(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 286 333**

(51) Int. Cl.:
H04Q 7/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **02804213 .3**
(86) Fecha de presentación : **02.12.2002**
(87) Número de publicación de la solicitud: **1454503**
(87) Fecha de publicación de la solicitud: **08.09.2004**

(54) Título: **Almacenamiento y acceso a datos en un dispositivo móvil y un módulo de usuario.**

(30) Prioridad: **04.12.2001 DE 101 59 398**

(45) Fecha de publicación de la mención BOPI:
01.12.2007

(45) Fecha de la publicación del folleto de la patente:
01.12.2007

(73) Titular/es: **Giesecke & Devrient GmbH**
Prinzregentenstrasse 159
81677 München, DE

(72) Inventor/es: **Kirsch, Jochen;**
Klaassen, Ralf y
Eckardt, Stefan

(74) Agente: **Torner Lasalle, Elisabet**

DESCRIPCIÓN

Almacenamiento y acceso a datos en un dispositivo móvil y un módulo de usuario.

La invención se refiere en general al campo técnico de almacenar y acceder a datos en dispositivos móviles, así como en módulos de usuario para dispositivos de este tipo. Los dispositivos móviles pueden dotar al usuario tanto de funciones de telecomunicaciones (por ejemplo, la transferencia de voz y/o datos a través de una red de telecomunicaciones) como de programas de aplicación (por ejemplo, una agenda o un editor de texto) son un área de aplicación preferida de la invención. Los dispositivos móviles de este tipo pueden, en particular, configurarse como teléfonos móviles potentes o como PDA (asistente digital personal).

La solicitud alemana abierta a consulta por el público DE 197 24 901 A1 da a conocer un teléfono móvil según la norma GSM (GSM= sistema global para comunicación móvil, *Global System for Mobile Communication*). El teléfono móvil comprende una unidad de control, una memoria de dispositivo y una interfaz para un módulo de identidad de abonado (SIM, *Subscriber Identity Module*). Los datos de usuario, tales como listas de direcciones, datos de volúmenes de ventas o listas de precios, por ejemplo, pueden cargarse en la memoria de dispositivo a través de una conexión de línea con un ordenador. También es posible cargar programas (no descritos en mayor detalle) en la memoria de dispositivo a través de la conexión de línea, y ejecutarlos posteriormente a través del teléfono móvil. Los datos pueden transferirse en una forma en la que se garantiza la integridad o cifrada.

Cuando se enciende un teléfono móvil GSM, generalmente hay una comprobación de autorización, en la que el usuario tiene que introducir un número secreto personal (PIN= número de identificación personal, *Personal Identification Number*). Sólo se habilita la interfaz de usuario completa, incluyendo la opción de acceder a los datos de usuario almacenados en el teléfono móvil, si se introduce correctamente el número secreto. Por lo tanto, los datos de usuario confidenciales están normalmente protegidos hasta cierto punto. Sin embargo, existe el problema de que los delincuentes suficientemente expertos puedan eludir esta seguridad. Los dispositivos de memoria del teléfono móvil pueden, por ejemplo, leerse directamente a nivel de hardware utilizando aparatos apropiados.

En particular, es beneficioso almacenar datos de usuario en el dispositivo móvil si el teléfono móvil también está configurado para ejecutar programas de aplicación para procesar estos datos de usuario. En la actualidad, las PDA y los teléfonos móviles GSM potentes tienen esta funcionalidad. Debido a las altas velocidades de transferencia de dispositivos móviles de la segunda generación y media y de la tercera generación, tal como, por ejemplo, dispositivos para las redes GPRS (servicio general de radio por paquetes, *General Packet Radio Service*), EDGE, UMTS (sistema universal de telecomunicaciones móviles, *Universal Mobile Telecommunications System*) y WCDMA (acceso múltiple por división de código de banda ancha, *Wideband Code-Division Multiple Access*), pueden cargarse y/o actualizarse programas de aplicación desde un proveedor de servicios en el dispositivo móvil a través de la interfaz aérea.

Dichos dispositivos móviles tienen problemas y requieren mejora en algunos aspectos. En primer lugar, debería ser posible impedir el acceso no autorizado a programas de aplicación también en tales dispositivos. Debería por tanto garantizarse que sólo el usuario autorizado pueda llamar a un programa de aplicación, o funciones protegidas individuales del programa de aplicación. En segundo lugar, sería deseable poder ofrecer al usuario una selección de funciones que se adaptasen tan rigurosamente como fuera posible a estos requisitos. En tercer lugar, las funciones proporcionadas deberían ser tan independientes del dispositivo como fuera posible.

