(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 369 848**

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **03292822 .8**
(96) Fecha de presentación: **14.11.2003**
(97) Número de publicación de la solicitud: **1427231**
(97) Fecha de publicación de la solicitud: **09.06.2004**

(54) Título: **PROCEDIMIENTO DE ESTABLECIMIENTO Y DE GESTIÓN DE UN MODELO DE CONFIANZA ENTRE UNA TARJETA INTELIGENTE Y UN TERMINAL RADIO.**

(30) Prioridad:
22.11.2002 FR 0214669

(45) Fecha de publicación de la mención BOPI:
07.12.2011

(45) Fecha de la publicación del folleto de la patente:
07.12.2011

(73) Titular/es:
SOCIÉTÉ FRANÇAISE DU RADIOTÉLÉPHONE-SFR
42, AVENUE DE FRIEDLAND
75008 PARIS, FR

(72) Inventor/es:
Bensimon, Michael;
Caloud, Philippe;
Pothin, Cédric y
Prunel, Nicolas

(74) Agente: **de Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Procedimiento de establecimiento y de gestión de un modelo de confianza entre una tarjeta inteligente y un terminal radio.

La presente invención concierne al ámbito de la radiotelefonía móvil. Más en particular, la presente invención concierne a un procedimiento que permite establecer una relación de confianza entre un terminal de radiocomunicación y una tarjeta inteligente de tipo SIM o equivalente, con el fin de garantizar la seguridad de los intercambios entre tarjeta y terminal.

En lo que sigue, por terminal se entenderá cualquier equipo emisor-receptor portátil, móvil, susceptible de funcionar en una red de radiotelefonía móvil tal como GSM, GPRS, UMTS y cualquier tipo de red análoga, por ejemplo WLAN. La invención está destinada a los teléfonos móviles dotados de una tarjeta inteligente, por ejemplo una tarjeta de tipo SIM, y se refiere en particular a la distribución de contenidos seguros para los teléfonos móviles.

En la técnica anterior, el problema del refuerzo de la seguridad en los intercambios y en las infraestructuras de tratamiento de la información ha sido abordado desde hace mucho tiempo. Hasta la fecha, se han propuesto numerosas soluciones, que se fundamentan en conocidas tecnologías de criptografía. La infraestructura de gestión de claves públicas en especial (PKI por "Public Key Infrastructure") es la solución que se fundamenta en tecnologías de claves asimétricas (pública Kp, privada Ks), que es la más desarrollada. Una clave pública Kp corresponde a una sucesión de cifras utilizada para cifrar o descifrar un mensaje transmitido entre un emisor y un receptor y asociado a una clave secreta aparejada, también denominada clave privada Ks. El mensaje puede ser así cifrado mediante una clave pública, conocida por un conjunto de usuarios, y descifrado mediante una clave secreta solo conocida por el receptor o, a la inversa, cifrado mediante una clave privada Ks y descifrado mediante la clave pública. Mientras que el cifrado mediante clave pública Kp asegura la confidencialidad del mensaje, el cifrado mediante clave privada Ks asegura su integridad.

Esta solución de hecho se fundamenta en la idea de que la inicialización de un intercambio seguro o de un acceso a un contenido seguro se fundamenta en la utilización de claves de encriptación públicas Kp, que garantizan que solamente el poseedor de la clave privada Ks asociada podrá desencriptar el mensaje, y de certificados que asocian de manera segura la identidad del asociado con la clave pública Kp, por estar certificada (encriptada mediante clave privada Ks) por una autoridad de certificación AUC (sigla para "Authentification Centre").

Según es sabido, el centro de autenticación AUC es el encargado de la autenticación de los abonados y participa en la confidencialidad de los datos que transitan por la interfaz radio entre el terminal móvil y la estación base a la que se halla vinculado en un momento dado.

No obstante, la referida solución no es completamente segura. Así, la inicialización del procedimiento de autenticación es un punto débil ya que hay muchas autoridades de certificación cuyas políticas de certificación no tienen en absoluto el mismo grado de seguridad. El usuario medio no está informado de ello y no sabe que, por ejemplo, puede ser muy arriesgado aceptar certificados validados por ciertas autoridades.

El artículo redactado por Chang-Seop Park y titulado «On Certificate-Based Security Protocols for Wireless Mobile Communication Systems» propone un ejemplo de protocolo de intercambio de clave autenticada de sesión que se basa en un certificado cuya validez está limitada en el tiempo. Este protocolo está basado en conocidos sistemas de encriptación con claves públicas, como por ejemplo las raíces cuadradas modulares o los sistemas implantados por Rivest, Shamir y Adleman. Los certificados basados en estos sistemas permiten por una parte un funcionamiento en teléfonos móviles cuyas capacidades informáticas son limitadas y, por otra parte, obviar el contacto con un elemento de la red mientras el certificado aún es válido. Esta solución presenta sin embargo el inconveniente de funcionar tan sólo en el período de validez del certificado.

Por otro lado, resulta problemático el almacenamiento de las claves privadas Ks, sobre todo en el caso en que puede interesar al usuario conocer esa clave para tener acceso a contenido protegido. La protección de contenido contra el pirateo tiene que estar adaptada en efecto en caso de que "el atacante" no es exterior, sino que típicamente es el propio usuario. Las soluciones existentes no toman en cuenta esta posibilidad.

Se prevé en la técnica anterior, a causa de las fallas de seguridad, una política de revocación de terminales móviles, pero, en la práctica, ésta es difícil de poner en práctica.

Se conoce asimismo en la técnica anterior el acceso a contenido protegido mediante derechos de acceso, por ejemplo con tecnologías de tipo DRM ("Digital Rights Management"). El principio general del DRM consiste en proporcionar al usuario un contenido encriptado así como una licencia de utilización. Esta licencia incorpora los derechos de uso así como una clave asociada que permite desencriptar el contenido. Con objeto de que esta clave asociada, generalmente simétrica, no sea accesible para el usuario, bien se envía la licencia mediante un canal que permite «impedir» al usuario leer la clave asociada así como transmitir la licencia, o bien se encripta la clave asociada. Las soluciones DRM actualmente propuestas se fundamentan en el uso de una clave simétrica o de una biclave asimétrica que se encuentra preinstalada en el terminal. Esta otra clave permite encriptar dicha clave

asociada a la licencia o generar una o varias claves, llamadas diversificadas, para la encriptación de la clave asociada a la licencia. En el terminal se implantan unos mecanismos para asegurar que dicha clave de desencriptación de la licencia, al igual que la clave contenida en la propia licencia, puedan ser conocidas por el terminal pero no por el usuario.

En las actuales soluciones de protección de un contenido, el código IMEI de identidad propio del terminal móvil ("International Mobile Equipement Identity") sirve para el establecimiento de un modelo de confianza entre, por una parte, la tarjeta SIM o USIM (para las redes llamadas de tercera generación) y, por otra parte, el terminal móvil. Teóricamente, el terminal móvil posee un código IMEI único y la mayoría de los procedimientos contemplados consisten en indicar a la tarjeta SIM un código IMEI con el que la tarjeta (U)SIM puede tener una relación de confianza.

Un inconveniente principal de estos procedimientos está en que el código IMEI no es un número secreto. Es sencillo, desde por ejemplo un PC con un lector de tarjeta inteligente, remitir el código IMEI de confianza a la tarjeta (U)SIM y, por lo tanto, establecer un modelo de confianza entre un PC y una tarjeta (U)SIM. Además, en muchos teléfonos móviles actuales, el código IMEI se modifica fácilmente. Así, cabe también la posibilidad de modificar el IMEI de un terminal móvil que, *a priori*, no es de confianza, para sustituirlo por el valor de un IMEI de confianza.

