(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 429 136**

(51) Int. CI.:

H04W 12/12 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **03.11.2004 E 04818151 (5)**

(97) Fecha y número de publicación de la concesión europea: **10.07.2013 EP 1683388**

(54) Título: **Método de gestión de la seguridad de aplicaciones con un módulo de seguridad**

(30) Prioridad:

04.11.2003 EP 03104069

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.11.2013

(73) Titular/es:

NAGRAVISION S.A. (100.0%)
Route de Genève 22-24
1033 Cheseaux-sur-Lausanne, CH

(72) Inventor/es:

KSONTINI, RACHED y
CANTINI, RENATO

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Método de gestión de la seguridad de aplicaciones con un módulo de seguridad

[0001] La presente invención se refiere al ámbito de las redes móviles llamadas también redes celulares. Se refiere más particularmente a la gestión de la seguridad de las aplicaciones utilizadas con un módulo de seguridad asociado a un equipo móvil de telefonía móvil.

[0002] El módulo de seguridad de un teléfono móvil o portátil es conocido bajo la denominación de "tarjeta SIM" (Subscriber Identity Module) que constituye el elemento central de la seguridad de estos teléfonos. El operador de telefonía introduce, en el momento de la fabricación y/o durante una fase de personalización, un número llamado IMSI (International Mobile Subscriber Identification) que sirve para identificar de manera segura y única cada abonado que desee conectarse a una red móvil. Cada teléfono móvil, llamado equipo móvil a continuación, es identificado físicamente por un número almacenado en una memoria no volátil del equipo móvil. Este número, llamado IMEI, (International Mobile Equipment Identifier) contiene una identificación del tipo de equipo móvil y un número de serie que sirve para identificar de manera única un equipo móvil dispuesto sobre una red del tipo GSM (Global System for Mobile communications), GPRS (General Packet Radio System) o UMTS (Universal Mobile Telecommunications System). Además, un equipo móvil se caracteriza por una versión de software SVN (Software Version Number) que indica el estado de actualización del software de base instalado sobre el equipo móvil. La combinación de la identificación del tipo y del número de serie del equipo móvil con la versión de software (SVN) proporciona una nueva identificación, llamada IMEISV (International Mobile Equipment Identifier and Software Version Number). El mismo concepto de identificación se aplica también al WLAN (Wireless LAN) o al cable TV bidireccional. El identificador físico puede ser una dirección MAC (Media Access Control) que corresponde a la dirección única que identifica la configuración del material de un usuario en una red IP (Internet Protocol) y la versión de programa puede ser transmitida por unos protocolos de capa superior basados en el IP.

[0003] Las normas ETSI ("European Telecommunications Standards Institute"), definen una estación móvil (MS, mobile station) compuesta por un equipo móvil (ME, mobile equipment) y un módulo de abonado (SIM, subscriber identity module). Este módulo de abonado es en general móvil es decir que puede ser o bien retirado o transferido de un equipo móvil a otro.

[0004] Durante la puesta en servicio de un equipo móvil, más particularmente durante su conexión a la red de un operador, unas informaciones comprendiendo los datos de identificación son intercambiadas entre el equipo móvil y el centro de gestión del operador que autoriza o no su utilización.

[0005] El documento EP0757502 describe un método de cierre de un módulo de identificación de usuario cuando el identificador físico del equipo móvil IMEI está en una lista negra. Cuando el equipo móvil se conecta a la red móvil, transmite el identificador IMEI a un centro de gestión. Este último verifica por comparación el identificador recibido con el contenido de una base de datos en la que el operador registra los identificadores de equipos móviles robados o defectuosos. Si un identificador recibido está presente en esa base de datos, el centro de gestión transmite un mensaje que contiene una orden de bloqueo al equipo móvil relacionado. Esta orden, después de verificar su autenticidad, es transmitida al módulo de identificación que ejecuta un procedimiento de cierre impidiendo toda conexión ulterior del equipo móvil con la red.