Se conoce un dispositivo móvil a partir del documento EP-A 1 107 627, en el que el dispositivo móvil comprende una memoria de dispositivo y está conectado con un módulo de usuario a través de una interfaz. Los datos de usuario en la memoria de dispositivo del dispositivo móvil se almacenan al menos en parte en forma cifrada, en la que el módulo de usuario, es decir, la tarjeta SIM, contiene la clave de acceso para descifrar los datos de usuario y habilita la clave de acceso después de la introducción del PIN.

Además, se conoce un sistema para el cifrado y descifrado de datos a partir del documento US-A 5 802 175, en el que las claves para el cifrado y descifrado se almacenan en un módulo portátil que se conecta con un ordenador.

El problema de las soluciones conocidas es que el proceso de cifrado y el proceso de descifrado, respectivamente, se realizan dentro del terminal, y pueden espiarse los datos intercambiados entre el terminal y el módulo y por lo tanto existe un riesgo en la seguridad.

El objetivo de la invención es solucionar dichos problemas, completamente o en parte. En particular, mediante la invención debería aumentarse la seguridad y protección contra el acceso no autorizado a datos de usuario en un dispositivo móvil. En configuraciones preferidas, la invención también debería proporcionar un alto grado de comodidad para el usuario y debería poder implementarse de manera económica.

Según la invención, se consigue este objetivo, completamente o en parte, mediante un método que tiene las características de la reivindicación 1, un dispositivo móvil que tiene las características de la reivindicación 8, y un módulo de usuario que tiene las características de la reivindicación 9. Las reivindicaciones dependientes se refieren a configuraciones preferidas de la invención.

La invención parte de la idea básica de cumplir los requisitos de seguridad mencionados anteriormente almacenando los datos de usuario de una manera adecuada. Los datos de usuario se almacenan, según la invención, en forma cifrada en la memoria de dispositivo del dispositivo móvil. Se utilizan funciones correspondientes, que se proporcionan por el módulo de usuario, al menos para descifrar (y, en configuraciones preferidas, también para cifrar) los datos de usuario.

Debido a que los datos de usuario en la memoria del dispositivo móvil están sólo en forma cifrada, dichos datos están protegidos de ojos curiosos incluso si un usuario no autorizado elude la interfaz de usuario normal del dispositivo móvil para acceder al contenido de la memoria de dispositivo. La memoria de dispositivo, que es en general bastante grande, puede utilizarse para almacenar los datos de usuario sin preocuparse de la seguridad, por lo que el dispositivo móvil puede transportar cantidades relativamente grandes de datos y estructuras de datos complejas.

Los datos de usuario que van a almacenarse según la invención pueden ser cualquier dato que el usuario desee. Preferiblemente, son datos que pueden también procesarse mediante un programa de aplicación que se ejecuta en el dispositivo móvil, tales como, por ejemplo, listas de direcciones y citas para procesarse mediante una agenda que tiene una función de libreta de direcciones, tablas comerciales para procesarse, por ejemplo, mediante programas de hojas de cálculo, datos de voz generados, por ejemplo, mediante programas de grabación de dictado, o textos generales para procesarse mediante editores de texto. También puede ser deseable almacenar datos de usuario para los que no hay un programa de aplicación apropiado disponible en el dispositivo móvil. En este caso, el dispositivo móvil actúa como un portador de datos seguro para intercambiar datos de usuario entre el lugar de trabajo y un equipo personal por ejemplo.

En configuraciones preferidas, las funciones de cifrado y descifrado se ejecutan, completamente o en parte, mediante una unidad de procesador del módulo de usuario, en las que la unidad de procesador accede a datos de claves que están contenidos en una memoria de módulo. Los datos de claves no necesitan abandonar el módulo de usuario en estas configuraciones, permitiendo que se obtenga un grado de seguridad particularmente alto. En particular, este es el caso si los datos de claves se generan también en el módulo de usuario y se escriben en la memoria de módulo. Sin embargo, también existen configuraciones de la invención en las que al menos el cifrado, y también opcionalmente el descifrado, de los datos de usuario se ejecuta/ejecutan, completamente o en parte, por una unidad de procesador del dispositivo móvil, a la que se transfieren las funciones de cifrado y/o descifrado proporcionadas por el módulo de usuario.