Consiguientemente, los derechos de uso de un contenido seguro se hallan de este modo asociados a un terminal móvil y no a un individuo. Con objeto de poder asociar los derechos de uso a un usuario, existe en consecuencia una necesidad de aprehender mejor el refuerzo de la seguridad entre la tarjeta SIM y el terminal por cuanto que el terminal no está protegido contra las manipulaciones y por cuanto que este último no puede ser autenticado mediante la tarjeta (U)SIM u otros medios difíciles de falsear.

Además, en las tecnologías de tipo DRM, si una clave como es dicha biclave es repudiada o expira, entonces ya no se podrá utilizar el terminal, al no haber previsto ningún mecanismo de reinicialización. Por otro lado, un eventual repudio de la biclave precisa de una muy hipotética detección de contenido protegido que le habría sido proporcionado al terminal y que habría sido hallado no protegido, por ejemplo en Internet.

Es por lo tanto un objeto de la presente invención establecer y gestionar un modelo de confianza entre un terminal de radiocomunicación y una tarjeta inteligente de tipo SIM o equivalente.

La presente invención tiene por objeto eliminar uno o varios de los inconvenientes de la técnica anterior definiendo un procedimiento que permite garantizar la seguridad de los intercambios entre una tarjeta SIM y un terminal, en el que el operador de una red de radiotelefonía móvil pasa a sustituir a las autoridades de certificación, permitiendo este procedimiento establecer una relación segura y revocable entre la tarjeta SIM o USIM y un terminal autenticado funcionalmente por la red, permitiendo asimismo este procedimiento, para las tecnologías de tipo DRM, almacenar dicha biclave de manera segura en la tarjeta SIM o USIM.

A tal efecto, la invención concierne a un procedimiento de establecimiento y de gestión de un modelo de confianza entre un módulo de identidad y un terminal radio, caracterizado por que incluye:

- una etapa de autenticación del terminal por dicho módulo de identidad, realizándose dicha etapa de autenticación por mediación de medios de autenticación proporcionados ya sea a dicho módulo de identidad por una red de radiotelefonía móvil en una etapa llamada de inicialización o análoga o en una etapa llamada de actualización, ya sea a dicho terminal por el módulo de identidad,

- una etapa de control por dicho módulo de al menos una característica específica del terminal, siendo previamente transmitida dicha característica específica a dicho módulo por radiotelefonía, desde un servidor seguro de dicha red de radiotelefonía móvil.

De acuerdo con otra particularidad de la invención, la vida útil de dichos medios de autenticación del terminal presentes en el módulo de identidad queda limitada por un plazo determinado, constituyéndose dichos medios de autenticación mediante al menos una clave de autenticación.

De acuerdo con otra particularidad de la invención, dicho módulo de identidad es una tarjeta inteligente de tipo SIM o una tarjeta USIM, para redes de tercera generación, o una tarjeta equivalente que incluye en una memoria datos representativos de abono.

De acuerdo con otra particularidad de la invención, el módulo de identidad mantiene una relación de confianza con el terminal radio generando unos medios de autenticación y proporcionando seguidamente estos medios de autenticación al terminal radio en virtud de mecanismos de intercambio seguros y que se fundamentan en medios de autenticación inicialmente disponibles del terminal radio.

La invención permite, por lo tanto, una provisión de funciones de seguridad y de almacenamiento seguro de datos en una tarjeta SIM o USIM y el establecimiento de un modelo de confianza entre el terminal y esa tarjeta. Los diferentes agentes del mundo de las telecomunicaciones tienden cada vez más a primar la relación entre un terminal móvil y la tarjeta (U)SIM para que esta última le proporcione funciones de seguridad. Estas funciones pueden ser funciones de

criptografía, de monedero electrónico como también funciones de almacenamiento y de acceso a datos.

De acuerdo con otra particularidad, el procedimiento según la invención incluye, en dicha etapa de inicialización o de actualización, una etapa de generación, realizada al menos por dicho módulo de identidad, de una clave llamada de confianza, siendo utilizada dicha clave de confianza por dicho módulo para encriptar al menos unos datos intercambiados entre el módulo de identidad y el terminal.

De acuerdo con otra particularidad de la invención, dicha etapa de inicialización de dichos medios de autenticación es efectuada, por iniciativa de la red de radiotelefonía, después de un repudio de clave iniciado por dicho módulo o la red de radiotelefonía móvil o el terminal radio, una expiración de la vigencia de clave o bien en la inicialización del módulo de identidad.

De acuerdo con otra particularidad, dicha etapa de autenticación comprende en particular las siguientes etapas:

- una etapa de utilización en el terminal de al menos una primera clave de autenticación memorizada en el terminal mediante al menos un primer algoritmo de autenticación memorizado en el terminal, teniendo dicha primera clave una vigencia limitada por un plazo determinado,

- una etapa de utilización por parte del módulo de identidad de al menos una segunda clave memorizada en el módulo de identidad mediante al menos un segundo algoritmo de autenticación memorizado en el módulo de identidad, siendo dicha segunda clave idéntica o complementaria de la primera clave y asociada al terminal, teniendo dicha segunda clave una vigencia limitada por dicho plazo determinado,

- una etapa de comparación en el módulo de identidad de los resultados obtenidos por dichos algoritmos primero y segundo.

De acuerdo con otra particularidad, la etapa de autenticación comprende la utilización de dicho plazo determinado.

De acuerdo con otra particularidad, dicha etapa de inicialización es iniciada por una red de radiotelefonía móvil e incluye asimismo:

- la generación por parte del módulo de identidad de al menos una de dichas claves primera y segunda,

- una memorización en el módulo de identidad de dicha segunda clave,

- una transmisión al terminal, por el módulo de identidad, de dicha primera clave, siendo encriptada esta primera clave por mediación de la clave de confianza.

De acuerdo con otra particularidad, dicha etapa de comparación se efectúa entre, por una parte, una respuesta producida por dicho primer algoritmo, memorizada en el terminal y transmitida a dicho módulo de identidad y, por otra parte, un resultado de respuesta, memorizado en el módulo de identidad, producido por dicho segundo algoritmo.

De acuerdo con otra particularidad, dicha primera clave puede ser una clave privada Ks asimétrica, siendo dicha segunda clave una clave pública Kp complementaria de la primera clave.

De acuerdo con otra particularidad, dicha primera clave puede ser simétrica, siendo dicha segunda clave memorizada en el módulo de identidad idéntica a la primera, formando estas claves una sola clave simétrica de autenticación.

De acuerdo con otra particularidad, el procedimiento según la invención comprende una etapa de actualización de dichas claves primera y segunda, iniciada por el módulo de identidad antes de dicho plazo determinado, incluyendo dicha actualización las siguientes etapas:

- autenticación entre el terminal y el módulo de identidad con ayuda de dichas claves primera y segunda,

- generación mediante un algoritmo de puesta al día del módulo de identidad de al menos una clave puesta al día que toma en cuenta una información para sustituir al menos una de dichas claves primera y segunda,

- memorización en el módulo de identidad de la clave puesta al día para sustituir dicha segunda clave,

- transmisión al terminal, por el módulo de identidad, de la clave puesta al día análoga a dicha primera clave.

De acuerdo con otra particularidad, dicha actualización comprende además el control de al menos un identificador del terminal y/o del módulo de identidad.

De acuerdo con otra particularidad, se realiza una encriptación de clave para dicha transmisión al terminal de la clave puesta al día análoga a la primera clave, efectuándose dicha encriptación de clave mediante dicha clave de confianza.

De acuerdo con otra particularidad, la actualización comprende asimismo las siguientes etapas:

- generación por parte del módulo de identidad de una nueva clave de confianza, después de dicha autenticación entre terminal y módulo,

- memorización en el módulo de identidad de la nueva clave de confianza,

- transmisión al terminal, por el módulo de identidad, de la clave de confianza recién generada.

