(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 384 952**

(51) Int. CI.:
H04W 12/02 (2009.01)
G07F 7/10 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **00988676 .3**
(96) Fecha de presentación: **01.12.2000**
(97) Número de publicación de la solicitud: **1240794**
(97) Fecha de publicación de la solicitud: **18.09.2002**

(54) Título: **Procedimiento para la codificación de datos y terminal de telecomunicaciones y tarjeta de autorización de acceso**

(30) Prioridad:
07.12.1999 DE 19958749
07.04.2000 DE 10017424

(45) Fecha de publicación de la mención BOPI:
16.07.2012

(45) Fecha de la publicación del folleto de la patente:
16.07.2012

(73) Titular/es:
IPCOM GMBH & CO. KG
ZUGSPITZSTRASSE 15
82049 PULLACH, DE

(72) Inventor/es:
HANS, Martin;
KOWALEWSKI, Frank;
LAUMEN, Josef;
SCHMIDT, Gunnar;
BAER, Siegfried;
BECKMANN, Mark y
ADI, Wael

(74) Agente/Representante:
Carvajal y Urquijo, Isabel

DESCRIPCIÓN

Procedimiento para la codificación de datos y terminal de telecomunicaciones y tarjeta de autorización de acceso.

Estado de la técnica

La invención parte de un procedimiento para la codificación de datos, de un terminal de telecomunicaciones y de una tarjeta de autorización de acceso del tipo de las reivindicaciones inde0pendientes.

Ya se conoce, por ejemplo, en telefonía móvil, transmitir datos entre un proveedor de servicios y un teléfono móvil a través de una red de telefonía móvil, por ejemplo para cargar E-Mails de Internet desde el proveedor de servicios en el teléfono móvil. En este caso, se conoce, por ejemplo, para un sistema de telefonía móvil según la Norma GSM (Global System for Mobile Communications) a partir de la publicación “GSM GIobal System for Mobile Communication” J. Eberspräcber, H, J. Vögel, B. G. Treubner, Stuttgart, 1997, codificar datos a transmitir a través de la red de telefonía móvil en una unidad de codificación correspondiente y de esta manera protegerlos contra acceso no autorizado. A este respecto, según la Norma GSM, se establece la clave, con la que se codifican los datos a transmitir, desde el sistema de telefonía móvil y, por lo tanto, desde el operador de la red. Por lo tanto, el control a través de esta clave está en el operador de la red, en el que está dado de alta precisamente el teléfono móvil. La funcionalidad de codificación presente en el teléfono móvil no puede ser utilizada, por lo tanto, por el usuario del teléfono móvil independientemente del operador de la red.

Además, ya se conoce a partir de la publicación “Radio Interface Protocol Architecture”, 3GPP TSG RAN WG2, TS25.301 v. 3.1.0, utilizar la unidad de codificación del teléfono móvil para codificar un identificador de aparatos del teléfono móvil y de esta manera protegerlo contra acceso no autorizado durante su transmisión hacia la red de telefonía móvil. El identificador de aparatos está predeterminado, sin embargo, por el fabricante del teléfono móvil. El usuario del teléfono móvil no puede utilizar, por lo tanto, la funcionalidad de codificación presente en el teléfono móvil tampoco independientemente del fabricante del teléfono móvil.

El documento WO/9939524 publica la codificación de mensajes entre una estación móvil y una red con una clave privada.

Ventajas de la invención

El procedimiento de acuerdo con la invención y el terminal de telecomunicaciones de acuerdo con la invención con las características de las reivindicaciones independientes tienen, sin embargo, la ventaja de que los datos a transmitir a través de la red de telecomunicaciones son codificados en función del proveedor de servicios seleccionado. De esta manera, no es necesaria una codificación predeterminada por el fabricante del terminal de telecomunicaciones o por el operador de la red de telecomunicaciones, de manera que se puede realizar una funcionalidad de codificación del terminal de telecomunicaciones independientemente del operador de la red y casi independientemente del fabricante del terminal de telecomunicaciones. En la codificación de datos a transmitir no hay que confiar ya en la asignación de claves a través del operador de la red o del fabricante del terminal de telecomunicaciones. La protección de datos a transmitir contra acceso no autorizado está más bien, de acuerdo con la invención, en manos del proveedor de servicios y del usuario del servicio en forma del terminal de telecomunicaciones y no en el operador de la red o en el fabricante del terminal de telecomunicaciones.

Otra ventaja consiste en que los datos a transmitir entre el terminal de telecomunicaciones y el proveedor de servicios están codificados a través de todo el trayecto de transmisión, de manera que resulta una llamada codificación de datos de extremo a extremo entre el terminal de telecomunicaciones y el proveedor de servicios. Los datos a enviar al proveedor de servicios no son descodificados entonces por el proveedor de servicios antes de llegar al proveedor de servicios para que sean transmitidos protegidos contra acceso no autorizado totalmente hacia el proveedor de servicios.

Otra ventaja consiste en que se posibilita una autentificación del terminal de telecomunicaciones directamente en el proveedor de servicios, cuando los datos a transmitir comprenden un identificador de aparatos del terminal de telecomunicaciones. Por lo tanto, la autentificación tiene lugar allí donde se decide también sobre el acceso del terminal de telecomunicaciones a servicios del proveedor de servicios, a saber, en el propio proveedor de servicios y no delante del proveedor de servicios en el operador de la red, que no tiene ninguna capacidad de decisión sobre el acceso a los servicios del proveedor de servicios. Por lo tanto, a través de la invención se posibilita la autentificación del terminal de telecomunicaciones directamente en el proveedor de servicios y, por consiguiente, es especialmente fiable. Lo mismo se aplica de una manera correspondiente a la inversa para una autentificación del proveedor de servicios en el terminal de telecomunicaciones.

En virtud de la invención, el usuario del terminal de telecomunicaciones obtiene la posibilidad de utilizar servicios seguros de un proveedor de servicios discrecional. En adelante no depende ya de utilizar el operador de la red también como proveedor de servicios o de utilizar proveedores de servicios preferidos por el operador de la red, sino que puede utilizar a su elección servicios de un proveedor opcional de servicios sin conocer el operador de la red o

el fabricante.

Independientemente del operador de la red y del fabricante del terminal de telecomunicaciones se pueden asignar clases secretas, que posibilitan una identificación unívoca y segura del usuario del terminal de telecomunicaciones y/o del proveedor de servicios. De esta manera, se posibilita una autentificación segura del usuario del terminal de telecomunicaciones en el proveedor de servicios y del proveedor de servicios en el terminal de telecomunicaciones, sin que el operador de la red o el fabricante del terminal de telecomunicaciones tengan ninguna influencia. A tal fin no es necesaria ninguna funcionalidad de codificación adicional en el terminal de telecomunicaciones.

A través de la disposición de la funcionalidad de codificación sobre una tarjeta de autorización e acceso resulta adicionalmente la ventaja de que la funcionalidad de la codificación no está establecida a través del hardware del terminal de telecomunicaciones, sino que se puede sustituir con la tarjeta de autorización de acceso. De esta manera se pueden poner a disposición técnicas y algoritmos de codificación nuevos y mejorados para el terminal de telecomunicaciones. Por medio de la funcionalidad de codificación en la tarjeta de autorización de acceso se puede conseguir una independencia completa de la codificación del hardware y, por lo tanto, del fabricante del terminal de telecomunicaciones y adicionalmente se puede utilizar la posibilidad de la adaptación a la capacidad de potencia que se eleva rápidamente de los microprocesadores, cuando ésta se aplica en la tarjeta de autorización de acceso. La tarjeta de autorización de acceso puede ser asignada por el proveedor de servicios a un usuario del terminal de telecomunicaciones, sin que el fabricante de aparatos o el proveedor de la red estén implicados. Cuando en el transcurso del tiempo los circuitos integrados y los microprocesadores se vuelven conductores, entonces el proveedor de servicios puede conceder fácilmente al usuario una nueva tarjeta de autorización de acceso con funcionalidad de codificación mejorada. El usuario debe sustituir entonces solamente la tarjeta de autorización de acceso en su terminal de telecomunicaciones para poder acceder a la funcionalidad mejorada de la nueva tarjeta de autorización de acceso.