Preferiblemente, se utiliza un método de cifrado asimétrico, tal como, por ejemplo, el método RSA (Rivest-Shamir-Adleman). En este caso, los datos de claves comprenden una clave pública y una clave privada. Sin embargo, también existen configuraciones en las que se utilizan métodos de cifrado simétrico. En términos conceptuales, se hace referencia a "funciones de cifrado y descifrado" también en estas configuraciones, aunque en ambos casos se ejecutan las mismas etapas de cálculo.

Según la invención, el módulo de usuario se requiere al menos para ejecutar las etapas de descifrado. Esto proporciona en sí un cierto grado de protección, puesto que el módulo de usuario y el dispositivo móvil pueden permanecer separados. Sin embargo, en realizaciones preferidas, se prevé que no se habilite al menos la función de descifrado hasta que se haya introducido una contraseña (frase de contraseña) y/o se haya llevado a cabo una prueba biométrica, tal como, por ejemplo, verificación de una huella dactilar o análisis de voz. A través de esta medida, se garantiza la seguridad de datos incluso si tanto el dispositivo móvil como el módulo de usuario se han extraviado.

En configuraciones preferidas, el dispositivo móvil es un dispositivo de telecomunicaciones, en particular un teléfono móvil o un asistente digital personal (PDA) que tiene funciones de telefonía. El módulo de usuario es preferiblemente un módulo de identidad de abonado (SIM), como se requiere para entrar en una red de telecomunicaciones. En particular, puede preverse que un módulo de usuario esté protegido de la manipulación como un denominado dispositivo fiable o dispositivo de seguridad, de manera que las funciones de cifrado y descifrado, o los datos de claves, o datos de configuración confidenciales estén protegidos de ojos curiosos. Puede utilizarse un módulo de identidad de abonado incluso si el dispositivo móvil no tiene ninguna función de telefonía o si el módulo no está registrado con un proveedor de telefonía, ya que los módulos de este tipo se producen en grandes cantidades y por lo tanto pueden obtenerse de forma relativamente barata.

El dispositivo móvil y el módulo de usuario se desarrollan preferiblemente además con características que corresponden a las características anteriormente mencionadas y/o las características citadas en las reivindicaciones del método dependientes.

Surgirán características, ventajas y objetivos adicionales de la invención a partir de la siguiente descripción detallada de una realización de la invención y de una pluralidad de configuraciones alternativas. Se hace referencia al dibujo, en el que la figura 1 muestra un diagrama de bloques de unidades funcionales esenciales de un sistema según la realización de la invención que se describe en el presente documento.

La figura 1 muestra un dispositivo 10 móvil y un módulo 12 de usuario, que están conectados entre sí a través de una interfaz 14. En la presente realización, el dispositivo 10 móvil está configurado como un teléfono móvil potente, que proporciona funciones de telecomunicación según la norma GSM para servicios de telefonía y según la norma GPRS para servicios de transferencia de datos. El módulo 12 de usuario está configurado en consecuencia como una

tarjeta SIM, que se inserta en el teléfono móvil o está dispuesta de manera fija en el teléfono móvil. El dispositivo 10 móvil puede acceder a una red 18 de telecomunicaciones correspondiente a través de una interfaz 16 aérea. En configuraciones alternativas, el dispositivo 10 móvil está configurado según una norma de telefonía móvil mejorada, tal como UMTS, y/o como un asistente digital personal (PDA), que también puede soportar servicios multimedia.

En una manera conocida *per se*, el dispositivo 10 móvil comprende un componente 20 de alta frecuencia, que envía y recibe ondas de radio a través de una antena 22. Se utiliza un procesador 24 de señales digitales (DSP, *Digital Signal Processor*) para procesar la señal transmitida o recibida. El procesador 24 de señales digitales también procesa señales de baja frecuencia, que se dirigen a un altavoz 28 a través de un componente 26 de baja frecuencia, o se envían desde un micrófono 30, a través del componente 26 de baja frecuencia, al procesador 24 de señales digitales. Una unidad 32 de procesador coordina todas las operaciones que tienen lugar en el dispositivo 10 móvil. La unidad 32 de procesador está conectada a la interfaz 14, al procesador 24 de señales digitales, a un visualizador 34, configurado en este caso como un visualizador LCD que puede mostrar gráficos, a un teclado 36 y a una memoria 38 de dispositivo. La memoria 38 de dispositivo puede configurarse de manera que esté instalada de forma fija o que pueda extraerse, en forma de una tarjeta de memoria, por ejemplo.

