(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 385 824**

(51) Int. CI.:
H04W 12/06 (2009.01)
H04W 12/02 (2009.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **03789430 .0**
(96) Fecha de presentación: **30.12.2003**
(97) Número de publicación de la solicitud: **1700444**
(97) Fecha de publicación de la solicitud: **13.09.2006**

(54) Título: **Procedimiento y sistema de protección de datos, red de comunicaciones relacionada y producto de programa informático**

(45) Fecha de publicación de la mención BOPI:
01.08.2012

(45) Fecha de la publicación del folleto de la patente:
01.08.2012

(73) Titular/es:
TELECOM ITALIA S.P.A.
PIAZZA DEGLI AFFARI, 2
20123 MILANO, IT

(72) Inventor/es:
LEONE, Manuel y
CAPRELLA, Ettore Elio

(74) Agente/Representante:
Ponti Sales, Adelaida

DESCRIPCIÓN

Procedimiento y sistema de protección de datos, red de comunicaciones relacionada y producto de programa informático

Campo de la invención

[0001] La presente invención se refiere en general a técnicas de protección de datos.

Descripción de la técnica relacionada

[0002] La criptografía se considera en la actualidad como una de las herramientas básicas para implementar la seguridad en sistemas y redes. En ese contexto, los esfuerzos se han centrado, y están centrándose, en sistemas criptográficos de clave pública.

[0003] Un sistema criptográfico de clave pública se basa en la suposición de que solamente el usuario conoce su clave privada. Esta condición es estrictamente necesaria, especialmente en el caso de servicios de firma digital. Para ese fin, las claves privadas de los usuarios se almacenan normalmente en dispositivos de seguridad específicos tales como tarjetas inteligentes, memorias USB o tarjetas PCI/PCMCIA. Estos dispositivos tienen la finalidad de almacenar las claves en memorias protegidas contra manipulaciones indebidas. También se encargan de todas las operaciones criptográficas basadas en tales claves, impidiendo normalmente la comunicación de tales claves al exterior con el fin de reducir el riesgo de comprometer su seguridad.

[0004] En el documento WO-A-98/44402 se proporciona un esquema de protección de derechos de autor en el que los datos se descargan desde un servidor, normalmente a través de Internet, hasta un cliente para su presentación a un usuario. Los datos descargados están protegidos criptográficamente mediante cifrado y funciones *hash*. Cuando se muestran por el cliente, las funciones de almacenamiento y de copiado se inhabilitan selectivamente con respecto a los datos para impedir un copiado no autorizado.

[0005] El documento US-A-2003/0097341 desvela un procedimiento de cifrado de datos, un terminal de telecomunicaciones y una tarjeta de autorización de acceso que permiten la utilización de servicios de uno o más proveedores de servicio independientemente de un operador de red o del fabricante del terminal de telecomunicaciones. Los datos cifrados se transmiten entre un proveedor de servicios y un terminal de telecomunicaciones a través de una red de telecomunicaciones. Los datos que van a transmitirse a través de la red de telecomunicaciones se cifran en función del proveedor de servicios seleccionado.

[0006] Además, el documento WO-A-02/052784 desvela un procedimiento de autenticación de un cliente que comprende la etapa de enviar una identidad de abonado a un servidor de autenticación, obtener al menos un desafío y al menos un primer secreto con respecto al servidor de autenticación basado en un secreto de un cliente específico del cliente. Etapas adicionales incluyen formar primeros credenciales, formar una primera clave de autenticación usando el al menos un primer secreto, cifrar los primeros credenciales usando la primera clave de autenticación, enviar el al menos un desafío y los primeros credenciales cifrados al cliente, formar una versión propia de la primera clave de autenticación con respecto al cliente. Los primeros credenciales cifrados se descifran usando la versión propia de la primera clave de autenticación. En un procedimiento de este tipo, los credenciales cifrados se envían junto con el al menos un desafío al cliente, de manera que el cliente sólo puede proceder con la autenticación si puede obtener el primer secreto a partir del al menos un desafío.

[0007] Además, el documento WO 03/037016 desvela un procedimiento para almacenar información alfanumérica, como por ejemplo números de teléfono y nombres de una agenda, en un centro de almacenamiento conectado a la red, y para la posterior recuperación y almacenamiento de los mismos en la memoria del teléfono o en una tarjeta SIM insertada en el mismo, donde dicho centro de almacenamiento comprende al menos un ordenador electrónico dotado de una memoria dividida en tantos bancos de memoria como número de usuarios que pueden usar el servicio de almacenamiento de datos, donde el teléfono móvil implementa un algoritmo de cifrado cuya clave consiste en una contraseña que puede introducirse por el usuario del teléfono, y donde los procedimientos de almacenamiento y de recuperación de información se basan en un intercambio de mensajes SMS sencillos cifrados de manera adecuada.

Objeto y resumen de la invención

[0008] Por tanto, el objeto de la invención es proporcionar una disposición adaptada para ofrecer flexibilidad y seguridad en lo que respecta a la protección de elementos de información privados de un usuario, tales como claves privadas y certificados de un usuario, especialmente cuando no resulta adecuado almacenarlos en dispositivos "ad

hoc".

[0009] Más específicamente, la invención tiene como objetivo garantizar un alto nivel de seguridad también para usuarios móviles y, en cualquier caso, para los usuarios que utilicen terminales tales como ordenadores de tamaño agenda, ordenadores portátiles, ordenadores personales, PDA, teléfonos inteligentes, etc., conectados a una red y que necesitan sus claves privadas criptográficas para acceder a servicios de seguridad.

[0010] Según un aspecto de la presente invención, tal objeto se consigue mediante un procedimiento para almacenar de manera segura al menos un elemento de información privado de un usuario, que incluye las etapas de:

- asignar a dicho usuario un módulo de identidad de abonado respectivo, almacenando dicho módulo de identidad de abonado al menos un algoritmo de seguridad;
- producir al menos una clave de cifrado a través de dicho al menos un algoritmo de seguridad; y
- proporcionar una ubicación de almacenamiento remota a la que puede acceder dicho usuario a través de una red de comunicaciones, donde dicho elemento de información privado del usuario está almacenado como un archivo cifrado a través de dicha al menos una clave de cifrado.

[0011] Según otro aspecto de la presente invención, tal objeto se consigue mediante un sistema que almacena de manera segura al menos un elemento de información privado de un usuario, que incluye:

- un módulo de identidad de abonado, almacenando dicho módulo de identidad de abonado al menos un algoritmo de seguridad;
- un terminal de usuario que comprende un módulo de procesamiento, pudiendo conectarse dicho módulo de procesamiento a dicho módulo de identidad de abonado para producir una clave de cifrado a través de dicho al menos un algoritmo de seguridad, utilizándose dicha clave de cifrado para cifrar dicho elemento de información privado del usuario; y
- una ubicación de almacenamiento remota, KR, a la que puede acceder dicho usuario a través de una red de comunicaciones, estando configurada dicha ubicación de almacenamiento remota, KR, para almacenar dicho elemento de información privado del usuario como un archivo cifrado a través de dicha clave de cifrado.

[0012] Según aspectos adicionales de la presente invención, tal objeto se consigue mediante una red de comunicaciones relacionada y un producto de programa informático que puede cargarse en la memoria de al menos un ordenador y que comprende partes de código software para llevar a cabo las etapas del procedimiento de la invención cuando el producto se ejecuta en un ordenador. Tal y como se utiliza en este documento, la referencia a tal producto de programa informático es equivalente a hacer referencia a un medio legible por ordenador que contiene instrucciones para controlar un sistema informático para coordinar el funcionamiento del procedimiento de la invención. La referencia a “al menos un ordenador” señala evidentemente la posibilidad de que el sistema de la invención se implemente de manera distribuida/modular.

[0013] Aspectos preferidos adicionales de la presente invención se describen en las reivindicaciones dependientes y en la siguiente descripción.

[0014] Específicamente, la disposición descrita en este documento proporciona el nivel de protección requerido utilizando un dispositivo que tiene un alto grado de difusión en el contexto de las comunicaciones móviles, concretamente un módulo de identidad de abonado o SIM.

[0015] Específicamente, en la disposición descrita en este documento, los elementos de información privados de un usuario (tales como, por ejemplo, claves privadas y certificados) están almacenados en un servidor remoto, protegidos mediante algoritmos criptográficos por medio de claves que sólo pueden generarse a través de los SIM de usuario que funcionan con un módulo de procesamiento específico instalado en los terminales de los usuarios. De esa manera, los usuarios pueden solicitar sus elementos de información privados desde cualquier terminal que tenga una conexión de red al servidor remoto en cuestión. Tales elementos de información privados se transmiten de manera cifrada y sólo pueden usarse si el usuario posee el SIM correcto, concretamente el SIM que ha cifrado tales elementos de información privados en una fase de registro anterior.