De acuerdo con otra particularidad, dicha actualización termina con una prueba de verificación que comprende una transmisión de vuelta por parte del terminal de al menos un dato representativo de la correcta recepción de la información transmitida por el módulo de identidad en la actualización.

De acuerdo con otra particularidad, dicha clave de confianza es una clave de cifrado/descifrado simétrica análoga o idéntica a dicha clave simétrica de autenticación.

De acuerdo con otra particularidad, dicha clave de confianza es una clave de sesión borrable.

De acuerdo con otra particularidad, se realiza una etapa llamada de revocación por iniciativa del módulo de identidad, del terminal o de la pertinente red de radiotelefonía, comprendiendo dicha etapa de revocación el borrado, en una memoria de dicho módulo de identidad, de al menos dicha primera clave asociada al terminal.

Es otro objeto de la invención aportar una solución a uno o varios de los problemas con los que se ha enfrentado la técnica anterior definiendo un módulo de identidad para la puesta en práctica del procedimiento según la invención.

Este objeto se logra mediante un módulo de identidad en un terminal para la puesta en práctica del procedimiento según la invención, caracterizado por que comprende medios para memorizar al menos una clave de autenticación así como al menos un algoritmo de autenticación, medios de cálculo para ejecutar al menos una etapa consistente en aplicar dicha clave de autenticación a dicho algoritmo de autenticación memorizado en el módulo de identidad, medios de comunicación, medios para iniciar una revocación y medios de revocación para revocar dicha clave de autenticación, medios de memorización de una característica específica del terminal y medios de activación de un algoritmo de puesta al día de dicha clave de autenticación, siendo aptos los medios de comunicación para proporcionar al terminal al menos una clave de autenticación y para recibir datos procedentes de un servidor seguro de una red de radiotelefonía móvil.

La invención, con sus características y ventajas, se desprenderá más claramente con la lectura de la descripción hecha con referencia a los dibujos que se acompañan, dados a título de ejemplos no limitativos, en los que:

La figura 1 representa esquemáticamente el proceso de inicialización puesto en práctica en la invención,

la figura 2 representa de una manera esquemática una autenticación del terminal frente al módulo de identidad en el procedimiento según la invención,

la figura 3 representa un ejemplo de proceso puesto en práctica en la invención para la actualización de una clave compartida por el terminal y el módulo de identidad,

la figura 4 representa esquemáticamente el principio de funcionamiento del que hacen uso las tecnologías de tipo DRM en la técnica anterior, y

la figura 5 representa un ejemplo de problemática con la que se enfrenta la técnica anterior en un caso DRM cuando no existe modelo de confianza entre el terminal y la tarjeta SIM.

De manera específica, en el ámbito de la telefonía móvil intervienen tres elementos. Un primer elemento, el terminal (MS), realiza funciones de acceso, de almacenamiento y comunicación de una información segura. Un segundo elemento, el módulo de identidad (SIM), permite identificar al usuario y permite almacenar datos confidenciales. Un tercer elemento por último, la red, puede comunicarse a través del terminal (MS) de manera segura con el módulo de identidad (SIM). En una forma de realización de la invención, el módulo de identidad (SIM) es una tarjeta inteligente, por ejemplo de tipo SIM, USIM, para redes de tercera generación, o de tipo equivalente, que incluye, en una memoria, datos representativos de abono, un microprocesador y un programa de funcionamiento que realiza las funciones que se relatan a continuación.

El módulo de identidad (SIM) puede incluir medios de comunicación que le permiten comunicarse a un tiempo con el terminal y con un servidor seguro (SS) de la red. En unas variantes, el terminal (MS) utilizado puede estar construido para comportarse de manera transparente cuando recepta un mensaje específico del tipo paquete de mando seguro, enviado desde el servidor seguro (SS) con destino al módulo de identidad (SIM). Por ejemplo, el servidor seguro (SS) puede enviar un SMS con una dirección que especifica como destino el módulo (SIM), por mediación de medios de puntero. Puede estar previsto un campo de destino para distinguir si el mensaje lo tiene que receptar el terminal (MS) o el módulo (SIM).

La figura 4 ilustra un ejemplo de principio actualmente utilizado para las tecnologías de tipo DRM ("Digital Rights Management"). El acceso a un contenido seguro queda sometido, en primer lugar, a la expresión de derechos de uso definidos por los titulares del derecho y, en segundo lugar, a la obtención de la clave de desencriptación del contenido. Como se representa en la figura 4, un contenido encriptado es distribuido en primera instancia, a través de una operación de descarga (E1) entre un servidor de contenido (S) y el terminal móvil (MS). Luego, en segunda instancia, se envía (E2) al terminal (MS) una licencia asociada necesaria para poder utilizar el contenido, con una regla llamada de "forward lock", a través de un centro MMS-C ("Multimedia Messaging Services Center"). La licencia contiene derechos de uso y la clave simétrica de desencriptación del contenido. Según las tecnologías y los estándares, esta licencia puede ser expedida al terminal con o separadamente del contenido. Hasta la fecha, en el mundo de la telefonía móvil, aún son débiles los medios de autenticación del terminal (MS) e inexistentes las soluciones para proteger la licencia. Así, la clave de cifrado no está protegida y, entonces, los ataques al contenido se ven facilitados. Igualmente, uno de de los planteamientos del OM, ilustrado en la figura 4, consiste en proporcionar al terminal móvil (MS) la clave simétrica en claro con el envío de la licencia (E2). Este planteamiento es, por ejemplo, el del "WAP-DOWNLOAD", en el que el contenido es enviado por un primer canal y la licencia es proporcionada (E2) por otro canal, por ejemplo MMS, impidiendo teóricamente la transferencia de la clave hacia otros terminales. Este canal, en principio, permite «impedir» al usuario leer la clave así como transmitir la licencia. Este tipo de proceso presenta en particular los siguientes inconvenientes:

- la clave contenida en la licencia se almacena de manera permanente y en claro en el terminal (MS),
- la licencia está ligada al terminal (MS) y no al usuario,
- la protección se puede eludir fácilmente, por ejemplo con ayuda de un PC dotado de un módem GSM/GPRS.

Otro planteamiento consiste en proporcionar la clave simétrica encriptada en virtud de una clave previamente almacenada y no conocida por el usuario en el terminal móvil (MS). No obstante, en este segundo planteamiento, la licencia sigue estando vinculada al terminal (MS), que se puede piratear. Además, es casi imposible controlar la integridad de la clave y no se puede contemplar una revocación sin hacer inutilizable el terminal móvil (MS).

El procedimiento según la invención permite el refuerzo de la seguridad en los intercambios de datos entre un módulo de identidad (SIM) tal como, por ejemplo, una tarjeta SIM o USIM y un terminal (MS). Para ello, se realiza una etapa de autenticación del terminal mediante dicho módulo de identidad (SIM), en orden a verificar que el terminal (MS) utilizado es efectivamente un terminal de confianza. El terminal (MS) tiene que poder identificarse frente al módulo de identidad (SIM) con ayuda de una clave simétrica o asimétrica. Si se utiliza una clave simétrica, ésta tiene que almacenarse a la vez en una memoria del terminal y en una memoria del módulo de identidad (SIM). Si se utilizan claves asimétricas, es decir, al menos una clave pública Kp y al menos una clave privada asociada, en el terminal sólo tiene que almacenarse la clave privada Ks. La clave pública Kp se memoriza en una memoria del módulo de identidad (SIM). De acuerdo con una variante de realización con claves asimétricas, la autenticación entre módulo de identidad (SIM) y terminal (MS) se hace con ayuda de una clave pública Kp almacenada en una memoria del módulo de identidad (SIM) y de una clave privada Ks asociada almacenada en una memoria del terminal (MS). La clave pública asimétrica Kp y la clave privada asimétrica Ks son complementarias. Este mecanismo de autenticación también puede ser utilizado para la primera autenticación (23), efectuada en la inicialización. Como variante, para la primera autenticación, la clave pública Kp y la clave privada Ks son sustituidas por una clave simétrica.