La memoria 38 de dispositivo se implementa por medio de una pluralidad de chips semiconductores en diversas tecnologías de memoria. En la representación conceptual de la figura 1, la memoria 38 de dispositivo comprende una región 40 de sólo lectura (implementada, por ejemplo, como una ROM programada mediante máscaras) y una región 42 de escritura, implementada, por ejemplo, como una memoria RAM o EEPROM o FLASH. La región 40 de sólo lectura de la memoria 38 del dispositivo contiene, en particular, programas 44 de funcionamiento, que se ejecutan por la unidad 32 de procesador como el sistema operativo básico del dispositivo 10 móvil, así como para implementar funciones de telecomunicación. Los programas 46 de aplicación y los datos 48 de usuario se cargan en la región 42 de escritura.

La figura 1 muestra, como un ejemplo de los programas 46 de aplicación, una agenda 46.1 (que tiene una función de libreta de direcciones) y un editor 46.2 de texto. En la figura 1 se muestran como datos 48 de usuario una lista 48.1 de direcciones y citas para la agenda 46.1 y una carta 48.2 para el editor 46.2 de texto. Los programas 46 de aplicación se ejecutan por la unidad 32 de procesador y acceden a los datos 48 de usuario. Los datos 48 de usuario se almacenan en forma cifrada en la memoria 38 de dispositivo, tal como se indica mediante rayado en la figura 1.

El módulo 12 de usuario está configurado como un SIM (módulo de identidad de abonado) para la red 18 de telecomunicaciones, y la interfaz 14 también se corresponde mecánica y eléctricamente con las normas previstas para esta red 18 de telecomunicaciones. El módulo 12 de usuario comprende una unidad 50 de procesador, que está configurada como un microcontrolador y está integrada con una memoria 52 de módulo sobre un único chip. La memoria 52 de módulo está subdividida, mediante diversas tecnologías de memoria, en una región 54 de sólo lectura y una región 56 de escritura.

La memoria 52 del módulo contiene datos y programas de control, que, en primer lugar, proporcionan funciones de sistema operativo básico para el módulo 12 de usuario y, en segundo lugar, permiten la entrada y el funcionamiento de telecomunicaciones del dispositivo 10 móvil con respecto a la red 18 de telecomunicaciones. Por claridad, estos datos y programas de control no se muestran por separado en la figura 1. Las funciones 58 criptográficas en la región 54 de sólo lectura de la memoria 52 de módulo, y datos 60 de claves y datos 62 de configuración en la región 56 de escritura, son particularmente importantes para los aspectos según la invención de la realización descrita en el presente documento, y por lo tanto se muestran en la figura 1.

Las funciones 58 criptográficas incluyen una función 64 de cifrado, una función 66 de descifrado y una función 68 de generación de claves. Los datos 60 de claves se dividen en una clave 70 pública y una clave 72 privada. Los datos 62 de configuración comprenden un registro de datos de configuración correspondientes para cada programa 46 de aplicación proporcionado en el dispositivo 10 móvil, es decir, en la realización descrita en el presente documento, un registro 62.1 de datos de configuración para la agenda 46.1 y un registro 62.2 de datos de configuración para el editor 46.2 de texto.

En funcionamiento, el sistema mostrado en la figura 1 proporciona las funciones de telecomunicación convencionales correspondientes a las normas respectivas, en el presente caso de GSM y GPRS. Además, el usuario puede iniciar los programas 46 de aplicación, y procesar los datos 48 de usuario u otros datos con los mismos.

Con el fin de proporcionar los programas 46 de aplicación, el dispositivo 10 móvil accede a los datos 62 de configuración en el módulo 12 de usuario cuando se enciende el dispositivo 10 móvil o, a más tardar, cuando el usuario desea iniciar un programa 46 de aplicación. Este acceso tiene lugar a través de la unidad 50 de procesador del módulo 12 de usuario, que, a su vez, requiere que se introduzca una contraseña antes de permitir el acceso. La solicitud de contraseña se visualiza en el visualizador 34 del dispositivo 10 móvil, y el usuario introduce la contraseña correspondiente a través del teclado 36. La unidad 50 de procesador comprueba que la contraseña introducida es la correcta.