[0016] De esta manera, el uso de los elementos de información se controla completamente por el SIM del propietario de los elementos de información. El acceso a los elementos de información privados cifrados no revelará por sí mismo ninguna información relacionada con los elementos de información privados de los usuarios. Además, incluso el servidor remoto que almacena los elementos de información privados cifrados no estará en posición de acceder a los elementos de información privados de los usuarios en forma de texto plano, al no disponer de los SIM de los usuarios. De esa manera, el servidor remoto no estará sujeto a ninguna responsabilidad específica y reducirá

los riesgos que pueda haber en la seguridad, incluso cuando ésta quede comprometida.

[0017] El mecanismo de protección de los elementos de información privados de los usuarios no está basado en mecanismos basados en contraseñas ni requiere hardware “ad hoc”. Esto hace posible neutralizar todos los ataques utilizados para comprometer la seguridad de todo el sistema.

[0018] Mediante la disposición descrita en este documento, el usuario puede acceder a sus claves privadas (o a cualquier otro elemento de información privado) desde cualquier terminal que tenga una conexión de red tal como una conexión a Internet. Una vez descifradas por el SIM, tales claves privadas pueden usarse directamente con un software instalado en el propio terminal. Normalmente, tal software ya está adaptado para utilizar tales claves privadas de manera nativa, como es el caso de la mayoría de plataformas de Microsoft™ (Internet Explorer, Outlook, Outlook Express, Explorer, Office, etc.; al menos algunas de estas designaciones son marcas registradas). Además, es razonable creer que el número de aplicaciones adaptadas para utilizar las claves privadas y los certificados de los usuarios de manera nativa, sin ningún software adicional, aumentará en el futuro.

[0019] Con el fin de proporcionar a un cliente un mayor grado de flexibilidad y movilidad, el módulo de procesamiento que se ejecuta en el terminal de usuario puede implementarse a través de tecnologías tales como los *applets* de Java o ActiveX. De esta manera, no es necesario que el módulo de procesamiento esté preinstalado en el terminal de usuario, ya que puede descargarse (e instalarse automáticamente) en tiempo real desde una página web, concretamente cuando el usuario solicita acceso a sus claves privadas. Usando técnicas de firma digital, que están disponibles tanto en entornos Java como ActiveX, el usuario puede comprobar si el software descargado es legítimo y no ha sido desarrollado maliciosamente por un pirata informático con el objetivo de revelar las claves privadas del usuario.

Breve descripción de los dibujos adjuntos

[0020] A continuación se describirá la invención, solamente a modo de ejemplo, haciendo referencia a las figuras adjuntas de los dibujos, en los que:

- la figura 1 es un diagrama de bloques a modo de ejemplo de la arquitectura de un sistema como el descrito en este documento,
- las figuras 2, 4, 6 y 7 son gráficos a modo de ejemplo del posible funcionamiento de un sistema según la disposición descrita en este documento, y
- las figuras 3 y 5 son diagramas de bloques funcionales que representan el tratamiento de datos en la disposición descrita en este documento.

Descripción detallada de realizaciones preferidas de la invención

[0021] La disposición descrita en este documento permite que usuarios móviles o, en cualquier caso, usuarios que utilizan terminales tales como ordenadores de tamaño agenda, ordenadores portátiles, ordenadores personales, PDA, teléfonos inteligentes y similares, tengan disponibles determinados elementos de información privados tales como, por ejemplo, claves privadas y certificados, cuando se conecten a una red.

[0022] Esto se produce en condiciones de seguridad, sin tener que recurrir a dispositivos de seguridad ad hoc, tales como tarjetas inteligentes, memorias USB, tarjetas PCI/PCMCIA, etc.

[0023] La protección de los elementos de información privados se realiza a través de un dispositivo de seguridad actualmente disponible para los usuarios de redes móviles, concretamente un módulo de identidad de abonado o SIM del usuario.

[0024] Específicamente, la disposición descrita en este documento permite a los usuarios de cualquier infraestructura de claves públicas (PKI), concretamente una infraestructura cuyos servicios están basados en una disposición criptográfica de clave pública, tener un mayor grado de seguridad con respecto a las contraseñas. Esto es así incluso si no poseen una tarjeta inteligente u otro elemento o dispositivo hardware dedicado específicamente a ese fin.

[0025] La disposición descrita en este documento requiere que los usuarios estén dotados de un SIM y que tal SIM pueda conectarse a un terminal de usuario. Tal terminal de usuario puede ser un ordenador de tamaño agenda, un ordenador portátil, un ordenador personal, un PDA, un teléfono móvil, etc.

[0026] En la actualidad existen varias maneras de interconectar tales dispositivos con un SIM.

[0027] Se hace referencia a una lista a modo de ejemplo en el diagrama de bloques de la figura 1.

[0028] Específicamente, en la disposición mostrada en la figura 1, el SIM puede interconectarse con un terminal de usuario TU de varias maneras tales como, pero sin limitarse a:

- un lector PCSC estándar 10;
- un teléfono móvil por medio de un canal *Bluetooth* 20 (utilizado como un lector de SIM inalámbrico);
- un teléfono móvil por medio de un canal IrDA 30; o
- un teléfono móvil 40 por medio de un cable conectado a un puerto serie/paralelo/USB/Firewire (utilizado como un lector de SIM cableado).

[0029] Se espera que la evolución tecnológica proporcione nuevos dispositivos y protocolos para interconectar un SIM con un sistema informático. La presente invención abarca el posible uso de tales nuevos dispositivos y protocolos.

[0030] A través del SIM respectivo y recurriendo a la disposición descrita en este documento, el usuario (designado en lo sucesivo como U) está en posición de:

- autenticarse con un repositorio de claves (en lo sucesivo, KR) que tiene almacenadas en el mismo, de manera cifrada, las respectivas claves privadas (o cualquier otro elemento de información privado);
- solicitar y descargar sus propias claves privadas de manera cifrada;
- descifrar tales claves privadas a través del SIM; y
- utilizar localmente tales claves privadas y borrarlas posiblemente de manera segura cuando ya no hagan falta.

[0031] Esencialmente, la disposición descrita en este documento requiere la presencia de los siguientes elementos:

SIM: tal y como se utiliza en este documento, designa una tarjeta SIM o una tarjeta USIM, utilizadas normalmente en redes móviles, tales como redes GSM o UMTS, respectivamente, para controlar y proteger el acceso del usuario a los recursos de red. Específicamente, para obtener acceso a una red móvil, un usuario debe autenticarse. En una red GSM/UMTS, esta autenticación se implementa como un mecanismo de desafío-respuesta clásico. La red envía un valor aleatorio, denominado RAND, al teléfono móvil del usuario que, a su vez, reenvía el valor al SIM. El SIM, que contiene una clave secreta única, llamada Ki, cifra esta RAND con un algoritmo dependiente de operador móvil llamado A3, para producir una respuesta de autenticación SRES. Esta respuesta de autenticación SRES se devuelve a la red la cual, conociendo la clave SIM Ki, lleva a cabo el mismo cálculo y comprueba su SRES con la suministrada por el usuario. Si los dos valores coinciden se concede acceso al usuario; en caso contrario, se rechaza la solicitud de acceso. En el primer caso, el SIM también cifrará el valor RAND con otro algoritmo dependiente de operador móvil, llamado A8, y con la clave Ki, para producir una clave de sesión, llamada Kc. Esta clave se pasará al teléfono móvil para proteger el enlace de radio entre el teléfono móvil y la estación transceptora de red móvil.

Usuario (U): es el propietario del SIM y de las claves privadas (o, más en general, de los elementos de información privados) a proteger. El usuario U puede necesitar utilizar tales claves privadas con una pluralidad de terminales, tales como ordenadores de tamaño agenda, ordenadores portátiles, ordenadores personales, PDA, teléfonos inteligentes, etc.

Terminal de usuario (TU): tal y como se utiliza en este documento, es el terminal conectado a una red que permite al usuario U contactar con un repositorio de claves KR que tiene almacenadas en el mismo sus claves privadas. Un terminal de este tipo está conectado además (véase la figura 1) al SIM del usuario. Una lista no limitativa de terminales de usuario TU adaptada para usarse en la disposición descrita en este documento incluye un ordenador personal, un ordenador de tamaño agenda, un ordenador portátil, un PDA, un teléfono inteligente. El terminal puede conectarse al SIM mediante varias tecnologías, por ejemplo a través de un lector de tarjetas inteligentes, un terminal móvil con *Bluetooth,* un terminal móvil con IrDA, un terminal móvil por medio de un cable.

[0032] Además, un módulo de procesamiento instalado en el terminal de usuario TU está adaptado para conectarse e intercambiar información con el repositorio de claves KR, por un lado, y con el SIM del usuario, por otro lado.