[0006] El documento US5864757 describe un método de activación de un combinado móvil con un módulo de abonado basado en la utilización de una clave propia al combinado que produce un código correspondiente a un identificador del módulo de abonado. El combinado incluye una clave única inviolable. Durante su activación, el centro de gestión del operador transmite un mensaje al combinado que sirve para que el operador calcule una clave específica utilizando la clave única del combinado. Esa nueva clave es utilizada en combinación con un identificador de la red o del módulo de abonado para generar una palabra de control que es confrontada con un código almacenado en el módulo de abonado. Si la contraseña de control concuerda con el código del módulo de abonado, el combinado es activado.

[0007] Los métodos descritos en esos dos documentos tratan exclusivamente aspectos que necesitan una identificación física del equipo móvil basada por ejemplo en el identificador IMEI. Cuando se ponen en práctica esos métodos, sus efectos se centran únicamente en el bloqueo / desbloqueo del módulo de abonado y/o del equipo móvil para impedir cualquier conexión del equipo móvil con la red.

[0008] Actualmente un equipo móvil ofrece al usuario, además de su función usual de establecimiento de conversaciones telefónicas a través de un acceso a una red móvil, el uso de varios otros servicios suplementarios de valor añadido tales como la consulta de diversas informaciones, las operaciones bancarias a distancia, el comercio electrónico, el acceso a un contenido multimedia, etc. Estos servicios evolucionados necesitan un nivel de seguridad cada vez más elevado para preequipar a los usuarios contra los fraudes eventuales causados por terceros que intentan aprovecharse de los fallos de seguridad que pueden aparecer en los equipos móviles.

[0009] Una verificación es por lo tanto necesaria al menos a dos niveles: por una parte al nivel del propio equipo móvil y por otra parte al nivel de las aplicaciones de software que permiten el funcionamiento de los diferentes servicios propuestos por el operador o por terceros. Se trata de garantizar el hecho de que el módulo de abonado funcione sólo con un equipo móvil de un tipo y versión de programa debidamente autorizado o homologado por el operador y/o por los proveedores de aplicaciones. Por funcionamiento del módulo de abonado, se entiende su capacidad para permitir la utilización de servicios solicitados por un usuario mediante la ejecución de un número de aplicaciones de software instaladas previamente en una memoria del equipo móvil y que utilizan el módulo de abonado como medio de protección.

[0010] Estas aplicaciones ejecutadas en el equipo móvil utilizan recursos disponibles en el módulo de abonado. Por recursos, se entienden diversas funciones y datos necesarios al buen funcionamiento de una aplicación. Algunos de estos recursos pueden ser comunes a varias aplicaciones, en particular a las funciones relacionadas con la seguridad. El módulo de abonado puede de este modo bloquear o alterar el funcionamiento de ciertas aplicaciones para las que las condiciones de seguridad establecidas por el operador y/o los proveedores de aplicaciones no son respetadas en el equipo móvil en cuestión o los derechos del usuario del equipo móvil son insuficientes.

[0011] Los documentos citados anteriormente no cubren los aspectos lógicos relativos a un conjunto de equipos móviles como por ejemplo unas informaciones relativas a unas aplicaciones de software instaladas, un número de versión de software o también una referencia de tipo o de modelo del equipo móvil, etc. Se trata por lo tanto de disponer de un método de gestión determinado de los recursos del módulo de abonado con el fin de activar / desactivar de una manera selectiva unas aplicaciones o funciones de aplicaciones que utilizan estos recursos. Sin embargo no es deseable que estas operaciones impidan que el equipo móvil acceda a la red mediante el bloqueo total del módulo de abonado.

[0012] El objetivo de la presente invención es de proponer un método de gestión de la seguridad del conjunto equipo móvil, módulo de abonado, aplicaciones con el fin de limitar los riesgos relacionados con el hecho de que un módulo de abonado sea utilizado con malas intenciones por unas aplicaciones ejecutadas sobre un equipo móvil de tipo y/o de versión de programa que no cumplen con algunos criterios de seguridad preestablecidos.

[0013] Otro objetivo consiste en proteger al usuario del equipo móvil así como a los proveedores de aplicaciones referentes contra los abusos resultantes de una clonación del equipo móvil y/o del módulo de abonado.

[0014] Estos objetivos son alcanzados por un método de gestión de la seguridad de aplicaciones según la reivindicación 1.