A través de las medidas indicadas en las reivindicaciones dependientes son posibles desarrollos ventajosos y mejoras del procedimiento para la codificación de datos y del terminal de telecomunicaciones de acuerdo con las reivindicaciones independientes.

Es especialmente ventajoso que para la transmisión de los datos se utilice un servicio del proveedor de servicios seleccionado y que los datos a transmitir a través de la red de telecomunicaciones sean codificados en función del servicio seleccionado. De esta manera se puede asegurar también la transmisión de datos por medio de servicios individuales ofrecidos por un proveedor de servicios, respectivamente, a través de una clave propia. El número de las claves secretas utilizadas y, por lo tanto, del servicio asegurado no está en este caso, en principio, limitado.

Otra ventaja consiste en que con la clave seleccionada para la autentificación del terminal de telecomunicaciones se codifican también los datos útiles a transmitir. De esta manera se puede ahorrar el número de las claves a memorizar en el terminal de telecomunicaciones y, por lo tanto, espacio de memoria.

Dibujo

Los ejemplos de realización de la invención se representan en el dibujo y se explican en detalle en la descripción siguiente. La figura 1 muestra un diagrama de bloques de un terminal de telecomunicaciones de acuerdo con la invención, la figura 2 muestra un diagrama de bloques de una estación de base y de un proveedor de servicios conectado con la estación de base a través de una puerta de acceso para la descripción de un proceso de autentificación, la figura 3 muestra un diagrama de bloques de una estación de base y de un proveedor de servicios conectado con la estación de base a través de una puerta de acceso para una transmisión de datos útiles codificados, la figura 4 muestra un diagrama de bloques de un terminal de telecomunicaciones con tarjeta de autorización de acceso de acuerdo con la invención insertada y la figura 5 muestra un diagrama de bloques de una estación de base y de un proveedor de servicios, conectado con la estación de base a través de una puerta de acceso con una unidad de protocolo para la intercambio de datos con la tarjeta de autorización de acceso insertada en el terminal de telecomunicaciones.

Descripción de los ejemplos de realización

En la figura 1, el número 5 identifica un terminal de telecomunicaciones, que puede estar configurado, por ejemplo, conectado por cable, sin cables o sin hilos. En la configuración como terminal de telecomunicaciones conectado por cable, se puede tratar, por ejemplo, de un terminal de telecomunicaciones de acuerdo con la Norma ISDB (Integrated Services Digital Network). En la configuración como terminal de telecomunicaciones sin cables se puede tratar, por ejemplo, de un terminal de telecomunicaciones de acuerdo con la Norma DECT (Digital European Cordless Telecommunications). En la configuración como terminal de telecomunicaciones sin hilos se puede tratar, por ejemplo, de un terminal de telecomunicaciones de acuerdo con la Norma GSM (Global System for Mobile Communications) o de acuerdo con la Norma UMTS (Universal Mobile Telecommunications System). A continuación se supone a modo de ejemplo que el terminal de telecomunicaciones 5 está configurado como terminal de telecomunicaciones sin hilos en forma de un teléfono móvil según la Norma UMTS.

El teléfono móvil 5 comprende en este caso un primer dispositivo de emisión 25, que debe estar configurado a continuación a modo de ejemplo como primer dispositivo de emisión / recepción. El teléfono móvil 5 comprende, además, un primer módulo de aplicación 30, que está conectado con el primer dispositivo de emisión / recepción 25. El primer módulo de aplicación 30 está conectado, por otra parte, con módulo de codificación 40, que comprende una primera unidad de codificación 15. En este caso, la primera unidad de codificación 15 está conectada directamente con el primer módulo de aplicación 30. El módulo de codificación 40 comprende, además, un control de direcciones 35, que está conectado de la misma manera directamente con el primer módulo de aplicación 30. El módulo de codificación 40 comprende, además, una memoria 20 con un primer espacio de memoria 21, un segundo espacio de memoria 22, un tercer espacio de memoria 23 y un n espacio de memoria 24, siendo n, en general, un número entero y mayor o igual a 1. En este ejemplo, n se selecciona mayor o igual a 4. En el primer espacio de memoria 21está memorizada una primera clave 11. En el segundo espacio de memoria 22 está memorizada una segunda clave 12. En el tercer espacio de memoria 23 está memorizada una tercera clave 13. En el n espacio de memoria 24 está memorizada una n clave 14. El control de direcciones 35 está conectado tanto con la memoria 20 como también con la primera unidad de codificación 15. La memoria 20 está conectada, además, con la primera unidad de codificación 15.

A través de una red de telecomunicaciones 10, que debe estar configurada en este ejemplo como red de telefonía móvil, se pueden intercambiar datos entre el teléfono móvil 5 y una estación de base 45 según la figura 2. Según la figura 2, la estación de base 45 está conectada a través de una unidad de conexión 50, que se designa a continuación también como puerta de acceso, con un proveedor de servicios 1. El proveedor de servicios 1 puede proporcionar en este caso los más diferentes servicios de transmisión, como por ejemplo servicios de E-Mail de Internet, servicios de transmisión por vídeo, servicios de fax o similares. La estación de base 45 comprende un segundo dispositivo de emisión / recepción 55, que está conectado con la puerta de acceso 50. En el lado del proveedor de servicios 1, la puerta de acceso 50 está conectada con el segundo módulo de aplicación 60, que está asociado al proveedor de servicios 1 y que está comprendido por el proveedor de servicios 1, y que comprende medios 65 para la generación de una solicitud de identificación. Los medios 65 para la generación de una solicitud de identificación están conectados, por una parte, directamente con la puerta de acceso 50 y, por otra parte, directamente con una segunda unidad de codificación 75, que está asociada de la misma manera al proveedor de servicios 1 y que está comprendida por éste. El segundo módulo de aplicación 60 comprende, además, un comparador 70, que está conectado, por una parte, directamente con la puerta de acceso 50 y, por otra parte, directamente con la segunda unidad de codificación 75. A la segunda unidad de codificación 75 está asociada, además, la segunda clave 12.

Entre el primer dispositivo de emisión / recepción 25 y el segundo dispositivo de emisión / recepción 55 se puede realizar un intercambio de datos a través de la red de telefonía móvil 10. A continuación se supone a modo de ejemplo que el teléfono móvil 5 quiere establecer un comunicación a través de la red de telefonía móvil 10 y la puerta de acceso 50 con el proveedor de servicios 1, para descargar, por ejemplo, E-Mails de Internet desde el proveedor de servicios 1 en el teléfono móvil 5. A tal fin, entre el usuario del teléfono móvil 5 y el proveedor de servicios 1 existe, en general, un contrato. De acuerdo con este contrato, se asegura ahora la utilización del servicio de E-Mail de Internet ofrecido por el proveedor de servicios 1 a través de una clave especial, para impedir en primer lugar que un terminal de telecomunicaciones no autorizado acceda a este servicio en el proveedor de servicios 1 y, en segundo lugar, para impedir que se acceda de manera no autorizada a datos que se transmiten en el marco del servicio de E-Mail de Internet entre el teléfono móvil 5 y el proveedor de servicios 1. A continuación se supone a modo de ejemplo que la clave asociada de esta manera al servicio de E-Mail de Internet del proveedor de servicios es la segunda clave 12. Si se inicia el establecimiento de la comunicación con el proveedor de servicios 1 desde el teléfono móvil 5, entonces esto se puede realizar porque el usuario del teléfono móvil 5 selecciona el número de llamada del proveedor de servicios 1. Por medio del número de llamada se puede elegir o bien seleccionar en este caso también ya un servicio del proveedor de servicios 1. Para el acceso al servicio de E-Mail de Internet del proveedor de servicios 1 es necesaria, en primer lugar, una autentificación del teléfono móvil 5 en el proveedor de servicios 1. A tal fin, los medios 65 generan una solicitud de identificación. La solicitud de identificación es codificada, por una parte, en la segunda unidad de codificación 75 por medio de la segunda clave 12. De esta manera se forma una respuesta de referencia codificada, que se alimenta al comparador 70. Por otra parte, la solicitud de identificación es conducida desde los medios 65 hacia la puerta de acceso 50, desde donde se transmite al segundo dispositivo de emisión / recepción 55 de la estación de base 45 a través de la red de telefonía móvil 10 al teléfono móvil 5. La solicitud de identificación es recibida entonces en el primer dispositivo de emisión / recepción 25 y es transmitida desde allí al primer módulo de aplicación 30. El primer módulo de aplicación 30 detecta la solicitud de identificación a partir de la corriente de datos recibida a través del primer dispositivo de emisión / recepción 25 desde la red de telefonía móvil 10. En este caso, en el primer módulo de aplicación 30 se conoce bajo qué dirección en la memoria 20 o bien en qué espacio de la memoria 20 está depositada la segunda clave 12 asociada al servicio de E-Mail de Internet del proveedor de servicios 1. En particular, para el caso de que el establecimiento de la comunicación no parta desde el teléfono móvil 5 sino desde el proveedor de servicios 1, puede estar previsto que la solicitud de identificación comprenda una identificación del proveedor de servicios y del servicio ofrecido por el proveedor de servicios. El primer módulo de aplicación 30 transmite entonces la solicitud de identificación detectada junto con esta identificación del proveedor de servicios y del servicio ofrecido por el proveedor de servicios al control