Si el usuario ha introducido la contraseña correcta, el módulo 12 de usuario transfiere los datos 62 de configuración solicitados (o bien todos los datos 62 de configuración o bien sólo el registro 62.1, 62.2 de datos previsto para el respectivo programa 46.1, 46.2 de aplicación) al dispositivo 10 móvil. La unidad 32 de procesador comprueba en-

tonces si, según los datos 62, 62.1, 62.2 de configuración transferidos se puede permitir ejecutar programas 46 de aplicación o el programa 46.1, 46.2 de aplicación específicamente solicitado. Si es así, se permite la ejecución del programa.

Si el programa 46.1, 46.2 de aplicación deseado ya está situado en la memoria 38 de dispositivo, puede iniciarse el programa inmediatamente. De lo contrario, el programa o datos de usuario requeridos, por los que puede cobrarse una tarifa, se cargan en la memoria 38 de dispositivo a través de la interfaz 16 aérea y la red 18 de telecomunicaciones desde un servidor de un proveedor ASP. Este proceso de descarga también tiene que autorizarse por el módulo 12 de usuario, que actúa como un denominado portero (*gatekeeper*). No obstante, incluso si el programa 46.1, 46.2 de aplicación deseado ya está contenido en la memoria 38 del dispositivo, puede llevarse una solicitud con el proveedor de servicios ASP, a través de la interfaz 16 aérea, en primer lugar para transferir datos de facturación y en segundo lugar para importar cualquier actualización de programa, que puede estar disponible, en el dispositivo 10 móvil.

En la realización descrita en el presente documento, los datos 62 de configuración se ocupan no sólo de las autorizaciones de usuario básicas, si no también de los ajustes preferidos de los programas 46 de aplicación, tales como, por ejemplo, trayectorias de archivos preestablecidas, ajustes de lenguaje, configuraciones de menú y otras preferencias de usuario. Estos ajustes se hacen accesibles para el programa 46 de aplicación iniciado, de manera que el usuario siempre trabaja con la configuración de programa que desee. Esto es cierto incluso si el usuario conecta su módulo 12 de usuario a un dispositivo 10 móvil nuevo o diferente.

Si las interfaces de programación de aplicaciones (API, *Application Programming Interface*) pasan a estar suficientemente normalizadas, tal como se espera a medio plazo utilizando el lenguaje de programación Java®, por ejemplo, los proveedores ASP podrán ofrecer servicios de programas de aplicación que se adapten individualmente a cada usuario y que sean independientes del dispositivo 10 móvil utilizado. También se obtendrá un alto nivel de seguridad, puesto que todos los programas 46 de aplicación sólo pueden llamarse si el módulo 12 de usuario está presente y si se ha introducido la contraseña. Con el fin de impedir la mala utilización del dispositivo 10 móvil, en el caso de que sea robado cuando está encendido (después de que el usuario haya introducido la contraseña), puede preverse que, después de que el usuario haya estado inactivo durante un periodo de tiempo predeterminado, se solicite que se vuelva a introducir la contraseña, tal como ya se conoce *per se* con protectores de pantalla para ordenadores de oficina estacionarios, por ejemplo.

En la realización descrita hasta ahora, un programa 46 de aplicación se consideraba como la unidad más pequeña para el mecanismo de autorización y opcionalmente el proceso de carga a través de la interfaz 16 aérea. Sin embargo, dependiendo de la tecnología de programación empleada, también puede utilizarse un nivel más fino de granularidad. Los datos 62 de configuración pueden referirse por tanto a la autorización del usuario para ejecutar funciones de programas individuales o módulos de programas individuales, por ejemplo, y estas funciones de programas o módulos de programas pueden, si se requiere, cargarse individualmente a través de la interfaz 16 aérea. Este enfoque permite, en primer lugar, evitar largos tiempos de carga y, en segundo lugar, una adaptación incluso más precisa a las preferencias del usuario. También, al actualizar programas 46 de aplicación a través de la interfaz 16 aérea, sólo se transfieren preferiblemente los módulos de programas que han cambiado realmente en relación con la versión que ya está en el dispositivo 10 móvil.

Los datos 48 de usuario procesados mediante los programas 46 de aplicación se almacenan en la memoria 38 de dispositivo, o bien completamente o bien al menos parcialmente en forma cifrada. Puede dotarse al usuario, por ejemplo, de un sistema de archivos para almacenar datos 48 de usuario, en el que se establecen selectivamente las carpetas individuales o unidades individuales para el almacenamiento de datos cifrados o no cifrados. Ya se conoce una funcionalidad similar para ordenadores de oficina estacionarios, que no emplean un módulo de usuario, a partir del producto PGPdisk®, del fabricante Network Associates, Inc.