[0015] Los recursos del módulo de abonado son bloqueados de manera determinada, esto con el objetivo de bloquear o reducir la función de algunas aplicaciones. No se bloquean directamente unas aplicaciones del equipo: se actúa de forma indirecta sobre las aplicaciones, es decir que el efecto de bloqueo se va a manifestar únicamente cuando el equipo intente ejecutar estas aplicaciones.

[0016] Este método se aplica preferiblemente a la red móvil. Por consiguiente, el equipo es un equipo móvil, como por ejemplo un equipo de telefonía móvil o teléfono móvil. El módulo de seguridad es un módulo de abonado insertado en el teléfono móvil del tipo tarjeta SIM (subscriber identity module). Este conjunto se conecta a una red móvil del tipo GSM (Global System for Mobile communications), GPRS (General Packet Radio System), UMTS (Universal Mobile Telecommunications System) u otra, gestionada por un servidor de control de un operador. Unas aplicaciones de software son instaladas en el equipo móvil y configuradas para utilizar unos recursos (datos o funciones) presentes en el módulo de abonado. Por lo que éstas sólo pueden ser utilizadas en su integridad si las condiciones de seguridad son satisfactorias según de los criterios preestablecidos por el operador y/o el proveedor de aplicaciones. Esta verificación de criterios está a cargo del servidor de control. La aplicación, según las instrucciones enviadas por el servidor de control, está finalmente a cargo del módulo de seguridad que puede dejar libre o bloquear el acceso a unos recursos necesarios al buen funcionamiento de una aplicación instalada en el equipo móvil.

[0017] Los datos de estos recursos pueden comprender informaciones tales como un número de cuentas, unos programas (en forma de código que puede ser instalado en el equipo móvil), unas llaves de encriptación / desencriptación, de los derechos de acceso a un contenido, etc..

[0018] Las funciones de estos recursos pueden comprender algoritmos criptográficos, procesos de verificación, procesos de generación de firmas digitales, procesos de encriptado, procesos de autentificación, procesos de validación de datos, procesos de control de acceso, procesos de salvaguardia de datos, procesos de pago etcétera.

[0019] El servidor de control tiene una función esencial de gestión de los elementos de confianza o de seguridad relacionados con el conjunto equipo móvil / módulo abonado. Éste interpreta los datos que le son transmitidos por el equipo móvil con el fin de controlar o limitar la utilización de aplicaciones, funciones o recursos disponibles por medio del módulo de abonado.

[0020] El servidor que recibe las informaciones de identidad de un equipo móvil y de su módulo de abonado y que comprende el IMEISV y el IMSI decide, según ciertos criterios, si se debe enviar una nueva instrucción al módulo de abonado para redefinir un nuevo perfil de protección que define los recursos del módulo de abonado que pueden ser utilizados por las aplicaciones ejecutadas en el equipo móvil. Los criterios pueden referirse, por ejemplo, a la actualización de la versión de software instalado sobre el equipo móvil, a la descarga de nuevas aplicaciones sobre el equipo móvil, al período de actualización del perfil de protección, al número de conexiones a la red, a la tecnología utilizada para el acceso a la red, a la identidad de la red de acceso utilizada. También están relacionados con distintos riesgos asociados al material o a los programas utilizados que el operador y/o el proveedor de aplicaciones y/o el usuario del equipo móvil desean tener en cuenta.

[0021] El método según la invención se ejecuta en general en cada conexión del equipo móvil a la red o después de cada actualización de la versión de software del equipo móvil o de la del módulo de abonado o también de la de recursos sobre el módulo de abonado. También se puede ejecutar la activación durante cada activación o desactivación de una aplicación sobre el equipo móvil.

[0022] Según una variante, ésta puede ser ejecutada periódicamente a un ritmo establecido por el servidor de control o después de cada puesta en funcionamiento de aplicación sobre el equipo móvil. Según otra variante, el módulo de abonado no va a recibir un nuevo mensaje del centro de control mientras que el identificador IMEISV del equipo móvil permanece igual.