En una forma de realización de la invención, las claves o unos medios de autenticación análogos se proporcionan al menos al módulo de identidad (SIM) mediante una transmisión por una red de radiotelefonía móvil en una etapa de inicialización o en una etapa de actualización. La transmisión de tales medios de autenticación se efectúa por iniciativa de la red, en unas condiciones de seguridad reforzada en las que los sistemas de comunicaciones son considerados sistemas de confianza, por ejemplo en comunicación con un servidor OTA ("Over The Air") seguro (SS). Tal como se ilustra en la figura 1, eventualmente se pueden transmitir (21) una o varias claves de autenticación al módulo de identidad (SIM) con motivo de una petición de inicialización (20) de clave por iniciativa del servidor OTA seguro (SS). Al menos una clave de autenticación puede corresponderse por ejemplo con una clave ya presente en el terminal (MS). Al menos una característica del terminal (MS), por ejemplo el código IMEI o también la velocidad máxima de transmisión teórica desde el terminal es transmitida (22) asimismo al módulo de identidad (SIM) por el servidor OTA (SS). Por mediación de la clave de autenticación del terminal (MS) se realiza una etapa (23) llamada de primera autenticación del terminal (MS) por el módulo de identidad (SIM). Esta primera etapa de autenticación (23) viene acompañada de un control (24) de característica(s) del terminal (MS), por ejemplo el código IMEI, efectuado por el módulo (SIM). Ello permite al módulo (SIM) asegurarse de que el terminal (MS) es un terminal de confianza. El módulo de identidad (SIM), en efecto, tan sólo debe proporcionar una clave de desencriptación o análoga a los terminales (MS) en los que tiene confianza. En otra variante de realización, la inicialización puede desarrollarse sin el uso de clave(s) de inicialización.

Para permitir esta transmisión de medios de autenticación, el módulo de identidad (SIM) tiene que ser de tipo "proactivo", es decir, equipado con medios para enviar comandos al terminal (MS) para que este último los ejecute.

En su defecto, se puede implantar un mecanismo de "pulling", es decir, el terminal (MS) va a consultar periódicamente al módulo de identidad (SIM) con el fin de asegurarse de que el módulo (SIM) no tiene nada que transmitirle.

A partir de un algoritmo de generación de clave del módulo (SIM), se genera (25) una clave de confianza, por ejemplo borrable y que funciona como una clave de sesión. Esta clave de confianza está destinada para el terminal (MS) y para el módulo de identidad (SIM) con el objetivo de encriptar los datos intercambiados entre el módulo de identidad (SIM) y el terminal (MS). Esta clave de confianza se memoriza a la vez en el módulo de identidad (SIM) y en el terminal (MS). Con motivo de las peticiones de actualización de la(s) clave(s), el módulo de identidad (SIM) genera al menos una nueva clave de autenticación para las próximas autenticaciones entre terminal (MS) y módulo de identidad (SIM). En el caso de una clave asimétrica, después de haber memorizado en una de sus memorias la clave pública Kp, el módulo de identidad (SIM) transmite (26) al terminal (MS) la clave privada Ks asociada. Esta transmisión (26) es segura por cuanto que la nueva clave privada Ks va encriptada con la clave de confianza. En una variante de realización, dicha clave de confianza puede ser una clave de cifrado/descifrado simétrica. Para el caso en que se genera una clave simétrica de autenticación, la clave de confianza puede ser, por ejemplo, análoga o idéntica a la clave simétrica que sirve para la autenticación. En una forma de realización de la invención, cuando el terminal (MS) se ha ajustado bien a un criterio de autenticación (23), de control (24) o a estos dos criterios (23, 24) y a continuación ha recibido bien en una memoria la o las clave(s) transmitida(s), éste puede remitir por ejemplo al módulo de identidad (SIM) un mensaje de confirmación (27). Seguidamente, de igual manera, el módulo de identidad (SIM) remite al servidor OTA (SS) de la red un mensaje de confirmación (28).

Así, tal como se ilustra en la figura 1, la red puede enviar un mensaje (20) al módulo de identidad (SIM) proporcionándole (21) una clave de inicialización, por ejemplo simétrica, que le permite autenticar al terminal (MS) y/o encriptar los intercambios con el terminal (MS). El módulo de identidad (SIM) puede inicializar entonces la transferencia de una nueva clave utilizando esa clave de inicialización (23) para autenticar al terminal (MS) y/o el módulo de identidad (SIM) como también para encriptar los intercambios. Para esta inicialización se puede requerir asimismo el control de eventuales características del terminal (MS) como claves de inicialización y certificados de inicialización presentes en el terminal (MS). Además, se pueden transmitir asimismo al módulo (SIM) características del terminal (MS) verificables por la red, por ejemplo el IMEI o la velocidad máxima de transmisión del terminal, para que aquel efectúe un control suplementario sobre el terminal (MS).

Por supuesto, en el procedimiento según la invención se pueden efectuar etapas de reinicialización, reactivación, idénticas o similares a la etapa de inicialización. En una forma de realización de la invención, dicha etapa de inicialización puede ser efectuada después de un repudio de clave, una expiración de la vigencia de clave o en la inicialización del módulo de identidad, por ejemplo en fábrica.

La etapa de autenticación puede consistir en particular, en primera instancia, en aplicar a uno o varios algoritmos memorizados en el terminal una clave de autenticación simétrica o asimétrica memorizada en el terminal (MS). De igual manera, en el módulo de identidad (SIM) se puede aplicar a uno o varios algoritmos memorizados en dicho módulo (SIM) la clave asociada, simétrica o asimétrica, memorizada en el módulo (SIM). La respuesta producida en el terminal (MS) es memorizada, por ejemplo, en el terminal y luego transmitida (11) al módulo de identidad (SIM), tal y como se ilustra en la figura 2. Esta respuesta es comparada (12) con la producida en el módulo (SIM). Si las respuestas se corresponden, entonces el terminal (MS) ha superado una primera prueba que indica que eventualmente se le puede considerar un terminal de confianza. Si el control (24) de una característica específica tal como por ejemplo el IMEI también confirma que el terminal es efectivamente el de "confianza", se podrán efectuar intercambios de datos (13), por ejemplo intercambios de contenidos únicamente accesibles mediante abono y transmitidos a través de la red radio. En el ejemplo de la figura 2, la etapa de autenticación se puede iniciar mediante una solicitud (10) por parte del módulo de identidad (SIM). En otras formas de realización, la autenticación también puede ser iniciada por el terminal (MS).

Ya que los terminales (MS) no están diseñados para resistir a los ataques a lo largo del tiempo, la vida útil de una clave preferentemente es limitada. Tanto en el módulo (SIM) como en el terminal (MS) se efectúa un procedimiento de comparación de la fecha límite de validez de una clave con la fecha actual, para permitir en su caso desencadenar una actualización. En una forma de realización de la invención, la vida útil de las claves almacenadas en el terminal (MS) y el módulo de identidad (SIM) es relativamente breve, limitada por un plazo determinado sinónimo de fin de validez. Un mecanismo de actualización de esas claves, por ejemplo a intervalos regulares, permite obviar problemas de protección de los terminales (MS) de forma duradera.

A continuación se describirá la invención en relación con las figuras 3 y 5.