[0033] Repositorio de claves (KR): tal y como se ha indicado anteriormente, es un servidor remoto que almacena de manera cifrada las claves privadas de los usuarios. Un servidor remoto de este tipo está adaptado para ser accesible a los terminales de los usuarios U con el fin de permitir el acceso a las respectivas claves privadas

cifradas.

[0034] Función de interfuncionamiento (IWF): tal y como se utiliza en este documento, es un servidor (normalmente bajo el control del operador móvil que facilitó el SIM) adaptado para verificar que los SIM que solicitan acceso a las claves privadas están activos y son válidos (concretamente, que no se haya notificado su robo, pérdida, etc.). Un servidor de este tipo está en posición de interactuar con la red respectiva (por ejemplo, una red GSM o una red UMTS) y específicamente con un denominado AuC (centro de autenticación) con el fin de llevar a cabo la función de autenticación de los usuarios U o, para ser más precisos, de los SIM. Por consiguiente, desempeña el papel de una pasarela de autenticación entre una red IP y una red GSM/UMTS. Tal y como se explicará posteriormente en mayor detalle, la presencia de una función de interfuncionamiento IWF no es obligatoria para los fines de funcionamiento de la disposición descrita en este documento. Sin embargo, los expertos en la técnica apreciarán que la presencia de una función de interfuncionamiento puede aumentar el nivel de seguridad de todo el sistema.

[0035] La presente descripción se refiere, solamente a modo de ejemplo, a una posible realización de la disposición descrita en este documento basada en una red GSM y en una infraestructura SIM relacionada. Los expertos en la técnica apreciarán fácilmente que la disposición descrita en este documento puede adaptarse para funcionar en el marco de, por ejemplo, una red UMTS utilizando la infraestructura USIM relacionada. Lo mismo puede aplicarse a cualquier otro marco de red soportado por una infraestructura de identidad de abonado basada en cifrado que sigue el esquema de desafío-respuesta o, si no, esencialmente similar a la infraestructura SIM.

[0036] Tal y como se utiliza en este documento, el término “SIM” abarca por tanto todas estas infraestructuras alternativas basadas en los mismos principios de funcionamiento.

[0037] Los elementos designados como TU, KR e IWF (si están presentes) están conectados a través de tecnologías y protocolos de red. Pueden usarse soluciones estándar o soluciones propietarias para este fin. La siguiente descripción se referirá, solamente a modo de ejemplo, a tecnologías y protocolos estándar definidos por el IETF (Grupo Especial de Ingeniería de Internet), la principal entidad internacional para la normalización de protocolos utilizados en redes IP.

[0038] Las etapas proporcionadas en la disposición descrita en este documento para localizar y descifrar las claves privadas del usuario pueden implementarse mediante el módulo de procesamiento presente en el terminal de usuario TU. Como se ha indicado, no es necesario que tal módulo de procesamiento esté preinstalado en el terminal. Puede descargarse fácilmente en línea desde un sitio web al que se conecta el usuario U.

[0039] Pueden usarse varias tecnologías, tales como Java y ActiveX, para este fin. Estas tecnologías permiten incluir código objeto ejecutable directamente en una página web mediante TAG. Un navegador adaptado para soportar tales tecnologías, como Internet Explorer, Netscape Navigator u Opera, están en posición de, después de detectar la presencia de un *applet* de Java o ActiveX, descargar localmente el código correspondiente y ejecutar el mismo.

[0040] Ambas tecnologías permiten definir políticas de seguridad cuando se descarga el código ejecutable. Específicamente, existe la posibilidad de configurar el navegador de manera que solo se descarguen *applets* de Java y ActiveX que lleven una firma digital. Esto es principalmente para reducir el riesgo de descargar el denominado "maleware", concretamente software escrito con la única finalidad de revelar los datos de los usuarios o de acceder de manera no autorizada a los terminales de usuario TU.

[0041] Pueden adoptarse otras soluciones para la misma finalidad, tal como descargar un código ejecutable a través de protocolos de red como FTP, TFTP, HTTP. Como alternativa, el código requerido puede preinstalarse a través de otros medios tales como un CD, un disco flexible, una memoria USB, etc. Por supuesto, una descarga en línea puede ser preferible en lo que respecta a garantizar una mayor variedad de dispositivos.

[0042] A continuación se considerarán dos procedimientos básicos, en concreto:

- procedimiento de registro de usuario, y
- acceso por parte del usuario a las claves privadas.

[0043] El procedimiento de registro de usuario tiene como objetivo crear, con el repositorio de claves KR, una asociación de los archivos que contienen las claves privadas, cifradas a través de los SIM, con los propios SIM.

[0044] Tal procedimiento se lleva a cabo inicialmente para registrar el usuario U y posteriormente cada vez que el usuario U desee modificar sus claves privadas o las claves secretas, generadas por el SIM, que protegen a su

vez las claves privadas (o, más en general, los elementos de información privados de los usuarios).

[0045] El procedimiento de registro de usuario puede llevarse a cabo en un entorno local, en una situación controlada y protegida, o de manera remota, en una red dedicada o pública. En este último caso, la integridad, la autenticación y la confidencialidad de la comunicación están protegidas contra ataques de repetición. Esto puede implementarse en función de varias soluciones conocidas en la técnica tales como, por ejemplo, IPsec, SSL/TLS, SSH, etc.

[0046] Tal y como se muestra en la figura 2, el procedimiento de registro de usuario implica las etapas detalladas a continuación.

[0047] En una primera etapa 100, el usuario U interconecta su terminal TU con un SIM del usuario. Para este fin pueden usarse varias soluciones diferentes, como se muestra en la figura 1.

[0048] Específicamente, el usuario U activa en su terminal TU un módulo de procesamiento adaptado para cifrar los archivos correspondientes con respecto a las claves privadas a través del SIM en función del mecanismo descrito en este documento. El módulo de procesamiento comprueba si un SIM está conectado al terminal de usuario TU mediante uno de los canales 10 a 40 mostrados en la figura 1.

[0049] Una vez que se ha detectado un SIM, el módulo de procesamiento comprueba la posible presencia de un PIN que protege un acceso. En ese caso, se solicita al usuario U que introduzca un PIN correspondiente, lo que se produce a través de, por ejemplo, una interfaz gráfica de usuario (GUI).

[0050] Posteriormente, en una etapa 102, el módulo de procesamiento accede a la SIM (posiblemente a través del PIN proporcionado por el usuario U) y, en una etapa 104 produce dos valores aleatorios RAND1 y RAND2, en particular dos valores aleatorios de 128 bits. Estos valores aleatorios RAND1 y RAND2 se reenvían al SIM.

[0051] En una etapa 106, el SIM calcula dos claves de sesión Kc1 y Kc2, que incluyen cada una 64 bits, basándose en la clave secreta Ki del SIM y el algoritmo de seguridad A8 GSM. El algoritmo de seguridad A8 GSM representa el algoritmo de seguridad básico almacenado en el SIM. Detalles específicos a este respecto pueden obtenerse en la especificación técnica GSM 03.20 (ETSI TS 100 929 v8.1.0) de GSM: "*Digital cellular telecommunication system (Phase 2+); Security Related network functions*", Instituto Europeo de Normas de Telecomunicaciones, julio de 2001; o en la especificación técnica GSM 11.11 (ETSI TS 100 977 v.8.3.0) de GSM: "*Digital cellular telecommunication system (Phase 2+); Specification of the Subscriber Identity Module - Module Equipment (SIM-ME) interface*", Instituto Europeo de Normas de Telecomunicaciones, agosto de 2000.

[0052] Tal cálculo está basado en los dos valores aleatorios RAND1 y RAND2 proporcionados por el módulo de procesamiento. En resumen: Kc1 = A8 (RAND1), Kc2 = A8 - (RAND2). Estas dos claves de sesión Kc1 y Kc2 se envían al módulo de procesamiento que, en una etapa adicional 108, calcula una clave de cifrado K, que incluye 128 bits, aplicando una función *hash* h a la concatenación de las dos claves de sesión Kc1 y Kc2. En resumen: K=h(Kc1, Kc2). Información general relacionada con este tipo de procesamiento puede encontrarse en el documento "*Handbook of Applied Cryptograpy*", de A.J. Menezes, P.C. van Oorschot, S. A. Vanstone, CRC Press, ISBN: 0-8493-8523-7, octubre de 1996.

[0053] Pueden usarse diferentes funciones para ese fin tales como (haciendo referencia a una lista no limitativa) una función SHA-1 o una función MD5.