[0023] Durante la reinicialización del módulo de abonado, es preferible bloquear cierto número de recursos hasta la llegada del criptograma. De este modo, si el equipo móvil quiere interceptar el criptograma y no transmitirlo al módulo abonado, todos o parte de los recursos (datos o funciones) del módulo de abonado no serán disponibles para las aplicaciones ejecutadas en el equipo móvil. Según el tipo de realización, ciertos recursos del módulo de abonado utilizados por unas aplicaciones de nivel de seguridad bajo, pueden estar puestas en funcionamiento por defecto antes de la llegada del criptograma. Éste es el caso también de unos recursos necesarios para la obtención del acceso a la red, sin lo cual no se podría conseguir el envío del criptograma por esa misma red.

[0024] Cuando el módulo de abonado verifica la validez del criptograma, éste identifica también de forma indirecta el equipo móvil y se asegura de que los datos provienen efectivamente del servidor de control. Dicho de otra manera, por medio de este criptograma, el servidor de control asegura implícitamente al módulo de abonado que el tipo y la versión de software del equipo móvil han sido tomados en cuenta antes de transmitir las instrucciones al módulo abonado. Estas últimas se encargan de esta manera, si llega el caso, de dar o negar la autorización de utilización completa o parcial de ciertas aplicaciones del equipo móvil.

[0025] El equipo móvil tiene una función de relevo en esta etapa de verificación estableciendo un diálogo casi directo entre el módulo de abonado y el servidor de control. De este modo la seguridad de los mensajes intercambiados es asegurada de principio a fin entre el servidor de control y el módulo de abonado por el entorno de ejecución de las aplicaciones puestas en práctica sobre el equipo móvil. Por lo que dicho equipo no puede "hacer trampas" o transformar los datos con respecto al módulo de abonado.

[0026] La presente invención se refiere también a un módulo de seguridad describe por la reivindicación 19.

[0027] Este módulo de seguridad es utilizado por ejemplo como módulo de abonado o tarjeta SIM conectado a un equipo móvil.

[0028] La invención será mejor entendida gracias a la descripción detallada siguiente y que se refiere a las figuras anexadas proporcionadas a modo de ejemplo en ningún caso limitativo, a saber:

- la figura 1 ilustra un esquema funcional que muestra las distintas partes del equipo móvil y del servidor empleadas durante el intercambio de los datos de identificación y del criptograma.
- la figura 2 representa un esquema funcional del conjunto equipo móvil / módulo abonado con las interacciones entre los distintas partes durante el funcionamiento de una aplicación.

[0029] La figura 1 muestra el conjunto equipo móvil (CB) y módulo de abonado (SIM) que transmite a través de una red móvil (NET) unos datos de identificación (ID) que el servidor de control (CSE) verifica. Este último reenvía un criptograma (J) hacia el módulo de abonado a través del equipo móvil (CB). El equipo móvil (CB) incluye una o varias aplicaciones de software (APP) que funcionan en un entorno de ejecución (AEE). Estas aplicaciones provienen o de un proveedor de aplicaciones (FA) asociado al servidor de control (CSE) del operador, o bien son programadas al origen por el fabricante del equipo móvil.

[0030] El módulo de abonado incluye unos recursos (RES) utilizados por las aplicaciones de software (APP).

[0031] La figura 2 muestra que el funcionamiento de las aplicaciones (APP) del equipo móvil (CB) depende directamente de los recursos (RES) disponibles en el módulo de abonado. En ausencia de recursos adecuados, la aplicación puede, o no empezar, o bien funcionar de forma muy limitada con unos parámetros por defecto que

pueden generar mensajes de error que inducen al usuario a realizar acciones correctivas necesarias como por ejemplo cambiar de equipo móvil (CB) o de módulo de abonado (SIM).