de dicciones 35. Con la ayuda de la identificación, el control de direcciones 35 puede detectar el proveedor de servicios iniciador y el servicio seleccionado por él y puede direccional la clave asociada a este proveedor de servicios y al servicio en la memoria 20. El control de direcciones 35 transmite a continuación la solicitud de identificación a la primera unidad de codificación 15 y direcciona la memoria 20 de acuerdo con la identificación evaluada. En el ejemplo descrito aquí, en este caso se direcciona el segundo espacio de memoria 22 con la segunda clave 12, que está asociada al servicio de E-Mail de Internet ofrecido por el proveedor de servicios 1. La segunda clave 12 es transmitida a continuación de la misma manera hacia la primera unidad de codificación 15, que codifica la solicitud de identificación entonces con la segunda clave 12 y de esta manera forma una respuesta codificada. La respuesta codificada es transmitida desde la primera unidad de codificación 15 al primer módulo de aplicación 30 y desde allí al primer dispositivo de emisión / recepción 25 para la difusión a través de la red de telefonía móvil 10 a la estación de base 45. La respuesta codificada es recibida de esta manera en el segundo dispositivo de emisión / recepción 55 y desde allí es transmitida a través de la puerta de acceso 50 al comparador 70. En el comparador 70 se compara la repuesta codificada recibida desde el teléfono móvil 5 con la repuesta de referencia codificada formada en la segunda unidad de codificación 75. Puesto que en la primera unidad de codificación 15 y en la segunda unidad de codificación 75 se aplica el mismo algoritmo de codificación, la solicitud de identificación conduce durante la codificación con la misma clave también a la misma respuesta codificada. Por lo tanto, si la respuesta codificada recibida por el teléfono móvil 5 coincide con la respuesta de referencia codificada en el comparador 70, entonces el teléfono móvil 5 es autentificado con éxito en el proveedor de servicios 1 y tiene autorización de acceso para el servicio de E-Mail de Internet. En otro caso, la autentificación es denegada y se rechaza el acceso al servicio de E-Mail de Internet para el teléfono móvil 5.

Una vez realizada con éxito la autentificación del teléfono móvil 5 en el proveedor de servicios 1, se puede llevar a cabo el intercambio de datos útiles entre el teléfono móvil 5 y el proveedor de servicios 1, para descargar, por ejemplo, por medio del servicio de E-Mail de Internet los E-Mails de Internet existentes en el proveedor de servicios 1 para el teléfono móvil 5 desde el proveedor de servicios 1 en el teléfono móvil 5. Para el intercambio de datos útiles del servicio de E-Mail de Internet entre el teléfono móvil 5 y el proveedor de servicios 1 se puede acordar en este caso una clave de datos útiles, con la que deben codificarse los datos útiles a enviar entre el teléfono móvil 5 y el proveedor de servicios 1 en el marco del servicio de E-Mail de Internet, en particular de los E-Mails de Internet a cargar propiamente dichos, con el fin de asegurarlos contra un acceso no deseado durante la transmisión. La clave de datos útiles se puede distinguir en este caso de la clave necesaria para la autentificación. No obstante, por razones de ahorro de capacidad de memoria también puede coincidir con la clave utilizada para la autentificación. Por lo tanto, a continuación debe suponerse a modo de ejemplo que la clave de datos útiles prevista para el servicio de E-Mail de Internet del proveedor de servicios 1 corresponde a la segunda clave 12. Los datos útiles a enviar en el marco del servicio de E-Mail de Internet desde el teléfono móvil 5 hacia el proveedor de servicio 1 se codifican entonces antes de su transmisión con la segunda clave 12 de la misma manera que la solicitud de identificación para el proceso de autentificación. En este caso, el primer módulo de aplicación 30 suministra, en lugar de la solicitud de identificación, los datos útiles a enviar al proveedor de servicios 1 a través del control de direcciones 35 a la primera unidad de codificación 15, donde se codifican de la manea descrita con la segunda clave 12. Los datos útiles codificados de esta manera son transmitidos entonces de la manera descrita a través del primer módulo de aplicación 30, el primer dispositivo de emisión / recepción 25, la red de telefonía móvil 10, la estación de base 45 y la puerta de acceso 50 hasta el proveedor de servicios 1. De acuerdo con la figura 3, se representa un diagrama de bloques para la estación de base 45, la puerta de acceso 50 y el proveedor de servicios 1, en el que los mismos signos de referencia identifican los mismos elementos que en la figura 2 y que solamente se diferencia con respecto al diagrama de bloques de la figura 2 porque el segundo módulo de aplicación 60 está representado muy en general y sin otros componentes. Los medios 65 necesarios para la autentificación para la generación de la solicitud de identificación y el comparador 70 no son necesarios ya para la fase del intercambio de datos útiles entre el teléfono móvil 5 y el proveedor de servicios 1, pero naturalmente están presentes como anteriormente. El segundo módulo de aplicación 60 tiene ahora, sin embargo, el cometido de descodificar los datos útiles recibidos por el teléfono móvil 5 y de conducir los E-Mails de Internet deseados por el teléfono móvil a una codificación a través de la segunda clave 12 en la segunda unidad de codificación 675 y transmitir los E-Mails de Internet codificados de esta manera a través de la puerta de acceso 50 al segundo dispositivo de emisión / recepción 55 para la difusión a través de la red de telefonía móvil 10 hasta el teléfono móvil 5. Estos E-Mails de Internet son recibidos entonces en el primer dispositivo de emisión / recepción 25 y son transmitidos al primer módulo de aplicación 30 para la descodificación. Los E-Mails de Internet transmitidos de esta manera representan del mismo modo datos útiles correspondientes. La descodificación de los datos útiles transmitidos entre el teléfono móvil 5 y el proveedor de servicios 1 se realiza de manera correspondiente después de la recepción en el módulo de aplicación 30, 60 correspondiente por medio de un algoritmo de descodificación asociado al algoritmo de codificación de la primera unidad de codificación 15 y de la segunda unidad de codificación 75, cuyo algoritmo de descodificación revierte la codificación de los datos realizada con el algoritmo de codificación y a tal fin utiliza igualmente de una manera correspondiente la segunda clave 12.