Si un programa 46 de aplicación fuese a almacenar datos 48 de usuario en una región del sistema de archivos previstos para el cifrado, estos datos se transfieren desde la unidad 32 de procesador a través de la interfaz 14 al módulo 12 de usuario. La unidad 50 de procesador del módulo 12 de usuario ejecuta la función 64 de cifrado, en la que se utiliza la clave 70 pública contenida en los datos 60 de claves. Los datos 48 de usuario cifrados se escriben en la memoria 38 del dispositivo a través de la interfaz 14 y la unidad 32 de procesador.

Se accede a los datos 48 de usuario que se han almacenado en forma cifrada de una manera correspondiente. En este caso también, la unidad 50 de procesador del módulo 12 de usuario realiza el descifrado real utilizando la función 66 de descifrado y la clave 72 privada. Sin embargo, antes de esto la unidad 50 de procesador solicita que el usuario introduzca una frase de contraseña. Sólo si se introduce la frase de contraseña correcta en el teclado 36 (o el usuario se identifica biométricamente de forma correcta de otra manera), se habilita el proceso de descifrado.

En la realización descrita en el presente documento, el cifrado y el descifrado se llevan a cabo según un método RSA asimétrico. Por el contrario, en configuraciones alternativas se proporcionan otros métodos de cifrado y descifrado asimétricos o simétricos, o formas híbridas de los mismos, tales como el cifrado simétrico que utiliza una clave cifrada asimétricamente. En los métodos simétricos, no hay necesidad de distinguir entre la clave 70 pública y la clave 72 privada.

En resumen, la tecnología propuesta garantiza que los datos 48 de usuario cifrados sólo pueden leerse o utilizarse si el módulo 12 de usuario del usuario autorizado está conectado a la interfaz 14, y el usuario se ha identificado correctamente, utilizando la frase de contraseña, por ejemplo.

En la presente realización, la totalidad del procedimiento de cifrado y descifrado se lleva a cabo mediante la unidad 50 de procesador del módulo 12 de usuario, no abandonando nunca los datos 60 de claves el módulo 12 de usuario. Sin embargo, existen, configuraciones alternativas en las que la función 64 de cifrado y la clave 70 pública, que no necesita que permanezca secreta, se transfieren al dispositivo 10 móvil, de manera que el proceso de cifrado puede llevarse a cabo mediante la unidad 32 de procesador, generalmente más potente, del dispositivo 10 móvil. En algunas configuraciones alternativas, la unidad 32 de procesador puede también utilizarse para el proceso de descifrado, siempre que no se comprometa la seguridad de la clave 72 privada de ese modo.

En la presente realización, la función 68 de generación de claves, que también se ejecuta por la unidad 50 de procesador del módulo 12 de usuario, se utiliza para generar los datos 60 de claves. De una manera conocida *per se*, este programa calcula un par de clave 70 pública y clave 72 privada. Esta medida garantiza un grado particularmente alto de seguridad de datos, puesto que la clave 72 privada no abandona el módulo 12 de usuario incluso cuando se está generando la clave.

La realización descrita en el presente documento no se limita ni a una única región cifrada para los datos 48 de usuario, ni a un único método de cifrado. Suponiendo que se ha suministrado prueba de identidad apropiada, por medio de la frase de contraseña, una región cifrada puede, por ejemplo, desactivarse en cualquier momento, y por tanto hacer que sea libremente accesible. La región también puede cifrarse de nuevo con el mismo o un módulo 12 de usuario diferente. Una pluralidad de regiones cifradas, opcionalmente con diferentes pares de claves y/o diferentes tamaños, puede también establecerse y gestionarse.

En particular, en la presente configuración que proporciona un proveedor ASP, los datos 48 de usuario cifrados pueden, además de almacenarse en el dispositivo 10 móvil, transferirse también a través de la interfaz 16 aérea a un servidor del proveedor ASP, y almacenarse allí. Los datos 48 de usuario que se almacenan en ambos lados pueden sincronizarse cada vez que un programa 46 de aplicación realiza un acceso de escritura, o si se termina una sesión de usuario, o si el usuario lo solicita explícitamente. Entonces, el usuario tiene, por un lado, acceso rápido a los datos 48 de usuarios almacenados localmente y es, por otro lado, independiente del dispositivo 10 móvil utilizado, puesto que puede recuperar los datos 48 de usuario que están almacenados con el proveedor ASP utilizando cualquier otro dispositivo móvil.