[0032] El equipo móvil (CB) se identifica, por ejemplo en cada solicitud de conexión a la red, al servidor de control (CSE) a través de la red móvil (NET) transmitiendo preferiblemente informaciones específicas a un equipo móvil: IMEISV (International Mobile Equipment Identity and Software Version Number) y un código propio a un módulo de abonado: IMSI (Internacional Mobile Subscriber Identity). El primer número IMEISV es una serie de 16 cifras que contiene principalmente un código de homologación del fabricante del equipo móvil un número de serie que identifica físicamente el equipo móvil de manera única y la versión de software instalada sobre el equipo móvil en cuestión. El segundo número IMSI es una serie de 15 cifras e incluye un código atribuido por el operador con el que un usuario ha suscrito un abono que permite identificar a un abonado de manera única. Para unos equipos móviles realizados según unas normas anteriores establecidas por ETSI (European Telecommunications Standards Institute), la combinación del número IMEI compuesto por una serie de 15 cifras y del número SVN compuesto por una serie de 2 cifras proporciona también las informaciones necesarias a la realización del método.

[0033] Durante la identificación de un equipo móvil, el servidor de control (CSE) analiza y verifica los datos (ID) transmitidos comparándolos con el contenido de una lista negra (datos que rechazar) o de una lista blanca (datos aceptados).

[0034] Un banco de datos permite afinar, si se necesita, la identificación de un abonado y determinar sus particularidades tales como servicios autorizados, pagos del abono y/o servicios efectuados o no, período de abono, perfil de seguridad asociado al equipo móvil utilizado, aplicaciones instaladas sobre el equipo móvil, recursos disponibles sobre el módulo de seguridad, preferencias del usuario del equipo móvil, etc.. Los resultados de esta verificación son posteriormente utilizados con el fin de determinar un criptograma, llamado ficha (J), que el servidor de control (CSE) transmite al equipo móvil (CB). Se debe señalar que el servidor de control (CSE) puede ser distinto del operador móvil y la solicitud que proviene de un equipo móvil será enviada hacia esa autoridad de control.

[0035] El entorno de ejecución de aplicaciones (AEE) del equipo móvil (CB) transmite la ficha (J) tal cual, sin alterarla, al módulo de abonado, el equipo móvil (CB) sólo tiene una función de relevo.

[0036] Si la ficha (J) es válida, el módulo de abonado puede liberar, respectivamente bloquear ciertos recursos (RES). La o las aplicaciones (APP) pueden ejecutarse de este modo según los criterios impuestos por el servidor de control (CSE). Efectivamente, la ficha (J) incluye o es acompañada por unas instrucciones particulares con destino hacia el módulo de abonado que pueden condicionar el funcionamiento de una u otra de las aplicaciones (APP) del equipo móvil (CB). Por ejemplo la ejecución de transacciones financieras puede ser limitada cuando el abonado está conectado a otra red que la red a la que está abonado, por ejemplo en un país diferente a su domicilio (roaming) debido a ciertos criterios de seguridad o de preferencias del abonado o de preferencias del proveedor del servicio financiero o de restricciones legales vigentes en el país en cuestión. En otro caso, cuando un módulo de abonado es insertado en un equipo móvil (CB) no reconocido o no homologado por el operador, la ficha (J) devuelta por el servidor de control (CSE) puede bloquear unos recursos (RES) del módulo de abonado y, de esta manera impedir o alterar, la ejecución de la o de las aplicaciones (APP).

[0037] En el caso de una posible clonación del equipo móvil (CB) y/o del módulo de abonado (SIM), los resultados de la verificación con el banco de datos incluirán unas instrucciones que dependen de los riesgos que el operador acepta tomar con unos teléfonos móviles clonados. Por ejemplo, la ficha (J) generada en consecuencia puede o bloquear todos los recursos (RES) del módulo de abonado, o bien limitar su utilización en el tiempo y/o crear un mensaje de advertencia para el abonado a través del ambiente de ejecución de las aplicaciones (AEE).

[0038] La ficha (J) puede por ejemplo estar asociada a una firma generada por medio de una clave privada RSA, (Rivest, Shamir, Adelman) K_{RSA_Pri} a partir de un conjunto de datos comprendiendo, por ejemplo, el IMSI, el IMEISV, las referencias de los recursos del módulo de abonado, un contador. Sólo el servidor de control conocería esta clave, mientras que el módulo de abonado conocería su parte pública K_{RSA_Pub}. La ventaja de utilizar claves asimétricas reside en el hecho de que la clave que sirve para crear firmas no se encuentra al exterior del servidor de control (CSE).