La invención se ha descrito a modo de ejemplo con la ayuda del proveedor de servicios 1 seleccionado por el teléfono móvil 5 y del servicio de E-Mail de Internet del proveedor de servicios 1 seleccionado de la misma manera por el teléfono móvil 5. A esta combinación de proveedor de servicios 1 seleccionado y servicio de E-Mail de Internet seleccionado está asociada en este caso a modo de ejemplo la segunda clave 12. De manera correspondiente,

puede estar previsto que el teléfono móvil pueda acceder también a toros servicios del proveedor de servicios 1, como por ejemplo el servicio de transmisión por vídeo o al servicio de Fax, a los que está asociado entonces en cada caso de nuevo una clave correspondiente, por ejemplo la primera clave 11 o la tercera clave 13. Como datos útiles se transmitirían en este caso entre el teléfono móvil 5 y el proveedor de servicios 1 entonces, entre otras cosas, datos de vídeo o datos de fax. Además, también puede estar previsto que el teléfono móvil 5 pueda seleccionar también un proveedor de servicios o varios proveedores de servicios diferentes del proveedor de servicios 1, para utilizar diferentes datos. A cualquier combinación de proveedores de servicios seleccionados y de datos útiles utilizados por el proveedor de servicios seleccionado puede estar asociada entonces una clave de la manera descrita para la autentificación y/o para el intercambio seguro de datos útiles. Pero también puede estar previsto que una o varias de las claves memorizadas en la memoria 20 estén asociadas solamente en cada caso a un proveedor de servicios, sin que esté asociada una clave propia a los servicios individuales ofrecidos por estos proveedores de servicios. De esta manera, se pueden utilizar todos los servicios de tal proveedor de servicios a través de la clave asignada o asociad a este proveedor de servicios, de modo que para el acceso a los diferentes servicios de tal proveedor de servicios no es necesaria en cada caso una utilización propia de usuario y una autentificación con éxito en tal proveedor de servicios permite utilizar todos los servicios ofrecidos por este proveedor de servicios para el teléfono móvil 5. En este caso, también puede estar previsto entonces que los datos útiles a transmitir para los diferentes servicios de este proveedor de servicios entre el teléfono móvil 5 y este proveedor de servicios sean codificados, independientemente del servicio utilizado con la misma clave de datos útiles, pudiendo tratarse en esta clave de datos útiles, por ejemplo, de la misma clave que se ha utilizado para la autentificación.

En la memoria 20 se puede tratar, por ejemplo, de una memoria Flash/EEPROM no volátil, cuyos contenidos no se pueden perder tampoco en el caso de fallo de la tensión.

En una variación del ejemplo de realización descrito con referencia a la figura 1, también se puede prever que la clave necesaria, en el ejemplo la segunda clave 12, sea transmitida desde el primer módulo de aplicación 30 junto con la solicitud de identificación a la primera unidad de codificación 15 para la codificación de la solicitud de identificación a través del control de direcciones 35. La primera unidad de codificación 15 genera entonces de la manera descrita la respuesta codificada y la retorna al módulo de aplicación 30. Sin embargo, si se memorizan las claves, como se representa en la figura 1, en la memoria 20, que está integrada junto con la primera unidad de codificación 15 en el módulo de codificación 40, entonces se pueden asegurar las claves mejor contra acceso no permitido, con la condición de que el módulo de codificación 40 esté asegurado contra acceso no permitido.

El control de direcciones 35 representa una interfaz entre el primer módulo de aplicación 30 y el módulo de codificación 40. En este caso, en una modificación del ejemplo de realización representado en la figura 1, también puede estar previsto opcionalmente que los datos codificados por la primera unidad de codificación 15 sean transmitidos como la solicitud de identificación codificada o los datos útiles codificados a través del control de direcciones 35 hacia el primer módulo de aplicación 30, para ser transmitidos desde allí a través del primer dispositivo de emisión / recepción 25, la red de telefonía móvil 10, la estación de base 45 y la puerta de acceso 50 hacia el proveedor de servicios 1. En la red de telefonía móvil UMTS, la transmisión de los datos entre el teléfono móvil 5 y la estación de base 45 se realiza a través de las llamadas portadoras de UMTS.

Con una capacidad correspondiente de la memoria 20 se puede memorizar allí un número casi ilimitado de claves, con las que se puede utilizar un servicio discrecional de un proveedor opcional de servicios de la manera descrita, sin que el primer proveedor de servicios seleccionado, por ejemplo, para el primer servicio tenga conocimiento de la selección de un segundo proveedor de servicios para un segundo servicio.

En la figura 4 se representa como otro ejemplo de realización una forma de realización alternativa del terminal de telecomunicaciones 5, donde los mismos signos de referencia identifican los mismos elementos que en las figuras 1 a 3. En este caos, en el terminal de telecomunicaciones 5 se introduce una tarjeta de autorización de acceso 100 a través de una caja de entrada no representada en la figura 4. El módulo de codificación 40 y el primer módulo de aplicación 30 no son ya, en el ejemplo de realización según la figura 4, componentes del terminal de telecomunicaciones, sino que están dispuestos sobre la tarjeta de autorización de acceso 100. La tarjeta de autorización de acceso 100 comprende, además, una primera unidad de interfaz 105, que está conectada en el primer módulo de aplicación 30 y está prevista para la conexión con una segunda unidad de interfaz 110 del terminal de telecomunicaciones 5. En la segunda unidad de interfaz 110 está conectado entonces el primer dispositivo de emisión / recepción 25.

La función del terminal de telecomunicaciones 5 representado en la figura 4 con la tarjeta de autorización de acceso corresponde a la función del terminal de telecomunicaciones según la figura 1 con la diferencia de que en el terminal de telecomunicaciones 5 según la figura 4 entre el primer dispositivo de emisión / recepción 25 y el primer módulo de aplicación 30 está dispuesto un circuito de interfaz formado por la primera unidad de interfaz 105 y la segunda unidad de interfaz 110, que asegura un intercambio bidireccional de los datos entre el terminal de telecomunicaciones 5 y la tarjeta de autorización de acceso 100.

En este caso, a continuación se supone a modo de ejemplo que la tarjeta de autorización de acceso 100 está configurada como tarjeta SIM (Módulo de Identidad del Abonado), por ejemplo en forma de una Tarjeta Inteligente y se emplea un protocolo común, a continuación a modo de ejemplo el protocolo SAT (SIM Application Toolkit), para una transmisión bidireccional entre la tarjeta de autorización de acceso 100 y el proveedor de servicios 1. Las tarjetas inteligentes comprenden un chip pequeño con microprocesador integrado y con una interfaz para el intercambio de datos y se utilizan, por ejemplo, por los bancos en los llamados cajeros automáticos. El protocolo SAT se conoce, por ejemplo, a partir de la publicación “Specification of SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM-ME) Interface”, GSM 11.14 versión 8.0.1 Release 1999, ETSI.

En este caso, según la figura 5, también en el proveedor de servicios 1 está previsto un circuito de interfaz en forma de una tercera unidad de interfaz 115, que está conectado entre el segundo módulo de aplicación 60 y la puerta de acceso y en este ejemplo debe estar realizado de la misma manera de acuerdo con el protocolo SAT. Otros módulos del proveedor de servicios 1, como se representan, por ejemplo, en las figuras 2 y 3, no se representan en la figura 5 para mayor claridad.

Un usuario, que quiere recibir un servicio del proveedor de servicios 1, recibe de éste la tarjeta de autorización de acceso 100, en la que el proveedor de servicios 1 memoriza una o varias de las claves secretas 11, 12, 13, 14 en la memoria 20. Ésta o estas claves pueden servir entonces durante el tiempo de vigencia del contrato entre el usuario y el proveedor de servicios 1 como medio seguro para la identificación mutua de las dos partes del contrato.