En algunas configuraciones, también puede proporcionarse dejar un componente de la clave con el operador de red o el proveedor ASP. Después de que el dispositivo 10 móvil ha entrado satisfactoriamente en la red 18 de telecomunicaciones, este componente de la clave se transfiere a través de la interfaz 16 aérea, de manera que el operador de red o proveedor ASP comparte con el usuario el control de ciertos datos 48 de usuario almacenados en el dispositivo 10 móvil.

REIVINDICACIONES

1. Método para almacenar y acceder a datos (48) de usuario en un dispositivo (10) móvil, en particular un teléfono móvil o un asistente digital personal, comprendiendo el dispositivo (10) móvil una memoria (38) de dispositivo y estando conectado a un módulo (12) de usuario a través de una interfaz (14), en el que

- los datos (48) de usuario se almacenan en la memoria (38) de dispositivo del dispositivo (10) móvil al menos parcialmente en forma cifrada,

caracterizado porque

- al menos el descifrado de los datos (48) de usuario en operaciones de acceso se realiza utilizando una función (66) de descifrado, proporcionándose la función (66) de descifrado mediante el módulo (12) de usuario y ejecutándose, al menos en parte, mediante una unidad (50) de procesador del módulo (12) de usuario.

2. Método según la reivindicación 1, **caracterizado** además porque el cifrado de los datos (48) de usuario en operaciones de almacenamiento se realiza utilizando una función (64) de cifrado, que se proporciona mediante el módulo (12) de usuario.

3. Método según tanto la reivindicación 1 como la reivindicación 2, **caracterizado** porque el módulo (12) de usuario comprende una memoria (52) de módulo, en la que están contenidas las funciones (64, 66) de cifrado y descifrado proporcionadas por el módulo (12) de usuario, así como los datos (60) de claves utilizados por estas funciones (64, 66), y porque las funciones (64, 66) de cifrado y descifrado se ejecutan, al menos en parte, por una unidad (50) de procesador del módulo (12) de usuario.

4. Método según la reivindicación 3, **caracterizado** porque se proporciona por el módulo (12) de usuario al menos una función (68) para generar los datos (60) de claves y para escribir los datos (60) de claves en la memoria (52) de módulo.

5. Método según cualquiera de las reivindicaciones 1 a 4, **caracterizado** porque al menos la ejecución de la función (66) de descifrado está protegida por una contraseña y/o una prueba biométrica.

6. Método según cualquiera de las reivindicaciones 1 a 5, **caracterizado** porque el dispositivo (10) móvil es un dispositivo que también está configurado para funciones de telecomunicaciones.

7. Método según cualquiera de las reivindicaciones 1 a 6, **caracterizado** porque el módulo (12) de usuario es un módulo de identificación de abonado que también se proporciona para entrar en una red (18) de telecomunicaciones.

8. Dispositivo (10) móvil, en particular un teléfono móvil o un asistente digital personal, comprendiendo el dispositivo (10) móvil una memoria (38) de dispositivo y una interfaz (14) para conectar un módulo (12) de usuario, en el que la memoria (38) de dispositivo comprende al menos una región para almacenar datos (48) de usuario en al menos una forma parcialmente cifrada,

caracterizado porque

el dispositivo (10) móvil está adaptado para utilizar, al menos para descifrar los datos (48) de usuario en operaciones de acceso, una función (66) de descifrado que se proporciona por el módulo (12) de usuario y se ejecuta, al menos en parte, por una unidad (50) de procesador del módulo (12) de usuario.

9. Módulo (12) de usuario, en particular un módulo de identificación de abonado para una red (18) de telecomunicaciones, comprendiendo el módulo (12) de usuario una unidad (50) de procesador y estando adaptado para conectarse, a través de una interfaz (14), a un dispositivo (10) móvil, en particular un teléfono móvil o un asistente digital personal, comprendiendo el dispositivo (10) móvil una memoria (38) de dispositivo que tiene al menos una región para almacenar datos (48) de usuario en al menos una forma parcialmente cifrada,

caracterizado porque

el módulo (12) de usuario está adaptado para proporcionar al dispositivo (10) móvil, a través de la interfaz (14), una función (66) de descifrado al menos para descifrar los datos (48) de usuario en operaciones de acceso, ejecutándose la función (66) de descifrado, al menos en parte, por la unidad (50) de procesador del módulo (12) de usuario.