[0039] Por supuesto, otros algoritmos de claves asimétricas tales como por ejemplo DSA (Digital Signature Algorithm), y ECC (Elliptic Curve Cryptography) pueden constituir unas alternativas a RSA.

[0040] Se puede preferir el uso de algoritmo de claves simétricas por razones de sencillez, de rapidez de las verificaciones o de costes de fabricación y de puesta en práctica más reducidos. En ese caso, el servidor (CSE) y el módulo de abonado conocerían la clave, por ejemplo un algoritmo IDEA (International Data Encryption Algorithm) podría ser utilizado para firmar el conjunto (IMSI, IMEISV, referencias de los recursos del módulo de abonado, contador). Como alternativa al algoritmo IDEA, unos algoritmos tales como, por ejemplo, TDES (Triple Data Encryption Standard) y AES (Advanced Encryption Standard) pueden ser utilizados también.

[0041] En estas dos variantes de claves asimétricas y simétricas, el módulo de abonado verifica la concordancia de los distintos campos que aparecen en la ficha (J), en particular controla el contador (CPT) comparándolo con un contador correspondiente memorizado en la tarjeta mantenida al día regularmente. Este contador permite evitar el uso doble de una misma ficha (J) dirigida al módulo de abonado con el fin de impedir un ataque de repetición (replay attack).

[0042] Una variante del contador consiste en utilizar un imprevisto aleatorio (número aleatorio) generado por el módulo de abonado. Este imprevisto aleatorio es transmitido con los datos enviados al servidor de control. Este último reenvía este imprevisto aleatorio en el criptograma de respuesta y el módulo de abonado puede verificar si se trata efectivamente de un nuevo mensaje. Más habitualmente, con el fin de evitar todo riesgo de uso de un antiguo criptograma, este último comprende una variable predecible por el módulo de abonado, sea un contador o un imprevisto aleatorio.

[0043] El módulo de abonado considera también las referencias de los recursos (RES) para los que autoriza o no la utilización mediante las aplicaciones ejecutadas en el equipo móvil (CB).

[0044] El módulo de abonado no conoce tal como son las referencias de aplicaciones (APP) instaladas en el equipo móvil (CB). Efectivamente, ciertas aplicaciones más globales poseen una interfaz relativamente abierta que les permite ser utilizadas por cualesquiera aplicaciones secundarias externas. Por ejemplo, sobre una aplicación general de pago se pueden añadir aplicaciones particulares en función del modo de pago utilizado. El módulo de abonado no puede basarse únicamente en las referencias de sus propios recursos (RES) (datos o funciones). Al aceptar los riesgos relacionados con un equipo móvil, el operador realiza una elección sabiendo cuáles son los recursos (RES) del módulo de abonado utilizados por tal(es) aplicación(es) (APP) ejecutadas en el equipo móvil (CB).

[0045] En otra variante la firma realizada con la ayuda de una clave del tipo RSA o IDEA puede ser reemplazada por un bloque generado con una clave compartida HMAC (Keyed-Hashing for Mensaje Authentication) a partir del conjunto (IMSI, IMEISV, referencias de recursos del módulo de abonado, contador). HMAC es un mecanismo para la autentificación de mensajes mediante la utilización de funciones de comprobación aleatoria criptográficas tales como MD5 (Message Digest) o SHA-1 (Secure Hash Algorithm), en combinación con una clave compartida es decir que la misma clave se encuentra en el servidor de control (CSE) y en el módulo de abonado.

[0046] Esta clave presente a la vez en el servidor de control (CSE) y en el módulo de abonado puede ser cargada durante la personalización del módulo de abonado o durante la instalación de ciertos recursos en el módulo de abonado. Según las opciones, cada recurso o grupo de recursos del módulo de abonado puede estar asociado a una clave diferente, o la clave puede ser global para el conjunto de recursos y único para un módulo de abonado proporcionado.

[0047] Para más seguridad, cuando el módulo de abonado ha recibido una ficha (J), éste puede retransmitir al servidor de control (CSE), a través del equipo móvil (CB) y la red móvil (NET), un mensaje de confirmación (CF) demostrando la buena recepción y el tratamiento adecuado de la ficha (J) por el módulo de abonado. La confirmación (CF) incluye al menos un código de éxito o de error de la operación así como un contador, similar al de la ficha (J), que sirve para la protección contra los ataques repetidos. Este mensaje permite también al servidor de control (CSE) actualizar el contador asociado al módulo de abonado.