[0054] También es posible calcular la clave de cifrado K de diferente manera, posiblemente usando también las respuestas de autenticación SRES obtenidas a través de los desafíos de autenticación (valores aleatorios) RAND1 y RAND2. En general, la clave de cifrado K puede calcularse como una función de las dos claves de sesión Kc1 y Kc2 y de las respuestas de autenticación SRES1, SRES2 obtenidas a través de los desafíos de autenticación RAND1 y RAND2: K=f (Kc1, Kc2, SRES1, SRES2). De esta manera, es posible cambiar la longitud de las claves de cifrado actuando sobre el número de entradas procesadas. Por ejemplo, es posible aumentar el número de entradas a procesar enviando una secuencia de desafíos de autenticación RAND1, RAND2,..., RANDn y procesando las salidas correspondientes del SIM Kc1, Kc2,..., Kcn, SRES1, SRES2,..., SRESn. Por lo tanto, en ese caso, K=f (Kc1, Kc2,…, Kcn, SRES1, SRES2,…, SRESn).

[0055] Además, el usuario U puede añadir una clave secreta personalizada K_U con el fin de cambiar la clave de cifrado K de manera que ya no depende exclusivamente de la función de seguridad GSM. De esta manera, ni siquiera el operador de red móvil, que tiene constancia de todos los datos relacionados con los SIM de los usuarios, puede llevar a cabo una función de recuperación de claves de las claves privadas de un usuario U sin la cooperación positiva del usuario U. En este último caso, la función para generar la clave de cifrado K se expresará mediante la

fórmula: K=f (K_U, Kc1, Kc2,…, Kcn, SRES1, SRES2,…, SRESn), donde K_U es la clave secreta personalizada seleccionada por el usuario U.

[0056] Posteriormente, el módulo de procesamiento también puede generar, en una etapa 110, un vector aleatorio, vector de inicialización definido IV, que incluye, por ejemplo, 128 bits. Tal vector aleatorio se utiliza en el procesamiento de cifrado (cifrar/descifrar) cuando se utiliza un modo de cifrado que solicita un vector de inicialización, tal como CBC (cadena de bloques de cifrado), CFB (retroalimentación de cifrado), OFB (retroalimentación de salida). El vector de inicialización IV también puede omitirse dependiendo del modo de funcionamiento de la entidad de cifrado; por ejemplo, el vector de inicialización IV no es necesario en el caso de ECB (libro de códigos electrónico). Detalles de los diversos procedimientos de procesamiento de cifrado a los que se ha hecho referencia anteriormente se proporcionan, por ejemplo, en el documento de Menezes et al., mencionado anteriormente.

[0057] En una etapa 112, el módulo de procesamiento cifra los archivos correspondientes a las claves privadas de usuario (o los elementos de información privados) a través de la clave de cifrado K y el vector aleatorio IV, por ejemplo usando el cifrado AES en el modo CBC. Sin embargo, puede usarse cualquier otro procedimiento de cifrado simétrico tal como, por ejemplo, RC6, Twofish, Serpent, 3DES, siendo ésta una lista no limitativa. Opcionalmente, el módulo de procesamiento puede llevar a cabo una compresión de los archivos que incluyen las claves privadas antes de aplicar las funciones de cifrado. Para este fin pueden usarse varios algoritmos que no producen pérdidas, tales como: PKZIP, GZIP, RAR, ACE, ARJ, LZH, siendo ésta una lista no limitativa. Los datos cifrados generados se indican mediante la referencia ED en la figura 3.

[0058] El módulo de procesamiento también inserta en el archivo cifrado una cabecera criptográfica CH para permitir el descifrado.

[0059] Tal y como se muestra en la figura 3, tal cabecera criptográfica CH incluye los siguientes campos:

- RAND1, RAND2, es decir, los dos valores aleatorios (desafíos de autenticación) enviados al SIM para generar la clave de cifrado K;
- IV, es decir, el vector aleatorio utilizado posiblemente para el cifrado (CBC u otro modo de cifrado que requiere un parámetro de este tipo) y generado por el módulo de procesamiento;
- Versión: es una cadena de caracteres auxiliar que codifica la versión del módulo de procesamiento, el algoritmo de cifrado utilizado (AES, RC6, 3DES, etc.), el modo de cifrado utilizado (CBC, ECB, OFB, etc.), la función *hash* utilizada (SHA-1, MD5, RIPEMD, Tiger, etc.), el algoritmo de compresión posiblemente utilizado (PKZIP, RAR, ARJ) y otra información útil; y
- MAC_K (RAND1, RAND2, IV, versión, archivo cifrado) es una suma de control criptográfica aplicada al archivo cifrado y a los tres campos anteriores. Tal suma de control criptográfica puede generarse mediante una función MAC (código de autenticación de mensaje). Funciones MAC a modo de ejemplo son, por ejemplo, HMAC-SHA-1, HMAC-MD5, AES-XCBC-MAC. En lo que sigue, se asumirá que se utiliza la función HMAC-SHA-1. En cualquier caso, tal suma de control criptográfica también detecta cualquier posible modificación no autorizada del archivo cifrado.

[0060] Volviendo al diagrama de flujo de la figura 2, en una etapa 114, el archivo cifrado, junto con un identificador SIM, se transfiere al repositorio de claves KR, en el cual el archivo cifrado se almacena en una base de datos. Puede recurrirse a varios elementos para que actúen como el identificador SIM. Algunos ejemplos son la IMSI (Identidad Internacional de Estación Móvil, en la actualidad Identidad Internacional de Abonado Móvil), el MSISDN (Número ISDN de Abonado Móvil), el número de serie SIM, etc. En lo sucesivo se asumirá que se utiliza el identificador IMSI. Finalmente, el repositorio de claves KR puede enviar el identificador SIM a la función de interfuncionamiento IWF (si la hubiera) para insertar el SIM del usuario en la lista de los SIM que pueden ofrecer tal servicio.

[0061] El procedimiento que permite al usuario U acceder al archivo cifrado permite acceder a y descargar localmente las claves privadas (o cualquier otro elemento de información privado) por parte de usuario U de manera segura bajo el control del SIM. Tal acceso puede tener lugar desde cualquier terminal de usuario TU dotado del módulo de procesamiento considerado anteriormente y conectado al repositorio de claves KR, al SIM y, posiblemente, a la función de interfuncionamiento IWF.

[0062] Específicamente, una realización preferida de la disposición descrita en este documento, proporciona, como se ilustra en la figura 4, una primera interacción entre el usuario U y la función de interfuncionamiento IWF. Tal interacción tiene como objetivo autenticar al usuario U a través del SIM y crear una clave de acceso K_{IWF} actuando conjuntamente con el usuario U y la función de interfuncionamiento IWF para utilizarse posteriormente en la comunicación con el repositorio de claves KR. Las etapas ilustradas en la figura 4 pueden llevarse a cabo en una red compartida.

[0063] En lo que sigue se asumirá que el usuario U ha interconectado de manera adecuada su propio terminal TU con el SIM. Esto puede suceder recurriendo a las diversas soluciones técnicas ilustradas en la figura 1.

[0064] En una etapa 200, el usuario U activa en su terminal el módulo de procesamiento que se conecta con la función de interfuncionamiento IWF a través de un protocolo tal como SSL/TLS o similar. Utilizar un protocolo tal como SSL/TLS permite al usuario U autenticar la función de interfuncionamiento IWF a través de técnicas convencionales (tales como certificados digitales) actualmente disponibles con los navegadores web (tales como Internet Explorer, Netscape Navigator, Opera) en varias plataformas tales como Windows 9X/Me/NT/2000/XP/PocketPC/CE, Linux, Sun Solaris, etc.

[0065] También es posible utilizar cualquier otro protocolo equivalente adaptado para proporcionar la autenticación del servidor (concretamente, de la función de interfuncionamiento IWF), confidencialidad en las comunicaciones, integridad en las comunicaciones y protección contra ataques de repetición.

[0066] En este punto, en dos etapas designadas como 202 y 204, respectivamente, el terminal de usuario TU solicita y obtiene un identificador del SIM. Este identificador SIM, representado, por ejemplo, por la IMSI, se envía a la función de interfuncionamiento IWF en una etapa 206.

[0067] La función de interfuncionamiento IWF lleva a cabo dos etapas de autenticación GSM típicas enviando al usuario U dos desafíos de autenticación RAND1 y RAND2, comprendidos por números generados aleatoriamente, y controlando las respuestas de autenticación correspondientes SRES1 y SRES2. Esto se produce en etapas posteriores. En las etapas 208 y 210, los dos desafíos de autenticación se envían desde la función de interfuncionamiento IWF al SIM a través del terminal de usuario TU. En dos etapas adicionales 212 y 214, las respuestas de autenticación SRES1 y SRES2 se envían desde el SIM a la función de interfuncionamiento IWF a través del terminal de usuario TU.

[0068] La autenticación GSM que sea satisfactoria se comunica mediante la función de interfuncionamiento IWF al terminal de usuario TU, en una etapa 216 (evidentemente, estas etapas también pueden transportar la información de una autenticación GSM abortada, en cuyo caso el procedimiento queda interrumpido).