El principio de actualización consiste en aprovechar la coubicación del módulo de identidad (SIM) y del terminal (MS). Consideremos, en primera instancia, que el módulo de identidad (SIM) y el terminal (MS) poseen una clave simétrica común que les permite autenticarse. Antes del fin de validez de la clave, el terminal (MS) inicia con el módulo de identidad (SIM), o viceversa, una actualización de esta clave. En el ejemplo de la figura 3, la petición de actualización (30) la inicia el módulo de identidad (SIM). El módulo de identidad (SIM) es entonces el encargado de generar la nueva clave, llamada actualizada, de almacenarla y de transmitirla al terminal (MS). La generación de

esta clave puesta al día la es realizada por un algoritmo de puesta al día de dicho módulo (SIM) que toma en cuenta una información, por ejemplo la fecha de validez de la antigua clave válida compartida. En esta actualización, el terminal (MS) y eventualmente dicho módulo (SIM) se autentican (31) en virtud de la antigua clave válida compartida. En una forma de realización de la invención, el almacenamiento en una memoria del módulo de identidad (SIM) de la clave puesta al día puede efectuarse mediante la mera y simple sustitución de la antigua clave. En esta fase se puede utilizar un identificador del terminal (MS) y/o del módulo (SIM), por intermedio o no de un certificado, para facilitar la administración del sistema y la autenticación del terminal (MS) y del módulo de identidad (SIM). Además, el intercambio de la clave puesta al día (33) se hace encriptando la clave puesta al día. Esta encriptación puede fundamentarse en el uso de la clave compartida para la encriptación, como también en virtud de la generación de una clave de sesión (32), realizada después de dicha autenticación entre el terminal (MS) y el módulo de identidad (SIM). En una actualización de este tipo no se efectúa ningún intercambio con la red, desempeñando el módulo de identidad la función de "entidad de certificación".

En una forma de realización de la invención, la generación de una llave llamada de confianza, como es una clave de sesión o análoga, se efectúa en el módulo de identidad (SIM), memorizándose a continuación la clave de confianza en dicho módulo (SIM). Dicha clave de confianza es transmitida a continuación al terminal (MS) y memorizada en el terminal (MS). En otra variante, la clave es generada a la vez en el terminal (MS) y el módulo (SIM). La actualización puede terminar con una prueba de verificación que comprende una transmisión de vuelta, por parte del terminal (MS), de al menos uno de los datos transmitidos por el módulo de identidad (SIM) en la actualización, o bien un dato representativo de la correcta recepción de la información transmitida por el módulo de identidad (SIM). Por ejemplo, cuando el terminal (MS) ha recibido y memorizado bien dicha clave puesta al día enviada (33) desde el módulo de identidad (SIM), éste remite al módulo de identidad (SIM) un mensaje de confirmación (34).

El refuerzo de la seguridad permitido por el procedimiento según la invención permite resolver la problemática a la que se enfrentan casos tales como la tecnología DRM. La figura 4 ilustra esquemáticamente la falta de refuerzo de seguridad en los intercambios de contenidos en los procedimientos de la técnica anterior, por ejemplo entre un terminal móvil y una tarjeta SIM. En primera instancia, el terminal (MS) controla (E3) simplemente las reglas de uso del contenido en posesión de la tarjeta SIM. Seguidamente la tarjeta SIM concede un permiso (E4) de "reproducir" el contenido y un acuerdo de transferencia de la llave de desencriptación. A continuación, la tarjeta SIM transmite la clave de desencriptación en claro al terminal (MS). En este tipo de procedimiento, la provisión de datos teóricamente no accesibles por el usuario queda abierta a terminales tales como un PC dotado de un lector de tarjeta inteligente. Por otro lado, si los intercambios no están encriptados, la utilización de una sonda también permite tener conocimiento de datos confidenciales. El procedimiento según la invención, con una verdadera etapa de autenticación del terminal (MS) por el módulo de identidad (SIM) y una encriptación de los intercambios, asegura un fiable refuerzo de la seguridad en los intercambios para evitar tales fallas.

En una forma de realización de la invención, es posible revocar la clave asociada al terminal (MS). El repudio de la clave se puede realizar por iniciativa del módulo de identidad (SIM) o de la red, y eventualmente por el terminal (MS). El principio consiste en repudiar la clave en el módulo de identidad (SIM) que eventualmente informa, en virtud de un programa memorizado en dicho módulo (SIM), a la red y al terminal (MS) de este repudio. La revocación comprende el borrado de al menos la clave que se va a repudiar asociada al terminal (MS) en una memoria de dicho módulo de identidad (SIM). Así, el terminal (MS), si desea repudiar la clave, por ejemplo en el caso en que detecta que se ha actualizado su SO, informa de ello al módulo de identidad (SIM), que eventualmente informa de ello a la red, en virtud de los mecanismos convencionales OTA seguro. Si la red desea repudiar la clave, por ejemplo en el caso en que detecta que unas características del terminal (MS) han cambiado, tales como el IMEI como también la velocidad máxima de transmisión teórica desde el terminal (MS), la red informa de ello al módulo de identidad (SIM) en virtud de los mecanismos convencionales OTA seguro. A continuación, el módulo de identidad (SIM) eventualmente informa de ello al terminal (MS). Si el módulo de identidad (SIM) desea repudiar la clave, éste informa de ello eventualmente al terminal (MS) y eventualmente a la red. Puede ser una alternativa el borrado de la clave de autenticación y de encriptación en el terminal (MS) y/o el módulo (SIM). En adelante, el módulo de identidad (SIM) ya no podrá autenticar al terminal (MS) y será necesaria una reinicialización.

En una forma de realización de la invención, el módulo de identidad (SIM) incluye medios para memorizar al menos una clave de autenticación, una clave de cifrado así como al menos dos algoritmos. El módulo (SIM) también puede tener los medios para almacenar la clave de cifrado así como el algoritmo de encriptación con el terminal (MS). Estos medios pueden ser por ejemplo una memoria de tipo EEPROM, de tipo ROM o una combinación de ambas. El módulo de identidad (SIM) también incluye unos medios de cálculo para ejecutar al menos una etapa consistente en aplicar dicha clave de autenticación al algoritmo memorizado en el módulo de identidad (SIM), y unos medios de activación de un algoritmo de puesta al día de dicha clave de autenticación. El módulo de identidad (SIM) también comprende unos medios para iniciar una revocación y unos medios de revocación para revocar la clave de autenticación asociada al terminal (MS), unos medios de memorización de una característica específica del terminal (MS) y unos medios de activación de un algoritmo de puesta al día de la clave de autenticación asociada al terminal (MS). El módulo de identidad (SIM), además, puede corresponder, en una forma de realización de la invención, a una tarjeta inteligente proactiva.

Los medios de revocación pueden permitir bien un procedimiento de borrado del área de memoria contenedora de la

clave de autenticación, o bien el posicionamiento de un bit asociado a esa área. En este último caso, el bit será leído sistemáticamente con cada petición de acceso a esa área y, según su valor, el acceso será autorizado (clave válida) o rechazado (clave revocada).

Después de un repudio, una expiración de la vida útil de la clave o en la inicialización, se da a la red la iniciativa de activación de las claves. La red decide inicializar o reinicializar el modelo de confianza cuando estima que el terminal (MS) es un terminal de confianza. La red envía un mensaje al módulo de identidad (SIM) en virtud de los mecanismos convencionales OTA seguro basados, por ejemplo, en los mecanismos previstos por la norma GSM 03.48 para indicar que dicho módulo (SIM) puede intercambiar una clave con el terminal (MS). El mensaje puede ser enviado por igual por la red a las otras dos entidades (SIM, MS). La inicialización o la reactivación pueden ser realizadas sin protección de los intercambios entre el módulo (SIM) y el terminal (MS). Pero ésta puede fundamentarse asimismo en el uso de una clave de inicialización que estaría presente en el terminal (MS) y proporcionada al módulo de identidad (SIM) por un mecanismo OTA seguro.

En la invención, el número de claves que pueden ser utilizadas no está en modo alguno limitado. Por supuesto, se pueden utilizar y generar varias claves. Cabe así la posibilidad de utilizar una clave para autenticar al terminal (MS) así como una clave para encriptar los intercambios, e incluso una clave por tipo de intercambio que ha de encriptarse. Igualmente es posible el uso de claves asimétricas en lugar de claves simétricas.