El terminal de telecomunicaciones 5 debe estar configurado, por ejemplo, como terminar de telefonía móvil UMTS. Si el usuario quiere utilizar un servicio del proveedor de servicios 1, solicita este servicio a través de la red de telecomunicaciones 10 configurada en este ejemplo como red de telefonía móvil UMTS, seleccionando, por ejemplo, el número de llamada del proveedor de servicios 1. A continuación, el proveedor de servicios 1 general, como se ha descrito, la solicitud de identificación y la envía a través de la red de telefonía móvil 10 hacia el terminal de telefonía móvil UMTS 5. Al mismo tiempo el proveedor de servicios 1 general, como se ha descrito, la respuesta de referencia codificada. Todo el ciclo correspóndela descrito ya para las figuras 1 a 3, con la diferencia de que el proveedor de servicios 1 envía la solicitud de identificación a través de la tercera unidad de interfaz 115 por medio del protocolo SAT al terminal de telefonía móvil UMTS 5. En este caso, la solicitud de identificación es empaquetada en la tercera unidad de interfaz 115 con la ayuda del protocolo SAT, siendo enviada simultáneamente con la solicitud de identificación una información de señalización, que está realizada, por ejemplo, como información de cabecera, que indica al primer dispositivo de emisión / recepción 25 del terminal de telefonía móvil UMTS 5, a la recepción, que los datos recibidos deben ser transmitidos con la solicitud de identificación a la segunda unidad de interfaz 110 en el terminal de telefonía móvil UMTS 5. Desde la segunda unidad de interfaz 110 se transmiten los datos con la solicitud de identificación entonces a través de la primera unidad de interfaz 105 al primer módulo de aplicación 30 en la tarjeta de autorización de acceso 100. El primer módulo de aplicación extrae entonces a partir de los datos recibidos desde la primera unidad de interfaz 105 de la manera descrita la solicitud de identificación, dado el caso con la dirección de un espacio de memoria para la clave cordada en la memoria 20. De la manera ya descrita, el módulo de codificación 40 forma entonces la respuesta codificada, que se transmite a través del primer módulo de aplicación 30 a la primera unidad de interfaz 105. Allí se empaqueta la respuesta codificada de nuevo por medio del protocolo SAT y se transmite a la segunda unidad de interfaz 110, desde donde se retorna a través del primer dispositivo de emisión / recepción 25 por medio de una portadora UMTS a través de la red de telefonía móvil UMTS 10 hasta el proveedor de servicios 1.

En la tercera unidad de interfaz 115 se desempaqueta la respuesta codificada recibida de nuevo según el protocolo SAT y se compara de la manera descrita con la respuesta de referencia codificada con objeto de la autentificación.

Si se desea no sólo realizar una autentificación como se ha descrito al comienzo de una transmisión de datos útiles, sino adicionalmente proteger toda la transmisión de datos útiles contra acceso no autorizado, como por ejemplo contra escucha, entonces de acuerdo con la invención se puede realizar también una codificación de los datos útiles de extremo a extremo como se ha descrito entre el proveedor de servicios 1 y la tarjeta de autorización de acceso 10 del terminal de telefonía móvil UMTS 5. Esta codificación de datos útiles de extremo a extremo se puede establecer en este caso igualmente de la manera descrita en el protocolo SAT utilizando la primera unidad de interfaz 105 y la segunda unidad de interfaz 110. De esta manera, también la codificación de datos útiles realizada por la tarjeta de autorización de acceso 100 es totalmente independiente del operador de la red, del fabricante del terminal de telefonía móvil UMTS 5 y de las capacidades de codificación del terminal de telefonía móvil UMTS 5 propiamente dicho.

Como durante la autentificación, el usuario con la adquisición de la tarjeta de autorización de acceso 100 puede acordar también con el proveedor de servicios 1 una clave secreta, que puede corresponder, pero no necesariamente, con la clave para la autentificación. Esta clave puede variar incluso de un servicio a otro, puesto que, e efecto, la memoria 20 proporciona varios espacios de memoria 21, 22, 23, 24 para claves secretas.

Esto significa que para diferentes servicios, de los cuales la identificación descrita es solamente uno de ellos, se pueden convenir diferentes claves secretas entre el usuario y el proveedor de servicios 1.

La ventaja de la utilización del protocolo SAT consiste en que este protocolo está normalizado y está implementado ya en muchos terminales de telefonía móvil configurados especialmente según la Norma GSM y, por lo tanto, está disponible. El protocolo SAT ofrece la posibilidad de recurrir a una interfaz independiente del fabricante entre el terminal de telefonía móvil respectivo y la tarjeta de autorización de acceso 100, con lo que se posibilita al proveedor de servicios 1 la realización de nuevas aplicaciones, para fomentar de esta manera la diferenciación de proveedores de servicios frente al operador de la red y/o frente a otros proveedores de servicios.

REIVINDICACIONES

1.- Procedimiento para la codificación de datos, en el que los datos codificados son transmitidos entre un proveedor de servicios (1) y un terminal de telecomunicaciones (5) a través de una red de telecomunicaciones (10), en el que los datos a transmitir a través de la red de telecomunicaciones (10) son codificados en función del proveedor de servicios (1) seleccionado, caracterizado porque antes de una transmisión de datos útil entre el terminal de telecomunicaciones (5) y el proveedor de servicios (1) se utiliza una solicitud de identificación desde el proveedor de servicios (1) hacia el terminal de telecomunicaciones (5), porque a partir de una cantidad de claves (11, 12, 13, 14) memorizadas en el terminal de telecomunicaciones (5) o en una tarjeta de autorización de acceso (100) introducida en el terminal de telecomunicaciones (5), se selecciona aquélla que está asociada al proveedor de servicios (1) seleccionado, porque la solicitud de identificación es codificada con la clave (11, 12, 13, 14) seleccionada, de manera que resulta una respuesta codificada y porque la respuesta es transmitida desde el terminal de telecomunicaciones (5) hacia el proveedor de servicios (1) para una identificación del terminal de telecomunicaciones (5).

2.- Procedimiento de acuerdo con la reivindicación 1, caracterizado porque para la transmisión de los datos se utiliza un servicio del proveedor de servicios (1) seleccionado y porque los datos a transmitir a través de la red de telecomunicaciones (10) son codificados en función del servicio seleccionado.

3.- Procedimiento de acuerdo con la reivindicación 2, caracterizado porque a partir de la cantidad de claves (11, 12, 13, 14) memorizadas en el terminal de telecomunicaciones (5) o en la tarjeta de autorización de acceso (100) introducida en el terminal de telecomunicaciones (5) se selecciona aquélla que está asociada al proveedor de servicios (1) seleccionado o adicionalmente al servicio seleccionado.

4.- Procedimiento de acuerdo con una de las reivindicaciones anteriores, caracterizado porque al proveedor de servicios (1) está asociada una clave de datos útiles (11, 12, 13, 14), con la que se codifican los datos útiles a transmitir.

5.- Procedimiento de acuerdo con la reivindicación 4, caracterizado porque al proveedor de servicios (1) seleccionado y adicionalmente al servicio seleccionado está asociada la clave de datos útiles (11, 12, 13, 14), con la que se codifican los datos útiles a transmitir.

6.- Procedimiento de acuerdo con una de las reivindicaciones anteriores, caracterizado porque con la clave (11, 12, 13, 14) seleccionada para la identificación del terminal de telecomunicaciones (5) se codifican también los datos útiles a transmitir.

7.- Terminal de telecomunicaciones (5) para la realización de un procedimiento de acuerdo con una de las reivindicaciones anteriores con una unidad de codificación (15) asociada al terminal de telecomunicaciones (5), caracterizado porque está prevista una memoria (20) asociada al terminal de telecomunicaciones (5), en la que están memorizadas varias claves (11, 12, 13, 14) asociadas, respectivamente, a un proveedor de servicios (1), con las que se codifican datos a transmitir hacia el proveedor de servicios (1) respectivo a través de una red de telecomunicaciones (10) en la unidad de codificación (15), porque la unidad de codificación (15) codifica una solicitud de identificación recibida desde un proveedor de servicios (1) seleccionado con una clave (11, 12, 13, 14) depositada en la memoria (20), de manera que resulta una respuesta codificada, en el que la clave (11, 12, 13, 14) seleccionada a partir de la memoria (20) para la codificación está asociada al proveedor de servicios (1) seleccionado, y porque está previsto un dispositivo de emisión (25), que emite la respuesta codificada al proveedor de servicios (1) para una autentificación del terminal de telecomunicaciones (5).

8.- Terminal de telecomunicaciones (5) de acuerdo con la reivindicación 7, caracterizado porque la al menos una clave (11, 12, 13, 14) memorizada en la memoria (20) está asociada adicionalmente a un servicio, con el que se transmiten los datos entre el terminal de telecomunicaciones (5) y el proveedor de servicios (1).