[0048] En una variante de la invención, el equipo móvil puede ser reemplazado por un equipo no móvil tal como un descodificador de televisión de pago o un ordenador. El servidor de control recibe por parte de un módulo de seguridad, el equivalente del módulo de abonado, el identificador del equipo conectado a la red y el identificador del módulo de seguridad. En respuesta, el servidor efectúa las verificaciones tales como se han descrito anteriormente y reenvía un criptograma al módulo de seguridad. Esta respuesta va a liberar o bloquear los recursos en el módulo de seguridad.

REIVINDICACIONES

1. Método de gestión de la seguridad de aplicaciones (APP) que funciona en un equipo móvil (CB) conectado a una red (NET), dicha red (NET) está administrada por un servidor de control (CSE) de un operador, dichas aplicaciones (APP) utilizan recursos (RES), datos o funciones, almacenados en un módulo de abono (SIM) conectado localmente a dicho equipo móvil (CB), que comprende las siguientes etapas preliminares:

• recepción de datos que comprenden al menos el tipo y la versión del software del equipo móvil (CB) y la identidad del módulo de abonado (SIM), a través de la red (NET), por el servidor de control (CSE),

• análisis y verificación por el servidor de control (CSE) de dichos datos (ID),

• generación de un criptograma (J) a partir del resultado de la verificación sobre dichos datos (ID), y transmisión de dicho criptograma (J), a través de la red (NET) y el equipo móvil (CB), al módulo de abonado (SIM),

• recepción y análisis del criptograma (J) por el módulo de abonado (SIM), el criptograma (J) comprende instrucciones que condicionan el funcionamiento de aplicaciones (APP) según los criterios establecidos por el proveedor de dicha aplicación (APP) y/o el operador y/o el usuario del equipo móvil (CB),

dicho método está **caracterizado por el hecho de que** el módulo de abonado (SIM) activo, respectivamente desactiva de manera selectiva al menos un recurso (RES), datos o funciones de dicho módulo de abonado (SIM), utilizando las instrucciones que se encuentran en el criptograma (J), los recursos (RES), datos o funciones necesarios para la obtención de un acceso a la red (NET) del equipo móvil (CB) entran en funcionamiento antes de la llegada del criptograma (J).

2. Método según la reivindicación 1, **caracterizado por el hecho de que** el equipo móvil (CB) es un equipo móvil (CB) de telefonía móvil.

3. Método según la reivindicación 1, **caracterizado por el hecho de que** la red (NET) es una red móvil del tipo GSM, GPRS o UMTS.

4. Método según una de las reivindicaciones 1 a 3, **caracterizado por el hecho de que** el módulo de abonado (SIM) es un módulo de abonado (SIM) insertado en el equipo móvil (CB) de telefonía móvil de tipo tarjeta SIM.

5. Método según una de las reivindicaciones 1 a 4, **caracterizado por el hecho de que** la identificación del conjunto equipo móvil / módulo de abonado (SIM) se efectúa a partir del identificador (IMEISV) del equipo móvil (CB) y del número de identificación del módulo de abonado (IMSI) propio de un abonado a la red (NET) móvil.

6. Método según una de las reivindicaciones 1 a 5, **caracterizado por el hecho de que** los criterios definen límites de utilización de una aplicación (APP) según los riesgos asociados a dicha aplicación (APP) y el tipo y la versión de software del equipo móvil (CB) que el operador y/o el proveedor de aplicaciones (APP) y/o el usuario del equipo móvil (CB) deseen considerar.

7. Método según una de las reivindicaciones 1 a 6, **caracterizado por el hecho de que** se ejecuta después de cada conexión del equipo móvil (CB) a la red (NET).

8. Método según una de las reivindicaciones 1 a 6, **caracterizado por el hecho de que** se ejecuta después de cada actualización de la versión de software del equipo móvil (CB).

