S6
15
16
S5
S4
S3
S1
14
3/5
6
S1‘
17
12
13
1

Fig. 3

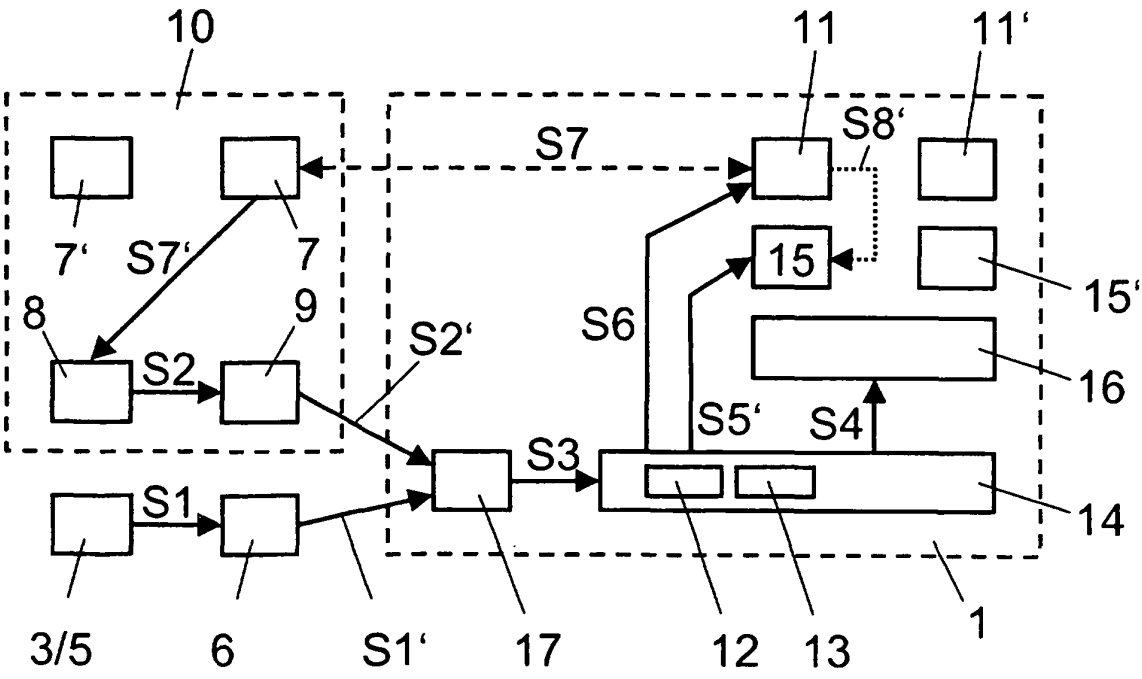
10
11
11‘
S7
S8‘
7‘
S7‘
7
15
15‘
8
9
S2
S2‘
S6
16
S5‘
S4
S3
S1
14
3/5
6
S1‘
17
12
13
1