9.- Terminal de telecomunicaciones (5) de acuerdo con la reivindicación 7 u 8, caracterizado porque la unidad de codificación (15) codifica la solicitud de identificación con una clave (11, 12, 13, 14) desde la memoria (20), en el que a partir de la cantidad de las claves (11, 12, 13, 14) memorizadas en el terminal de telecomunicaciones (5) se selecciona aquélla que está asociada al proveedor de servicios (1) seleccionado y adicionalmente a un servicio seleccionado para la transmisión de datos.

10.- Terminal de telecomunicaciones (5) de acuerdo con una de las reivindicaciones 7 a 9, caracterizado porque al proveedor de servicios (1) seleccionado está asociada una clave de datos útiles (11, 12, 13, 14) depositada en la memoria (20), con la que la unidad de codificación (15) codifica los datos útiles a transmitir.

11.- Terminal de telecomunicaciones (5) de acuerdo con la reivindicación 10, caracterizado porque al proveedor de servicios (1) y adicionalmente al servicio seleccionado está asociada la clave de datos útiles (11, 12, 13, 14), con la que la unidad de codificación (15) codifica los datos útiles a transmitir.

12.- Terminal de telecomunicaciones (5) de acuerdo con una de las reivindicaciones 7 a 11, caracterizado porque la unidad de codificación (15) codifica con la clave (11, 12, 13, 14) seleccionada para la codificación del terminal de telecomunicaciones (5) también los datos útiles a transmitir.

13.- Terminal de telecomunicaciones (5) de acuerdo con una de las reivindicaciones 7 a 12, caracterizado porque la unidad de codificación (15) y la memoria (20) están dispuestas en el terminal de telecomunicaciones (5).

14.- Terminal de telecomunicaciones (5) de acuerdo con una de las reivindicaciones 7 a 12, caracterizado porque el terminal de telecomunicaciones (5) comprende una caja de entrada para la introducción de una tarjeta de autorización de acceso (100), en el que la tarjeta de autorización de acceso (100) comprende la unidad de codificación (15) y la memoria (20), y porque el terminal de telecomunicaciones (5) comprende una unidad de interfaz (110) para la sustitución de datos codificados con la tarjeta de autorización de acceso (100).

15.- Tarjeta de autorización de acceso (100) para la realización de un procedimiento de acuerdo con una de las reivindicaciones 1 a 6 con una unidad de codificación (15), caracterizada porque está prevista una memoria (20), en la que están memorizadas varias claves (11, 12, 13, 14) asociadas, respectivamente, a un proveedor de servicios (1), con las que se codifican datos a transmitir hacia el proveedor de servicios (1) respectivo a través de una red de telecomunicaciones (10) en la unidad de codificación (15), porque está prevista una unidad de interfaz (105) para el intercambio de datos codificados con un terminal de telecomunicaciones (5), porque la unidad de codificación (15) codifica una solicitud de identificación recibida por un proveedor de servicios (1) seleccionado con una clave (11, 12, 13, 14) depositada en la memoria (20), de manera que resulta una respuesta codificada, en la que la clave (11, 12, 13, 14) seleccionada a partir de la memoria (20) para la codificación está asociada al proveedor de servicios (1) seleccionado, y porque se realiza una emisión de la respuesta codificada al proveedor de servicios (1) para una autentificación del terminal de telecomunicaciones (5) a través del dispositivo de emisión (25) del terminal de telecomunicaciones (5).

16.- Tarjeta de autorización de acceso (100) de acuerdo con la reivindicación 15, caracterizada porque la al menos una clave (11, 12, 13, 14) memorizada en la memoria (20) está asociada adicionalmente a un servicio, con el que se transmiten los datos entre el terminal de telecomunicaciones (5) y el proveedor de servicios (1).

17.- Tarjeta de autorización de acceso (100) de acuerdo con la reivindicación 15 ó 16, caracterizada porque la unidad de codificación (15) codifica la solicitud de identificación con una clave (11, 12, 13, 14) desde la memoria (20), en la que a partir de la cantidad de claves (11, 12, 13, 14) memorizadas en la memoria (20) se selecciona aquélla que está asociada al proveedor de servicios (1) seleccionado y adicionalmente a un servicio seleccionado para la transmisión de datos.

18.- Tarjeta de autorización de acceso (100) de acuerdo con una de las reivindicaciones 15 a 17, caracterizada porque al proveedor de servicios (1) seleccionado está asociada una clave de datos útiles (11, 12, 13, 14) depositada en la memoria (20), con la que la unidad de codificación (15) codifica los datos útiles a transmitir.

19.- Tarjeta de autorización de acceso (100) de acuerdo con la reivindicación 18, caracterizada porque al proveedor de servicios (1) seleccionado y adicionalmente al servicio seleccionad está asociada la clave de datos útiles (11, 12, 13,14), con la que la unidad de codificación (15) codifica los datos útiles a transmitir.

20.- Tarjeta de autorización de acceso (100) de acuerdo con una de las reivindicaciones 15 a 19, caracterizada porque la unidad de codificación (15) codifica con la clave (11, 12, 13, 14) seleccionada para la autentificación del terminal de telecomunicaciones (5) también los datos útiles a transmitir.