Una de las ventajas del procedimiento según la invención es la toma en cuenta de manera flexible y económica del problema fundamental de la autenticación del terminal ante el módulo (SIM): al principio del diálogo entre el módulo de identidad (SIM) y el terminal (MS), el módulo de identidad (SIM) debe tener pruebas de que el terminal es efectivamente aquel que pretende ser, y de que efectivamente pone en práctica los mecanismos esperados. En lugar de basarse en un mecanismo estático de certificación del terminal, el procedimiento descrito propone una certificación dinámica del terminal, que utiliza la red como una herramienta de certificación dinámica, por ser funcional: si el terminal es efectivamente aquel que pretender ser, tiene que ser capaz de superar con éxito un cierto número de pruebas, que implican en especial intercambios con el módulo de identidad (SIM) y bajo el control de este módulo (SIM). Resulta entonces muy difícil crear un simulador de terminal para tener acceso a la clave de autenticación/cifrado del entorno seguro, pues hará falta que ese terminal realice correctamente todas las funciones sometidas a prueba, lo cual en la práctica será muy difícil de realizar.

Otra de las ventajas de la invención respecto a las técnicas existentes es que incluso si parece que algunos terminales (MS) no seguros han roto el anterior mecanismo y permitido a terceros no autorizados tener acceso a contenido seguro, es muy difícil revocar esos terminales (MS), ya que el módulo de identidad (SIM) no deja de ser el elemento maestro del dispositivo y la red puede enviarle en todo momento una orden de invalidación.

Otra ventaja de la invención radica en el acoplamiento entre el módulo de identidad (SIM) y el terminal (MS), que puede ser utilizado para proteger datos conocidos y modificables del usuario, por ejemplo el «login» y la contraseña de acceso al banco del usuario, para almacenar datos que el usuario no debe poder modificar, por ejemplo derechos de utilización de un programa o de una música. Este acoplamiento puede aplicarse asimismo para el almacenamiento de datos que el usuario no debe poder conocer, por ejemplo almacenamiento de una clave que permite desencriptar una música antes de su ejecución. Las funciones transmitidas al terminal (MS) por el módulo de identidad (SIM) pueden ser funciones de criptografía, de monedero electrónico como también funciones de almacenamiento y de acceso a datos.

Son múltiples las aplicaciones de la invención. Así, en una aplicación DRM, la tarjeta SIM puede ser utilizada para almacenar derechos de utilización y eventuales claves de desencriptación de contenido. Cuando un programa de aplicación del terminal (MS) necesitará una de sus claves, podrá consultar al terminal (MS), que identificará la aplicación y que se autenticará ante la tarjeta SIM. En consecuencia, la tarjeta SIM, al considerar al terminal (MS) de confianza, podrá controlar los derechos de uso de las claves por parte del programa de aplicación y transmitir luego las claves necesarias para el programa de aplicación. La transmisión de estas claves podrá ser encriptada, en virtud de la utilización de una clave de sesión o en virtud de la utilización de una clave prevista al efecto, como también en virtud de la utilización de la clave de cifrado.

Debe ser evidente para las personas peritas en la materia que la presente invención permite formas de realización en numerosas otras formas específicas sin apartarse del ámbito de aplicación de la invención según se reivindica. Consecuentemente, las presentes formas de realización deben ser tomadas a título de ilustración, pero pueden ser modificadas dentro del ámbito definido por el alcance de las reivindicaciones adjuntas, y la invención no debe quedar limitada a los detalles dados anteriormente.

REIVINDICACIONES

1. Procedimiento de establecimiento y de gestión de un modelo de confianza entre un módulo de identidad (SIM) y un terminal radio (MS), caracterizado por que incluye:

- una etapa de autenticación del terminal (MS) por dicho módulo de identidad (SIM), realizándose dicha etapa de autenticación por mediación de medios de autenticación proporcionados ya sea a dicho módulo de identidad (SIM) por una red de radiotelefonía móvil en una etapa llamada de inicialización o en una etapa llamada de actualización, ya sea a dicho terminal (MS) por el módulo de identidad (SIM),

- una etapa de control por dicho módulo (SIM) de al menos una característica específica del terminal (MS), siendo previamente transmitida dicha característica específica a dicho módulo por radiotelefonía, desde un servidor seguro (SS) de dicha red de radiotelefonía móvil.

2. Procedimiento según la reivindicación 1, en el que la vida útil de dichos medios de autenticación del terminal (MS) presentes en el módulo de identidad (SIM) queda limitada por un plazo determinado, constituyéndose dichos medios de autenticación mediante al menos una clave de autenticación.

3. Procedimiento según la reivindicación 1 ó 2, en el que dicho módulo de identidad (SIM) es una tarjeta inteligente de tipo SIM o una tarjeta USIM para redes de tercera generación o una tarjeta equivalente que incluye en una memoria datos representativos de abono.

4. Procedimiento según una de las reivindicaciones 1 a 3, en el que el módulo de identidad (SIM) mantiene una relación de confianza con el terminal radio (MS) generando unos medios de autenticación y proporcionando seguidamente estos medios de autenticación al terminal radio (MS) en virtud de mecanismos de intercambio seguros y que se fundamentan en medios de autenticación inicialmente disponibles del terminal radio (MS).

5. Procedimiento según una de las reivindicaciones 1 a 4, que incluye, en dicha etapa de inicialización o de actualización, una etapa de generación, realizada al menos por dicho módulo de identidad (SIM), de una clave llamada de confianza, siendo utilizada dicha clave de confianza por dicho módulo (SIM) para encriptar al menos unos datos intercambiados entre el módulo de identidad (SIM) y el terminal (MS).

6. Procedimiento según una cualquiera de las reivindicaciones 2 a 5, en el que dicha etapa de inicialización de dichos medios de autenticación es efectuada, por iniciativa de la red de radiotelefonía, después de un repudio de clave iniciado por dicho módulo (SIM) o la red de radiotelefonía móvil o el terminal radio (MS), una expiración de la vigencia de clave o bien en la inicialización del módulo de identidad (SIM).

7. Procedimiento según una de las reivindicaciones 1 a 6, en el que dicha etapa de autenticación comprende en particular las siguientes etapas:

- una etapa de utilización en el terminal (MS) de al menos una primera clave de autenticación memorizada en el terminal (MS) mediante al menos un primer algoritmo de autenticación memorizado en el terminal (MS), teniendo dicha primera clave una vigencia limitada por un plazo determinado,

- una etapa de utilización, por parte del módulo de identidad (SIM), de al menos una segunda clave memorizada en el módulo de identidad (SIM) mediante al menos un segundo algoritmo de autenticación memorizado en el módulo de identidad (SIM), siendo dicha segunda clave idéntica o complementaria de la primera clave y asociada al terminal (MS), teniendo dicha segunda clave una vigencia limitada por dicho plazo determinado,

- una etapa de comparación (12) en el módulo de identidad (SIM) de los resultados obtenidos por dichos algoritmos primero y segundo.

8. Procedimiento según una cualquiera de las reivindicaciones 2 a 7, en el que la etapa de autenticación comprende la utilización de dicho plazo determinado.

9. Procedimiento según la reivindicación 7 u 8, en el que dicha etapa de inicialización es iniciada por una red de radiotelefonía móvil e incluye asimismo:

- la generación por parte del módulo de identidad (SIM) de al menos una de dichas claves primera y segunda,

- una memorización en el módulo de identidad (SIM) de dicha segunda clave,

- una transmisión al terminal (MS), por el módulo de identidad (SIM), de dicha primera clave, siendo encriptada esta primera clave por mediación de la clave de confianza.