[0069] Si el procedimiento continúa, la función de interfuncionamiento IWF y el usuario U generan localmente la clave de acceso K_{IWF}, calculada como $K_{IWF}=h(Kc1, Kc2)$. Las respectivas etapas son esencialmente similares a las descritas anteriormente con relación a las etapas 104 a 108 de la figura 2.

[0070] La función de interfuncionamiento IWF almacena en la base de datos IWF la clave de acceso K_{IWF}.

[0071] Además, la función de interfuncionamiento IWF almacena en la base de datos IWF la asociación de la clave de acceso K_{IWF} y el identificador SIM, concretamente la IMSI, junto con otra información de registro tal como, por ejemplo, los últimos datos de acceso LA, la clave de acceso anterior $K_{IWF\text{-}anterior}$, etc. La estructura de datos correspondiente está representada en la figura 5, que es un ejemplo de un registro típico adaptado para su almacenamiento en la base de datos IWF.

[0072] Además, en este caso, existe la posibilidad de generar la clave de acceso K_{IWF} según diferentes estrategias. Por ejemplo, la clave de acceso K_{IWF} puede calcularse como $K_{IWF}=f(K_{U\text{-}IWF}, Kc1, Kc2,..., Kcn, SRES1, SRES2,..., SRESn)$ donde $K_{U\text{-}IWF}$ es la clave secreta personalizada K_U compartida en el procedimiento de registro de usuario entre el usuario U y la función de interfuncionamiento IWF, mientras que SRES1,..., SRESn, Kc1, Kcn son n respuestas de autenticación y n claves de sesión obtenidas a través de los algoritmos de seguridad A3 y A8 GSM en función de n desafíos de autenticación RAND1,..., RANDn. También es posible utilizar otras estrategias de autenticación basadas o no en el SIM.

[0073] El módulo de procesamiento del terminal de usuario TU se conecta posteriormente al repositorio de claves KR a través del protocolo SSL/TLS u otro similar. Esto implica esencialmente una etapa de establecimiento de conexión designada como 300 en la figura 6.

[0074] Utilizar un protocolo tal como SSL/TLS permite al usuario U autenticar el repositorio de claves KR mediante técnicas convencionales (certificados digitales), actualmente disponibles en los navegadores web (tales como Internet Explorer, Netscape Navigator, Opera) de varias plataformas (Windows 9X/Me/NT/2000/XP/PocketPC/CE, Linux, Sun Solaris, etc.). También es posible utilizar para ese fin cualquier otro protocolo funcionalmente equivalente adaptado para proporcionar una autenticación de servidor (concretamente autenticación del repositorio de claves KR), confidencialidad en las comunicaciones, integridad en las comunicaciones y protección contra ataques de repetición.

[0075] Posteriormente, el módulo de procesamiento lleva a cabo una solicitud de acceso a las claves privadas de usuario mediante un mensaje de solicitud. Para este fin, el terminal de usuario TU solicita y obtiene del SIM el identificador SIM respectivo (IMSI), en dos etapas designadas como 302 y 304 en la figura 6. Este identificador SIM se envía posteriormente en una etapa 306 al repositorio de claves KR junto con otros parámetros, tales como:

- un identificador, designado como ID, de la clave privada que se ha solicitado; este parámetro puede identificar una o más claves privadas asociadas con el mismo usuario;
- una marca de tiempo de la solicitud (si está disponible); este parámetro, designado como T, identifica la hora en un formato acordado por las partes, tal como UTC;
- Un N_{once} N_u, concretamente un parámetro adaptado para neutralizar posibles ataques de repetición; generalmente está comprendido por valores aleatorios, números de secuencia o parámetros de tiempo.

[0076] El repositorio de claves KR comprueba si el SIM especificado está registrado y, si es así, la coherencia del parámetro T.

[0077] Si la comprobación genera un resultado positivo, el repositorio de claves KR genera un N_{once} N_{KR} respectivo, y en una etapa 308 envía al terminal de usuario TU un mensaje que comprende la siguiente información: IMSI, ID, T, N_U N_{KR}.

[0078] En este punto, el módulo de procesamiento comprueba, en el mensaje recibido, la presencia y validez de los diversos parámetros y después calcula una suma de control criptográfica MAC_{KIWF} para el mensaje recibido basándose en la clave de acceso K_{IWF}. En resumen: MAC_{KIWF} (IMSI, ID, T, N_U, N_{KR}). Tal suma de control criptográfica se devuelve al repositorio de claves KR (etapa 310).

[0079] En una etapa posterior 312, el repositorio de claves KR envía a la función de interfuncionamiento IWF, a través de un canal seguro, el siguiente mensaje: IMSI, ID, T, N_U, N_{KR}, MAC_{KIWF} (IMSI, ID, T, N_U, N_{KR}).

[0080] La protección de las comunicaciones entre el repositorio de claves KR y la función de interfuncionamiento IWF puede realizarse a través de diferentes soluciones. Una lista no limitativa es: TLS/SSL, IPsec, SSH, enlace dedicado.

[0081] La función de interfuncionamiento IWF comprueba la suma de control criptográfica MAC_{KIWF} para determinar la validez accediendo a la base de datos IWF utilizando una clave de búsqueda primaria correspondiente a la IMSI proporcionada por el SIM.

[0082] Si la comprobación proporciona un resultado positivo, la función de interfuncionamiento IWF extrae del registro almacenado en la base de datos IWF la clave de acceso K_{IWF} y calcula la suma de control criptográfica MAC_{KIWF} basándose en los datos recibidos con el fin de comprobar la validez de los mismos con respecto a los proporcionados por el repositorio de claves KR.

[0083] En una etapa 314, el resultado de la comparación se devuelve al repositorio de claves KR, mientras que la operación se almacena en un archivo de registro correspondiente.

[0084] Evidentemente, un fallo en cualquiera de las comprobaciones mencionadas anteriormente hace que el procedimiento se interrumpa, enviándose una alerta correspondiente al usuario U.

[0085] En caso de que la autenticación sea satisfactoria, el repositorio de claves KR accede a su base de datos con una clave de búsqueda primaria correspondiente a la IMSI proporcionada por el SIM con el fin de recuperar la(s) clave(s) privada(s) K_{ID} solicitada(s) por el usuario U y presente(s) en la base de datos dentro del archivo cifrado. La(s) clave(s) privada(s) K_{ID} se envía(n) al usuario U.

[0086] El usuario U recibe el archivo cifrado y lo descifra dejando que el SIM reconstruya el valor de la clave de cifrado K basándose en la información contenida en la cabecera criptográfica CH.

[0087] Específicamente, en el diagrama de flujo de la figura 7, las etapas 400 y 402 representan etapas de acceso esencialmente idénticas a las etapas designadas como 100 y 102 en la figura 2.

[0088] En una etapa 404, el módulo de procesamiento ubicado en el terminal de usuario TU lee el contenido de los campos RAND1 y RAND2 de la cabecera criptográfica CH que representan los dos valores aleatorios RAND1

y RAND2, respectivamente. Los valores aleatorios RAND1 y RAND2 se transfieren al SIM.

[0089] En una etapa 406, el SIM calcula las dos claves de sesión Kc1 = A8 (RAND1) y Kc2 = A8 (RAND2). Las dos claves de sesión Kc1 y Kc2 se envían después al módulo de procesamiento.

[0090] En una etapa 408, el módulo de procesamiento reconstruye la clave de cifrado K calculando la función *hash* h aplicada a la concatenación de las dos claves de sesión Kc1 y Kc2. En resumen: K=h(Kc1, Kc2). También es posible utilizar técnicas de construcción alternativas para la clave de cifrado K consideradas anteriormente, por lo que la clave de cifrado K puede expresarse generalmente como $K=f(K_U, Kc1, Kc2,\ldots, Kcn, SRES1, SRES2,\ldots, SRESn)$.

[0091] En una etapa 410, el módulo de procesamiento accede al archivo cifrado y vuelve a calcular la suma de control criptográfica MAC_K en función de la clave de cifrado K que acaba de (re)construirse, el contenido del archivo cifrado y los campos RAND1, RAND2, IV y versión contenidos en la cabecera criptográfica CH. Este valor se compara después con el valor de la suma de control criptográfica MAC_K presente en la cabecera criptográfica CH.

[0092] En el caso de un resultado positivo, el módulo de procesamiento lee de la cabecera criptográfica CH el campo IV (etapa 412) y en la etapa 414 descifra el archivo cifrado a través de, por ejemplo, el algoritmo AES en un modo CBC con el vector aleatorio IV seleccionado y la clave de cifrado K reconstruida por el SIM.