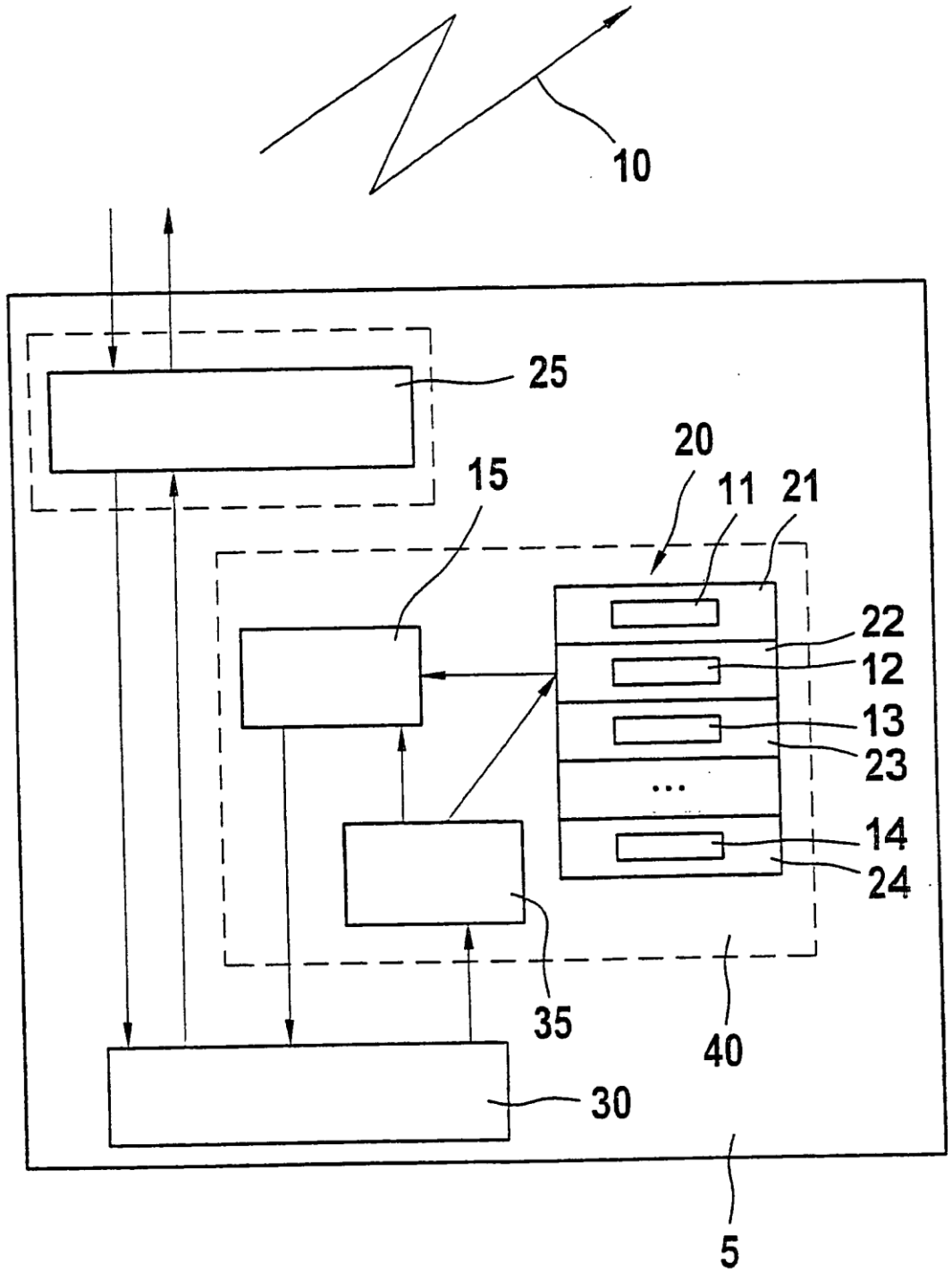

FIG. 1

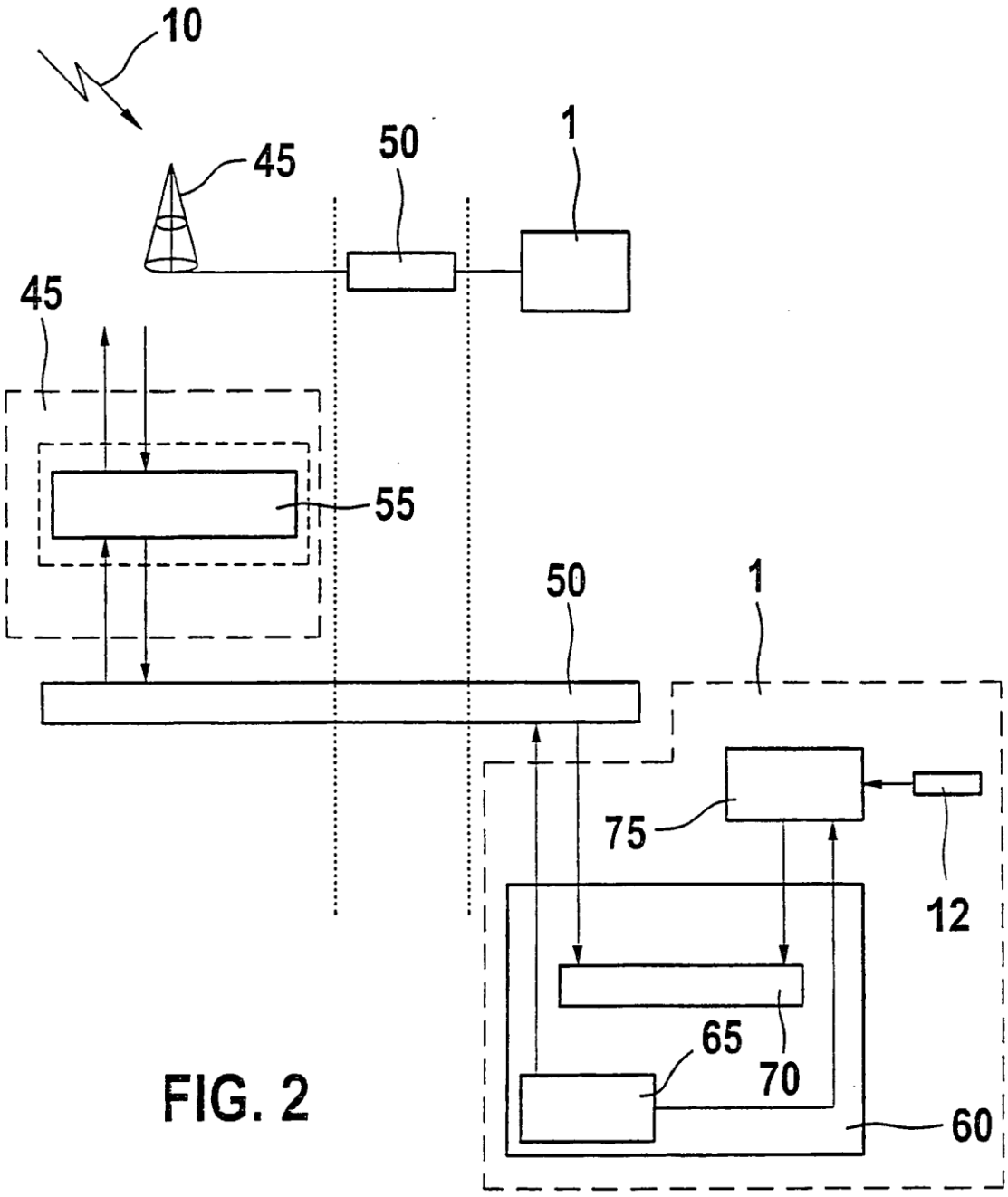

FIG. 2

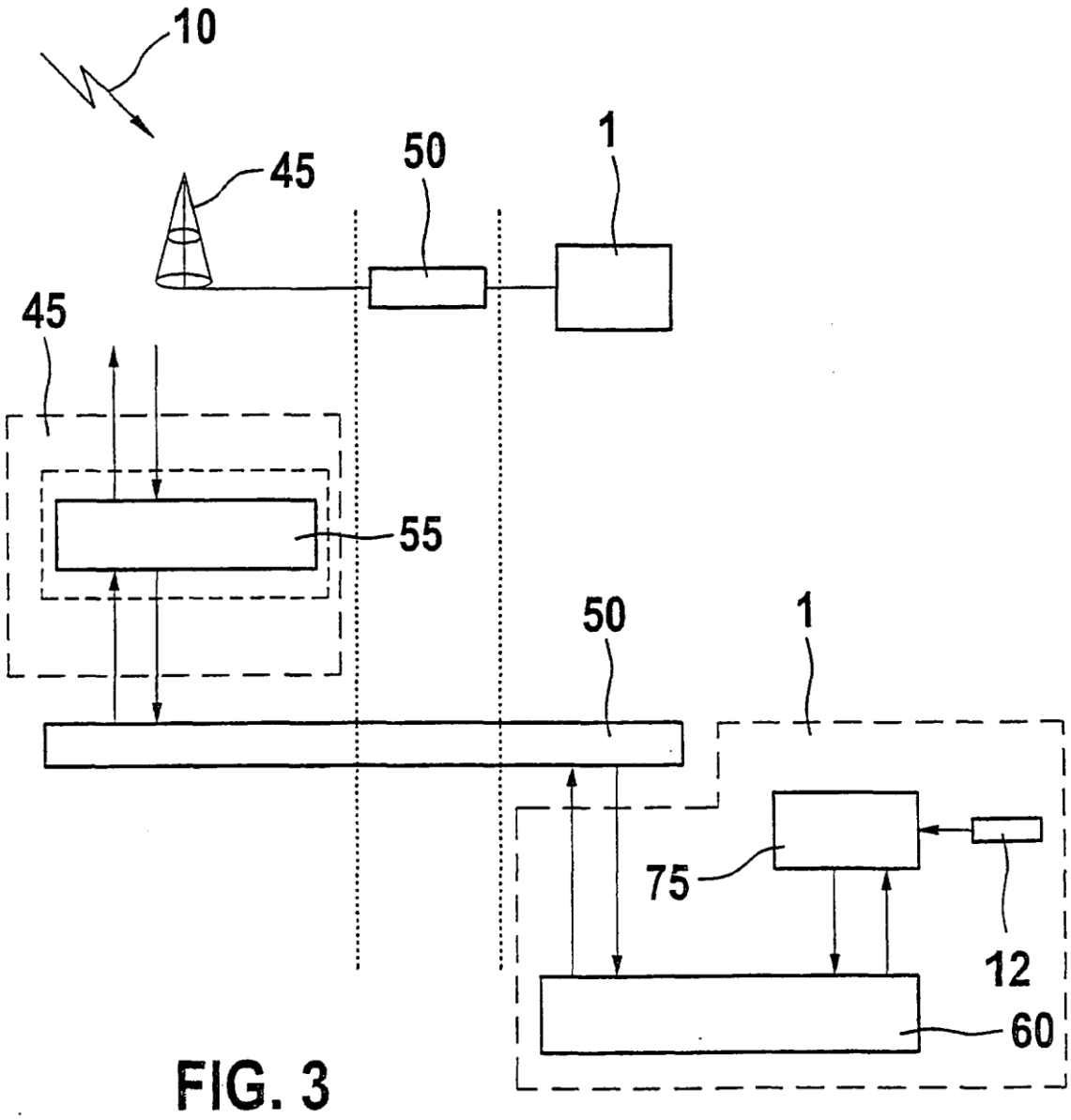