10. Procedimiento según una cualquiera de las reivindicaciones 7 a 9, en el que dicha etapa de comparación (12) se efectúa entre, por una parte, una respuesta producida por dicho primer algoritmo, memorizada en el terminal (MS) y transmitida (11) a dicho módulo de identidad (SIM) y, por otra parte, un resultado de respuesta, memorizado

en el módulo de identidad (SIM), producido por dicho segundo algoritmo.

11. Procedimiento según una de las reivindicaciones 7 a 10, en el que dicha primera clave es una clave privada Ks asimétrica, siendo dicha segunda clave una clave pública Kp complementaria de la primera clave.

12. Procedimiento según una de las reivindicaciones 7 a 10, en el que dicha primera clave es simétrica, siendo dicha segunda clave memorizada en el módulo de identidad (SIM) idéntica a la primera, formando estas claves una sola clave simétrica de autenticación.

13. Procedimiento según una de las reivindicaciones 7 a 12, que comprende una etapa de actualización de dichas claves primera y segunda, iniciada por el módulo de identidad (SIM) antes de dicho plazo determinado, incluyendo dicha actualización las siguientes etapas:

- autenticación (31) entre el terminal (MS) y el módulo de identidad (SIM) con ayuda de dichas claves primera y segunda,

- generación mediante un algoritmo de puesta al día del módulo de identidad (SIM) de al menos una clave puesta al día que toma en cuenta una información para sustituir al menos una de dichas claves primera y segunda,

- memorización en el módulo de identidad (SIM) de la clave puesta al día para sustituir dicha segunda clave,

- transmisión (33) al terminal (MS), por el módulo de identidad (SIM), de la clave puesta al día análoga a dicha primera clave.

14. Procedimiento según la reivindicación 13, en el que dicha actualización comprende además el control de al menos un identificador del terminal (MS) y/o del módulo de identidad (SIM).

15. Procedimiento según una de las reivindicaciones 13 ó 14, en el que se realiza una encriptación de clave para dicha transmisión (33) al terminal (MS) de la clave puesta al día análoga a la primera clave, efectuándose dicha encriptación de clave mediante dicha clave de confianza.

16. Procedimiento según una de las reivindicaciones 13 a 15, en el que la actualización comprende asimismo las siguientes etapas:

- generación (32), por parte del módulo de identidad (SIM), de una nueva clave de confianza, después de dicha autenticación (31) entre terminal (MS) y módulo (SIM),

- memorización en el módulo de identidad (SIM) de la nueva clave de confianza,

- transmisión al terminal, por el módulo de identidad (SIM), de la clave de confianza recién generada.

17. Procedimiento según una cualquiera de las reivindicaciones 13 a 16, en el que dicha actualización termina con una prueba de verificación que comprende una transmisión de vuelta, por parte del terminal (MS), de al menos un dato representativo de la correcta recepción de la información transmitida por el módulo de identidad (SIM) en la actualización.

18. Procedimiento según una cualquiera de las reivindicaciones 5 a 17, en el que dicha clave de confianza es una clave de cifrado/descifrado simétrica idéntica a dicha clave simétrica de autenticación.

19. Procedimiento según una cualquiera de las reivindicaciones 5 a 18, en el que dicha clave de confianza es una clave de sesión borrable.

20. Procedimiento según una cualquiera de las reivindicaciones 7 a 19, en el que se realiza una etapa llamada de revocación por iniciativa del módulo de identidad (SIM), del terminal (MS) o de la pertinente red de radiotelefonía, comprendiendo dicha etapa de revocación el borrado, en una memoria de dicho módulo de identidad (SIM), de al menos dicha primera clave asociada al terminal (MS).

21. Módulo de identidad (SIM) en un terminal (MS) para la puesta en práctica del procedimiento según una de las reivindicaciones 1 a 20, caracterizado por que comprende medios para memorizar al menos una clave de autenticación así como al menos un algoritmo de autenticación, medios de cálculo para ejecutar al menos una etapa consistente en aplicar dicha clave de autenticación a dicho algoritmo de autenticación memorizado en el módulo de identidad (SIM), medios de comunicación, medios para iniciar una revocación y medios de revocación para revocar dicha clave de autenticación, medios de memorización de una característica específica del terminal (MS), medios de control de al menos una característica específica del terminal (MS) y medios de activación de un algoritmo de puesta al día de dicha clave de autenticación, siendo aptos los medios de comunicación para proporcionar al terminal (MS) al menos una clave de autenticación y para recibir datos procedentes de un servidor seguro (SS) de una red de radiotelefonía móvil.