Fig. 4

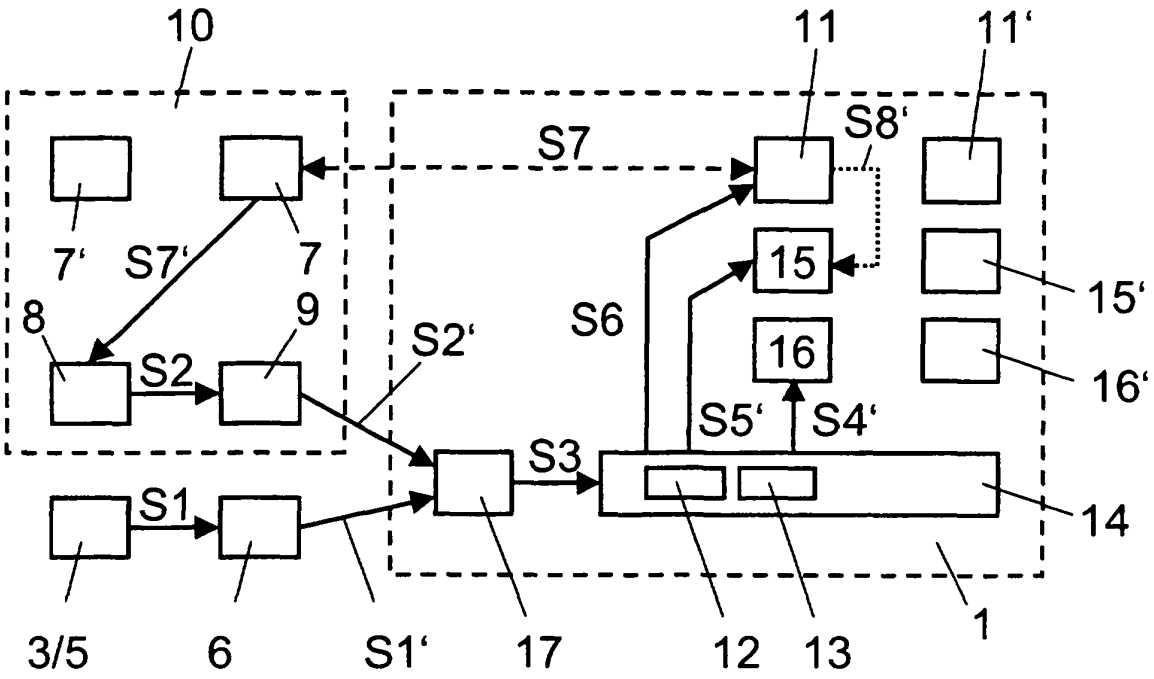
10
11
11‘
S7
S8‘
7‘
S7‘
7
15
15‘
8
9
S6
S2‘
16
16‘
S2
S5‘
S4‘
S3
S1
14
3/5
6
S1‘
17
12
13
1

Fig. 5

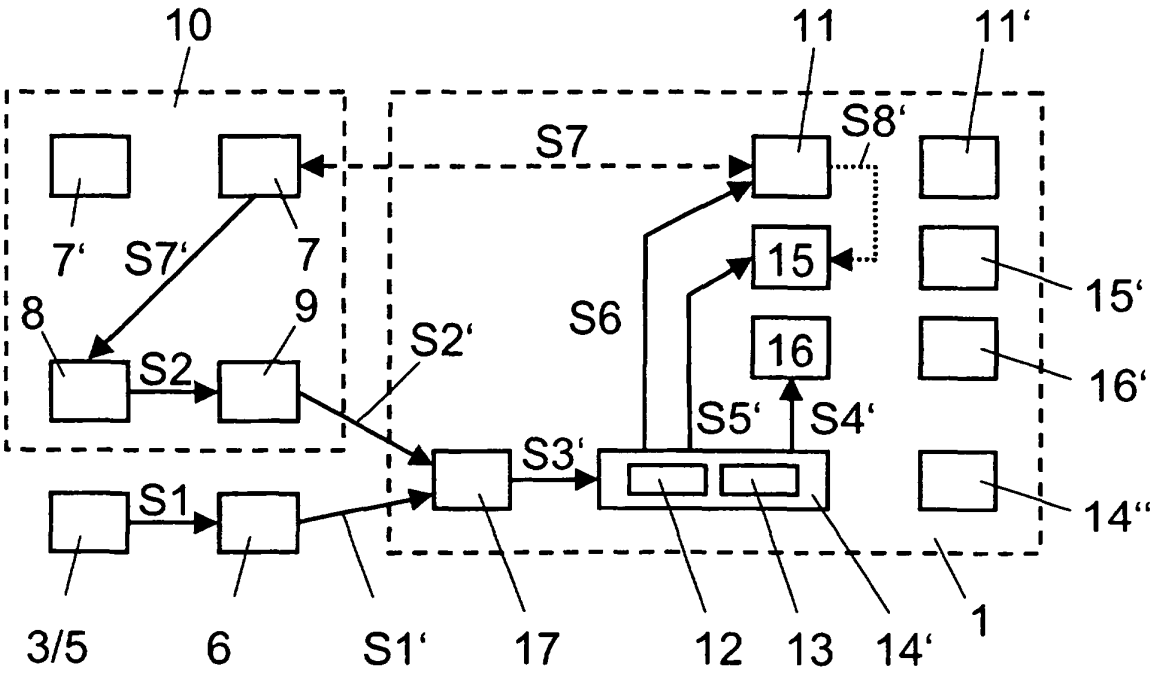
10
11
11‘
S7
S8‘
7‘
S7‘
7
15
15‘
8
9
S6
S2‘
16
16‘
S2
S5‘
S4‘
S3‘
S1
14‘
3/5
6
S1‘
17
12
13
14‘
1

Fig. 6