FIG. 3

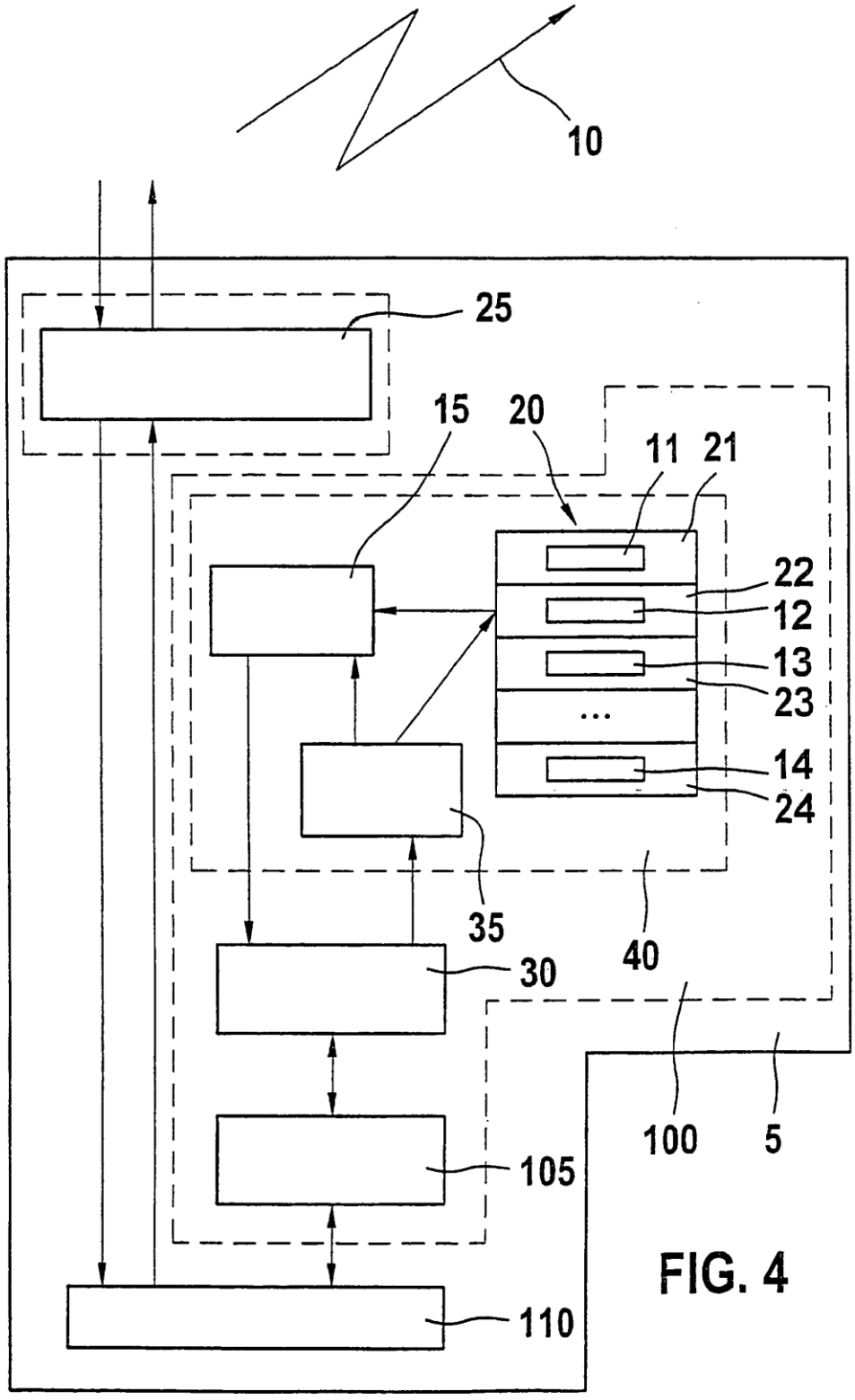

FIG. 4

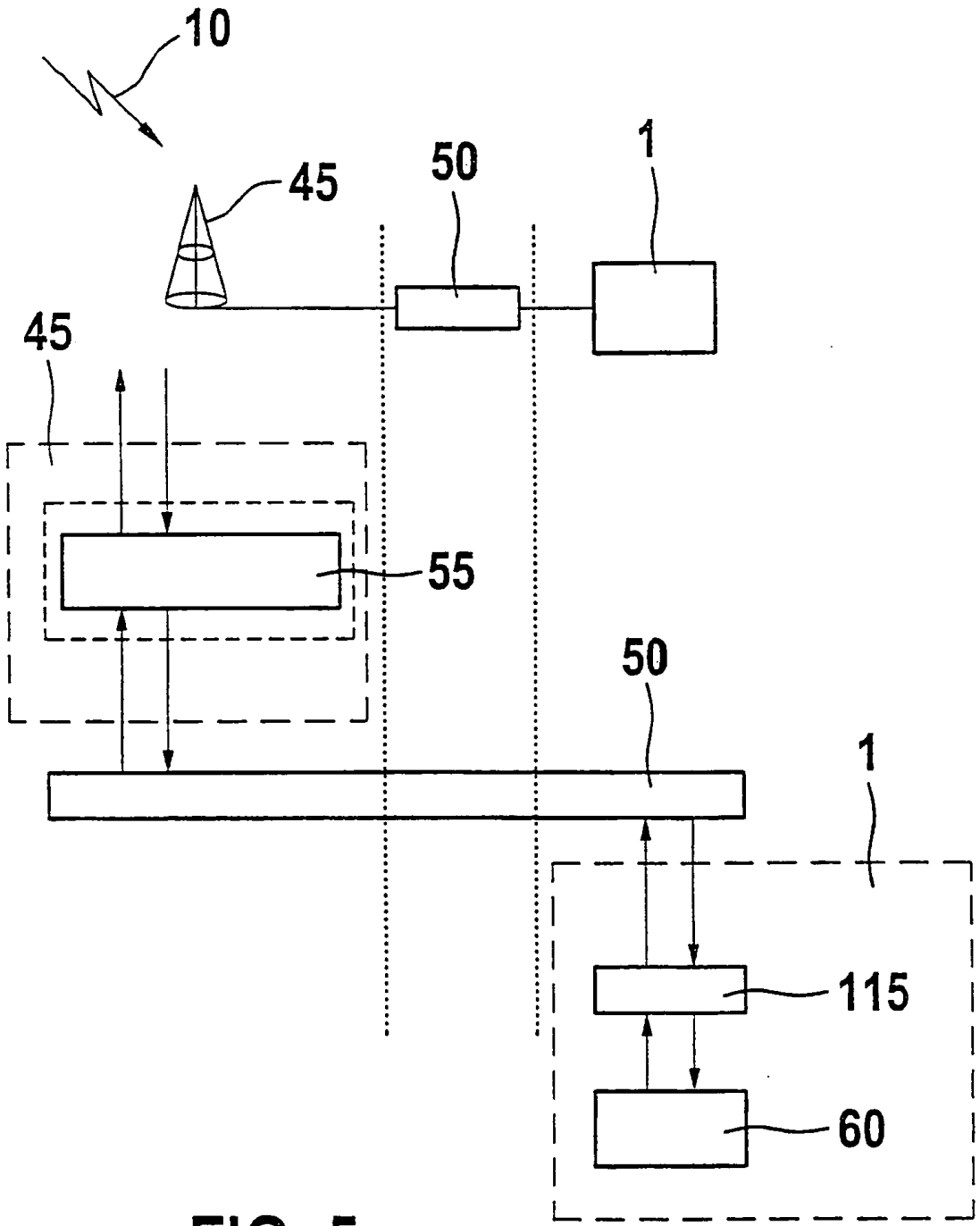

FIG. 5