[0093] La(s) clave(s) privada(s) K_{ID} del usuario U está(n) ahora en forma de texto plano y puede(n) usarse en cualquier módulo de software compatible presente en el terminal de usuario TU.

[0094] Tal y como se ha indicado anteriormente, la disposición descrita en este documento también puede funcionar sin proporcionarse la función de interfuncionamiento IWF. En ese caso, el procedimiento de registro de usuario se modifica con el fin de definir un procedimiento de autenticación para el repositorio de claves KR y el usuario U.

[0095] El procedimiento para acceder al archivo cifrado que contiene las claves privadas finaliza directamente en el repositorio de claves KR.

[0096] Específicamente, el repositorio de claves KR autenticará al usuario U de manera tradicional, por ejemplo, recurriendo a una disposición de nombre de usuario/contraseña compartida durante el procedimiento de registro de usuario. En este punto, dependiendo del resultado de la fase de autenticación durante la solicitud, el repositorio de claves KR decidirá si el archivo cifrado que contiene la clave privada va a enviarse al usuario U.

[0097] En este caso, el nivel de seguridad del proceso de autenticación es menor. Sin embargo, el nivel de seguridad general se mantiene esencialmente ya que el archivo cifrado, una vez enviado y recibido por el usuario U, solo puede descifrarse a través del SIM que lo protegió.

[0098] Evidentemente, el repositorio de claves KR puede autenticar al usuario U recurriendo a otros mecanismos tales como: contraseñas de un solo uso, sistemas biométricos, autenticación basada en SIM, siendo ésta una lista no limitativa.

[0099] El repositorio de claves KR también puede configurarse para conectarse a la función de interfuncionamiento IWF con el solo objetivo de comprobar el estado del SIM correspondiente a la IMSI recibida. Dicho de otro modo, el repositorio de claves KR puede solicitar simplemente a la función de interfuncionamiento IWF una indicación de si el SIM asociado con la IMSI recibida es todavía válido y está activo, o si ha sido revocado por el operador móvil o por el usuario U (por ejemplo, debido a que se haya perdido, haya sido robada, esté estropeada, etc.).

[0100] La disposición descrita en este documento permite la recuperación de claves privadas por parte del usuario U incluso cuando el SIM respectivo no está disponible. En este último caso, será posible iniciar un procedimiento que permita al usuario U, una vez se conozca la cabecera criptográfica del archivo cifrado que contiene la(s) clave(s) privada(s)/elementos de información, reconstruir la clave de cifrado K.

[0101] Esto puede ocurrir, por ejemplo, comunicando de manera segura al operador de la red móvil la cabecera criptográfica asociada al archivo cifrado o simplemente los dos desafíos de autenticación (valores aleatorios) RAND1 y RAND2, obteniendo al mismo tiempo la respuesta de autenticación correspondiente SRES1 y SRES2 y las dos claves de sesión Kc1, Kc2.

[0102] Empezando por estos parámetros, junto con el vector aleatorio IV, la cadena de caracteres ‘versión’ y

la clave secreta posiblemente personalizada K_U, el usuario U estará en posición de reconstruir la clave de cifrado K y, por tanto, de descifrar sus claves privadas que pueden estar protegidas por un nuevo SIM.

[0103] Los expertos en la técnica apreciarán fácilmente que la disposición descrita en este documento puede adaptarse para proteger cualquier información confidencial para el usuario U. De hecho, la disposición descrita en este documento no permite al repositorio de claves KR acceder a los contenidos de texto plano de los archivos de usuario. Esto hace que el sistema sea más seguro y esté mejor adaptado para proteger cualquier tipo de archivo o información digital.

[0104] Tal y como se ha indicado, la disposición descrita en este documento está adaptada para funcionar también con relación a otra clase de tarjeta de tipo SIM tal como SIM de UMTS, denominadas actualmente como USIM. Las USIM contienen funciones de seguridad que son análogas a las funciones de seguridad de los sistemas GSM: están basadas en uno o más desafíos de autenticación RAND que permiten la generación de claves criptográficas que se utilizarán como se ha descrito anteriormente.

[0105] Además, en el caso de UMTS, un único desafío de autenticación RAND está adaptado para generar varias claves (CK, IK, etc.) haciendo por tanto posible utilizar un único desafío aleatorio RAND para generar claves criptográficas que se utilizarán en la protección de claves privadas de los usuarios.

[0106] Además, debe apreciarse que, tal y como se utiliza en este documento, la conversión de “procesamientos de cifrado” entre un elemento de información privado y un archivo correspondiente cifrado a través de al menos una clave de cifrado se aplica al cifrado del elemento de información privado, para generar un archivo cifrado correspondiente, o a la recuperación del elemento de información privado descifrando el archivo cifrado correspondiente, o incluso a la combinación del cifrado y descifrado anteriores.

[0107] Por lo tanto, sin prejuicio del principio subyacente de la invención, los detalles y las realizaciones pueden variar, también de manera significativa, con respecto a lo que se ha descrito a modo de ejemplo, sin apartarse del alcance de la invención definida en las siguientes reivindicaciones.

REIVINDICACIONES

1. Un procedimiento para almacenar de manera segura al menos un elemento de información privado de un usuario, que incluye las etapas de:

- asignar a dicho usuario un módulo de identidad de abonado respectivo, SIM, almacenando dicho módulo de identidad de abonado, SIM, al menos un algoritmo de seguridad;
- producir al menos una clave de cifrado a través de dicho al menos un algoritmo de seguridad; y
- proporcionar una ubicación de almacenamiento remota, KR, a la que puede acceder dicho usuario a través de una red de comunicaciones, TU, IWF, donde dicho elemento de información privado del usuario está almacenado como un archivo cifrado a través de dicha al menos una clave de cifrado.

2. El procedimiento según la reivindicación 1, **caracterizado porque** incluye las etapas de:

- recibir una solicitud de usuario (402) para dicho elemento de información privado del usuario a través de dicha red de comunicaciones, TU, IWF;
- enviar a través de dicha red de comunicaciones, TU, KR, dicho elemento de información privado solicitado del usuario a dicho usuario solicitante como dicho archivo cifrado; y
- descifrar dicho archivo cifrado en dicho usuario solicitante, TU, mediante dicha al menos una clave de cifrado para recuperar dicho elemento de información privado solicitado del usuario.

3. El procedimiento según cualquiera de las reivindicaciones 1 ó 2, **caracterizado porque** la etapa de producir al menos una clave de cifrado a través de dicho al menos un algoritmo de seguridad incluye las etapas de:

- generar al menos un valor aleatorio, RAND1, RAND2;
- someter dicho al menos un valor aleatorio, RAND1, RAND2, a dicho al menos un algoritmo de seguridad para generar al menos dos claves de sesión, Kc1, Kc2; y
- mezclar dichas al menos dos claves de sesión Kc1, Kc2, a través de una función de mezcla, h, para producir dicha al menos una clave de cifrado.

4. El procedimiento según la reivindicación 3, **caracterizado porque** dicha función de mezcla es una función *hash,* h.

5. El procedimiento según la reivindicación 4, **caracterizado porque** comprende la etapa de incluir en dicha función de mezcla, h, un secreto específico del usuario, por lo que dicha al menos una clave de cifrado no puede predecirse incluso conociendo cualquiera de las claves almacenadas en dicho módulo de identidad de abonado, SIM.

6. El procedimiento según cualquiera de las reivindicaciones 1 a 5, **caracterizado porque** incluye la etapa de incluir en dicho archivo cifrado una cabecera criptográfica, CH, comprendiendo dicha cabecera criptográfica, CH, una suma de control criptográfica, MAC_K, utilizada para detectar cualquier modificación no autorizada de dicho archivo cifrado.

7. El procedimiento según cualquiera de las reivindicaciones 2 a 6, **caracterizado porque** incluye la etapa de aceptar dicha solicitud de usuario (402) supeditada a dicha autenticación del usuario solicitante con dicha ubicación de almacenamiento remota, KR.

8. El procedimiento según la reivindicación 7, **caracterizado porque** la etapa de aceptar dicha solicitud de usuario supeditada a dicha autenticación del usuario solicitante con dicha ubicación de almacenamiento remota incluye la etapa de autenticar dicho usuario solicitante con dicha ubicación de almacenamiento remota, KR, mediante al menos uno de los siguientes elementos de identidad: nombre de usuario, contraseña, contraseña de un solo uso, sistemas biométricos, autenticación basada en SIM.

9. El procedimiento según la reivindicación 7, **caracterizado porque** la etapa de aceptar dicha solicitud de usuario supeditada a dicha autenticación del usuario solicitante con dicha ubicación de almacenamiento remota incluye la etapa de autenticar dicho usuario solicitante con dicha ubicación de almacenamiento remota mediante al menos una función de interfuncionamiento, IWF.