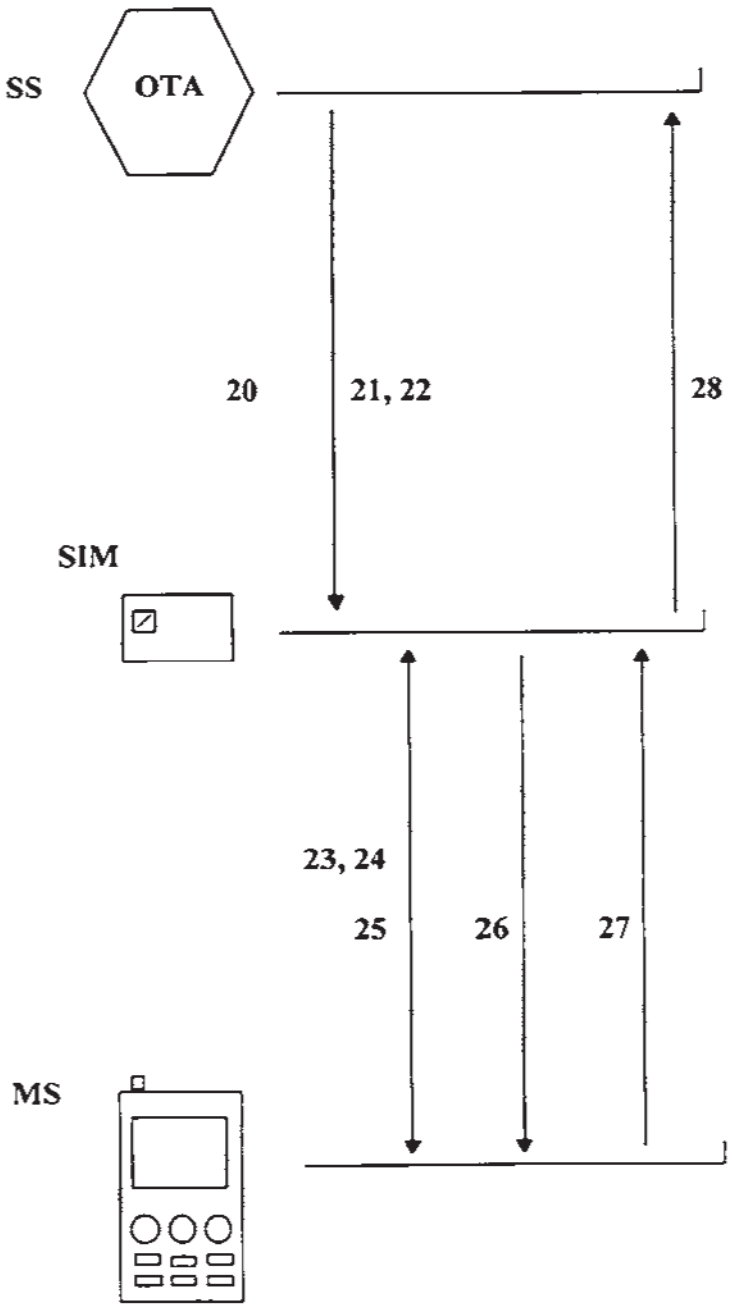

FIG 1

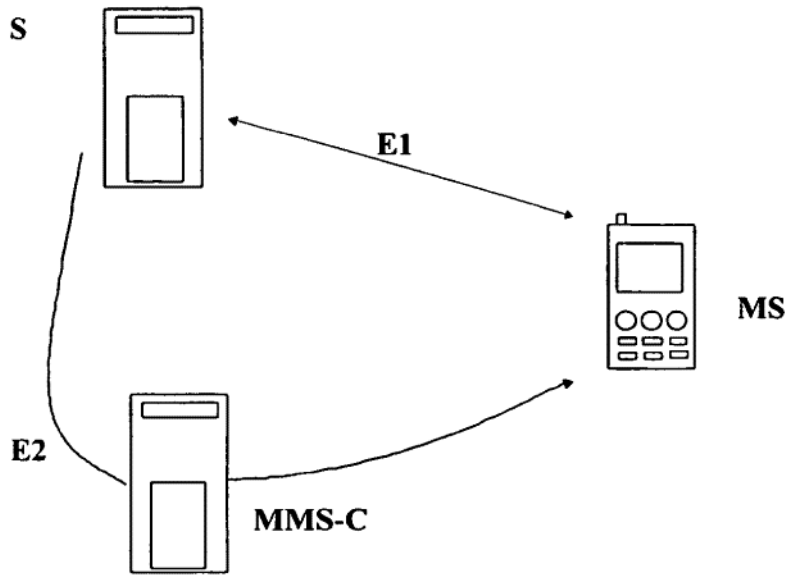

FIG 4

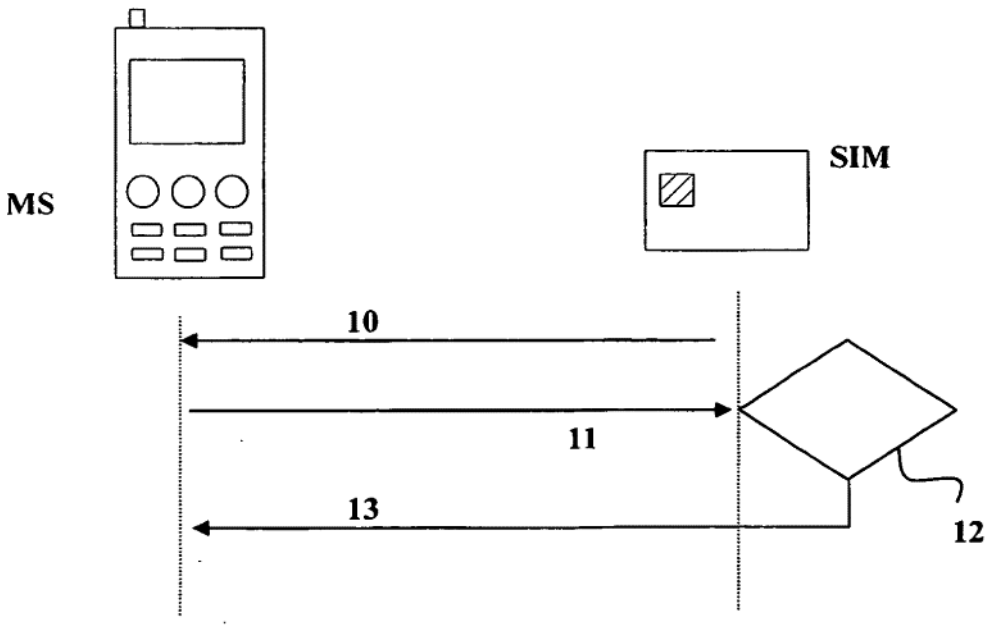

FIG 2

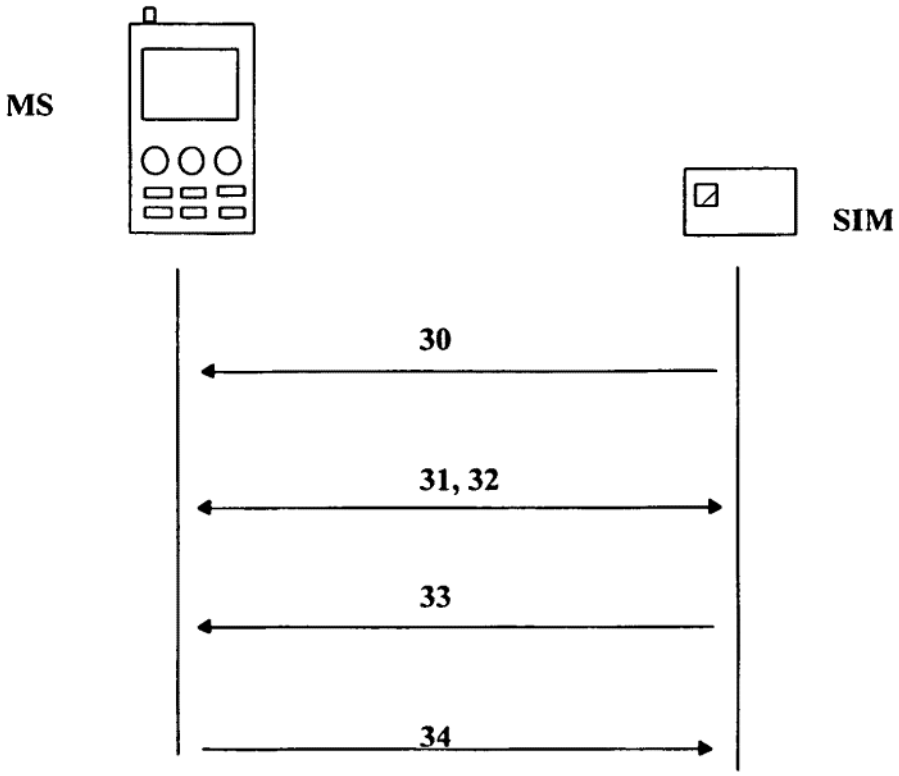

FIG 3

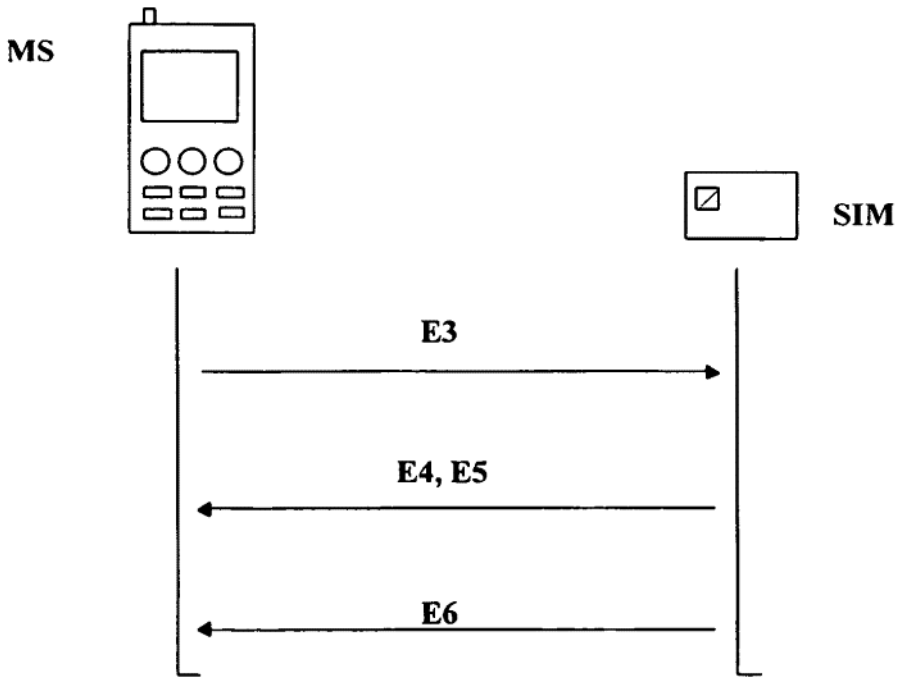

FIG 5