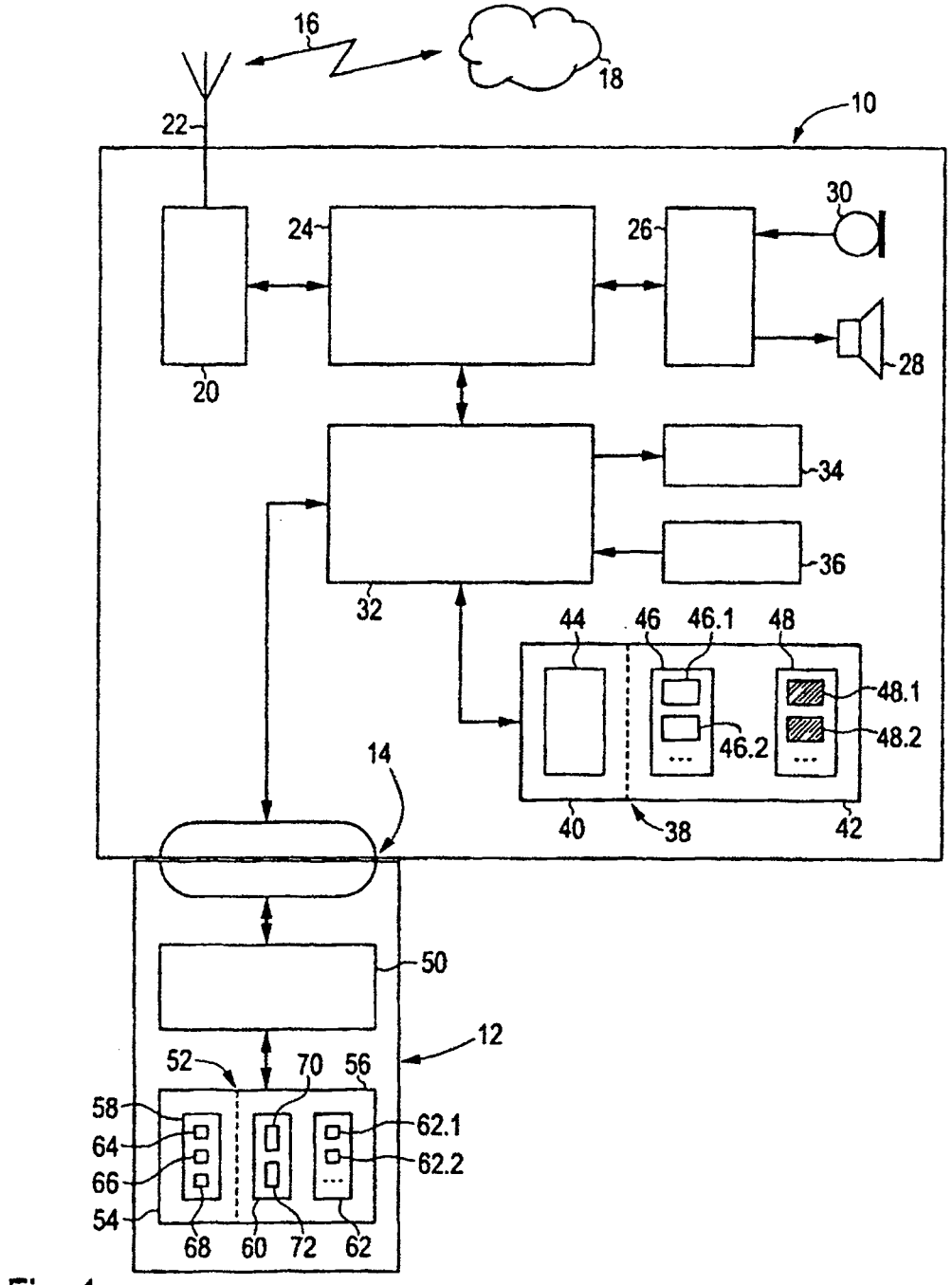
16
18
22
10
30
24
26
28
20
34
36
32
44
46
46.1
48
48.1
46.2
48.2
14
40
38
42
50
12
52
70
56
58
64
66
54
62.1
62.2
68
60
72
62

Fig. 1