10. El procedimiento según la reivindicación 9, **caracterizado porque** la etapa de autenticar dicho usuario solicitante con dicha ubicación de almacenamiento remota mediante al menos una función de interfuncionamiento incluye las etapas de:

- interconectar dicho módulo de identidad de abonado, SIM, con dicha función de interfuncionamiento, IWF;
- comprobar si dicho módulo de identidad de abonado, SIM, está incluido en una lista de módulos de identidad de abonado en el marco de dicha red de comunicaciones, TU, KR, IWF;
- si dicho módulo de identidad de abonado, SIM, está habilitado, hacer que dicha función de interfuncionamiento, IWF, genere al menos una clave de acceso, K_{IWF}, utilizándose dicha al menos una clave de acceso, K_{IWF}, para acceder a dicho al menos un elemento privado almacenado como un archivo cifrado en dicha ubicación de almacenamiento remota, KR.

11. El procedimiento según la reivindicación 10, **caracterizado porque** dicha etapa de hacer que dicha función de interfuncionamiento, IWF, genere al menos una clave de acceso incluye las etapas de:

- generar al menos un número aleatorio, RAND1, RAND2;
- enviar dicho al menos un número aleatorio, RAND1, RAND2, en forma de un desafío de autenticación;
- supervisar al menos una respuesta correspondiente a dicho desafío de autenticación, RAND1, RAND2;
- determinar una autenticación satisfactoria de dicho usuario en función de dicha al menos una respuesta; y
- generar al menos dicha clave de acceso, K_{IWF}, en función de al menos una entidad seleccionada a partir de un grupo que comprende:
  - dicho al menos un número aleatorio, RAND1, RAND2; y
  - dicha al menos una respuesta correspondiente;

12. Un sistema para almacenar de manera segura al menos un elemento de información privado de un usuario, que incluye:

- un módulo de identidad de abonado, SIM, almacenando dicho módulo de identidad de abonado, SIM, al menos un algoritmo de seguridad;
- un terminal de usuario, TU, que comprende un módulo de procesamiento, pudiendo conectarse dicho módulo de procesamiento a dicho módulo de identidad de abonado, SIM, para producir una clave de cifrado a través de dicho al menos un algoritmo de seguridad, utilizándose dicha clave de cifrado para cifrar dicho elemento de información privado del usuario; y
- una ubicación de almacenamiento remota, KR, a la que puede acceder dicho usuario a través de una red de comunicaciones, estando configurada dicha ubicación de almacenamiento remota, KR, para almacenar dicho elemento de información privado del usuario como un archivo cifrado a través de dicha clave de cifrado.

13. El sistema según la reivindicación 12, **caracterizado porque** dicho terminal de usuario, TU, incluye un ordenador personal, un ordenador de tamaño agenda, un ordenador portátil, un PDA o un teléfono inteligente.

14. El sistema según cualquiera de las reivindicaciones 12 ó 13, **caracterizado porque** dicho terminal de usuario está conectado a dicho módulo de identidad de abonado, SIM, por medio de un lector de tarjetas inteligentes, un terminal móvil con *Bluetooth*, un terminal móvil con IrDA o un terminal móvil a través de un cable.

15. Una red de comunicaciones, que incluye un sistema según cualquiera de las reivindicaciones 12 a 14.

16. Un producto de programa informático que puede cargarse en la memoria de al menos un ordenador y que comprende partes de código software para llevar a cabo el procedimiento según cualquiera de las reivindicaciones 1 a 11 cuando se ejecuta por el al menos un ordenador.

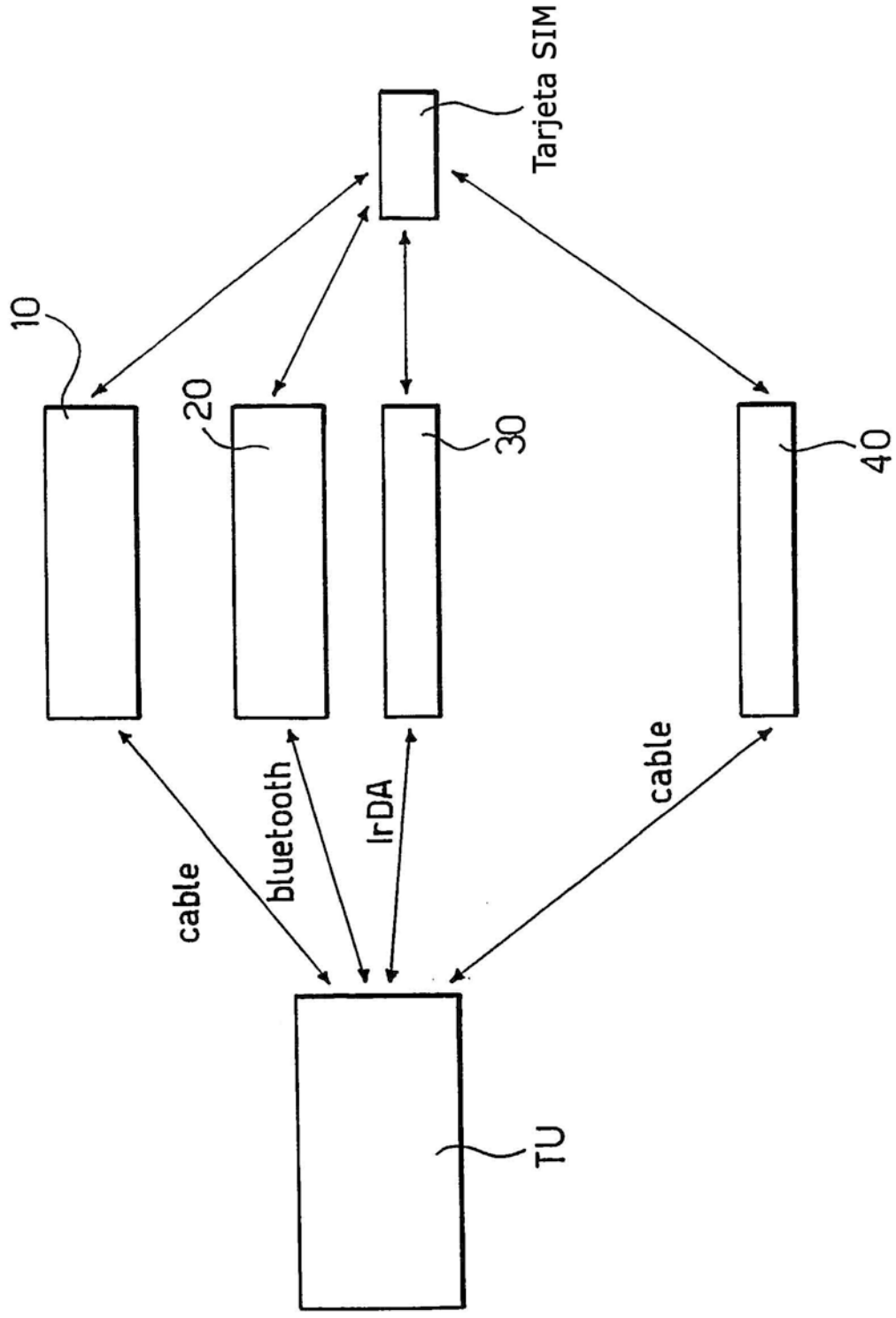

Fig. 1

Fig. 2

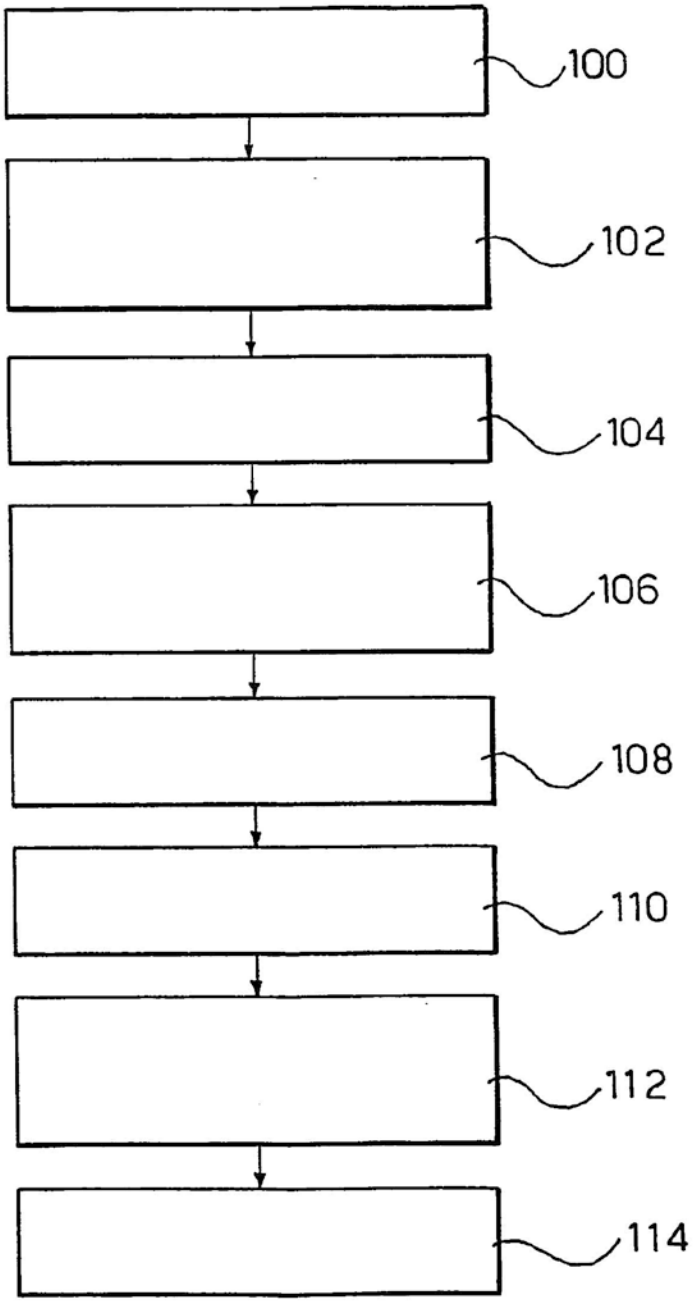

Fig. 3

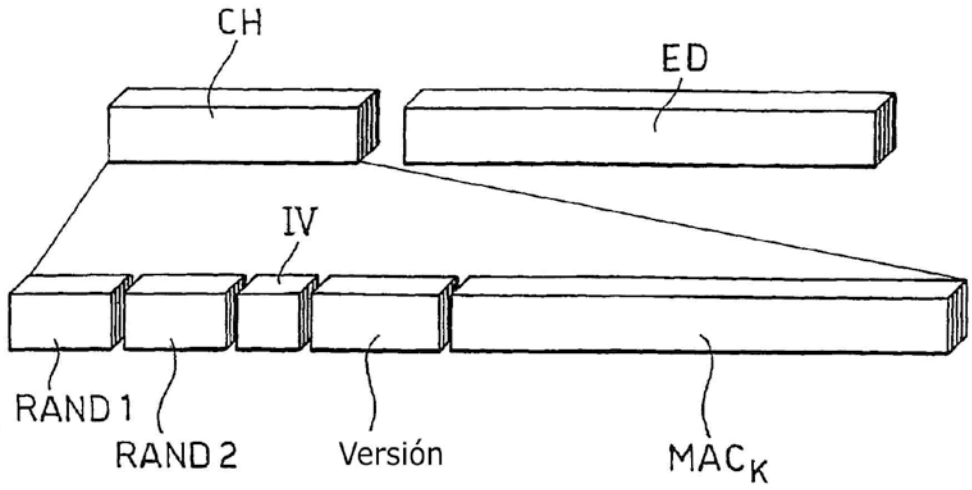
CH
ED
IV
RAND 1
RAND 2
Versión
MAC$_K$

Fig. 4

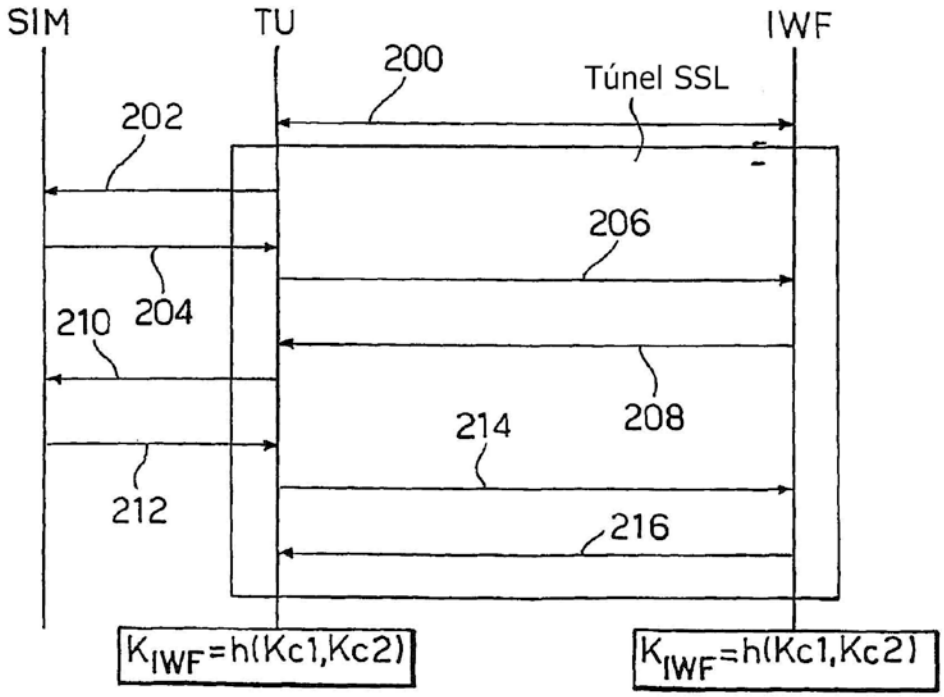
SIM
TU
IWF
200
Túnel SSL
202
206
204
210
208
214
212
216
K_{IWF}=h(Kc1,Kc2)
K_{IWF}=h(Kc1,Kc2)

Fig. 5

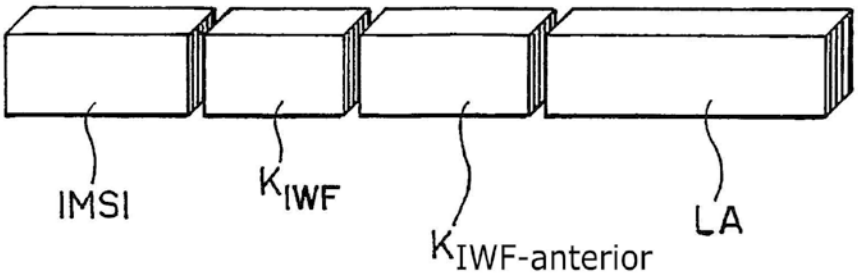
IMSI
K_{IWF}
$K_{IWF\text{-}anterior}$
LA

Fig. 6

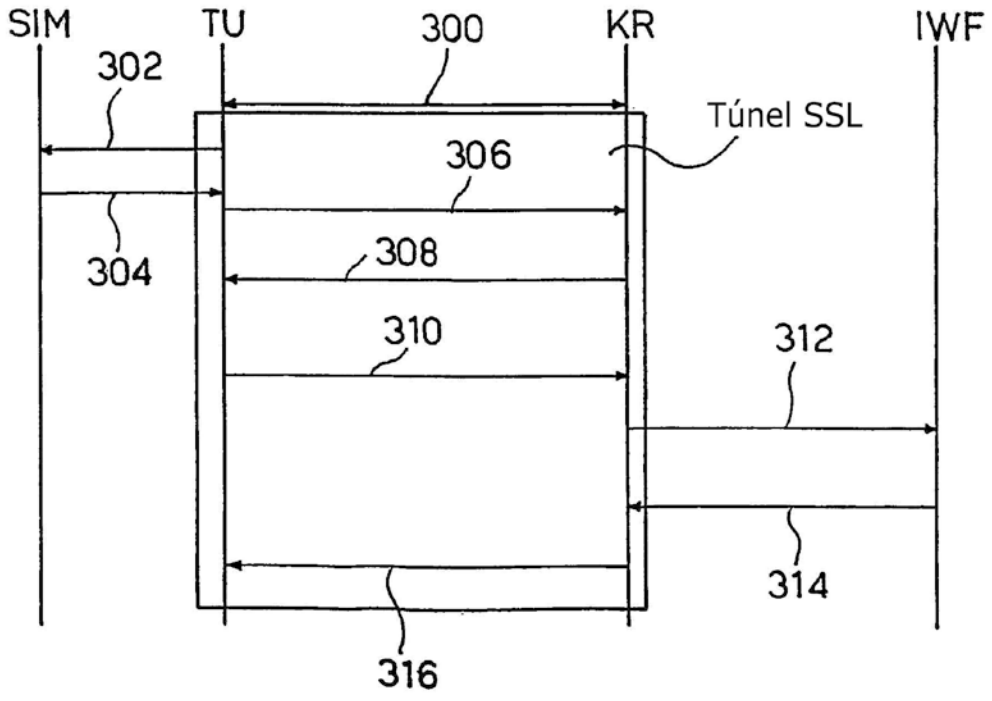
SIM
TU
300
KR
IWF
302
Túnel SSL
306
304
308
310
312
314
316

Fig. 7