9. Método según una de las reivindicaciones 1 a 6, **caracterizado por el hecho de que** se ejecuta después de cada activación o desactivación de una aplicación (APP) en el equipo móvil (CB).

10. Método según una de las reivindicaciones 1 a 6, **caracterizado por el hecho de que** se ejecuta después de cada actualización de la versión de software del módulo de abonado (SIM).

11. Método según una de las reivindicaciones 1 a 6, **caracterizado por el hecho de que** se ejecuta después de cada actualización de recursos (RES) en el módulo de abonado (SIM).

12. Método según una de las reivindicaciones 1 a 6, **caracterizado por el hecho de que** se ejecuta periódicamente a un ritmo dado por el servidor de control (CSE).

13. Método según una de las reivindicaciones 1 a 6, **caracterizado por el hecho de que** se ejecuta después de cada inicio de una aplicación (APP) en el equipo móvil (CB).

14. Método según cualquiera de las reivindicaciones precedentes, **caracterizado por el hecho de que** el módulo de abonado (SIM), previamente al cumplimiento de las instrucciones dadas por el criptograma (J), compara el identificador (IMEISV) del equipo móvil (CB) con el recibido previamente e inicia la operación de verificación solamente si el identificador (IMEISV) ha cambiado.

15. Método según una de las reivindicaciones 1 a 5, **caracterizado por el hecho de que** el servidor de control (CSE), previamente a la transmisión del criptograma (J), compara el identificador (IMEISV) del equipo móvil (CB) con el recibido previamente e inicia la operación de verificación solamente si el identificador (IMEISV) ha cambiado.

16. Método según una de las reivindicaciones 1 a 15, **caracterizado por el hecho de que** el criptograma (J) está constituido por un mensaje encriptado por el servidor de control (CSE) con ayuda de una clave de encriptación asimétrica o simétrica a partir de un conjunto de datos que contiene, entre otros datos, el identificador (IMEISV) del equipo móvil (CB), el número de identificación (IMSI) del módulo de abonado (SIM), referencias de recursos (RES) del módulo de abonado (SIM) y una variable predecible (CPT).

17. Método según una de las reivindicaciones 1 a 16**, caracterizado por el hecho de que** el módulo de abonado (SIM) transmite al servidor de control (CSE), a través del equipo móvil (CB) y la red móvil (NET), un mensaje de confirmación (CF) cuando el módulo de abonado (SIM) ha recibido el criptograma (J), dicho mensaje acredita la buena recepción y el tratamiento adecuado del criptograma (J) por el módulo de abonado (SIM).

18. Método según la reivindicación 1, **caracterizado por el hecho de que** el equipo móvil (CB) es un descodificador de televisión de pago o un ordenador al que está conectado el módulo de abonado (SIM).

19. Módulo de abonado (SIM) que incluye recursos (RES) destinados a ser localmente accedidos por al menos una aplicación (APP) instalada en un equipo móvil (CB) conectado a una red (NET), dicho equipo móvil (CB) incluye medios de lectura y de transmisión de datos que incluyen al menos el identificador (IMEISV) del equipo móvil (CB) y el identificador (IMSI) del módulo de abonado (SIM), dicho módulo de abonado (SIM) comprende medios de recepción y de análisis de un criptograma (J) que comprende instrucciones condicionantes del funcionamiento de la aplicación (APP) según los criterios preestableces por el proveedor de dicha aplicación (APP) y/o el operador y/o el usuario del equipo móvil (CB), el módulo de abonado (SIM) está **caracterizado por el hecho de que** comprende medios de activación, respectivamente de desactivación selectiva de al menos un recurso (RES), datos o funciones, de dicho módulo de abonado (SIM), dichos medios de activación, respectivamente de desactivación selectiva utilizan las instrucciones comprendidas en el criptograma (J), los recursos, datos o funciones necesarios para la obtención de un acceso a la red (NET) del equipo móvil (CB) entran en funcionamiento antes de la llegada del criptograma (J).

20. Módulo de abonado (SIM) según la reivindicación 19, **caracterizado por el hecho de que** constituye un módulo de abonado (SIM) del tipo "tarjeta SIM" conectado a un equipo móvil (CB).

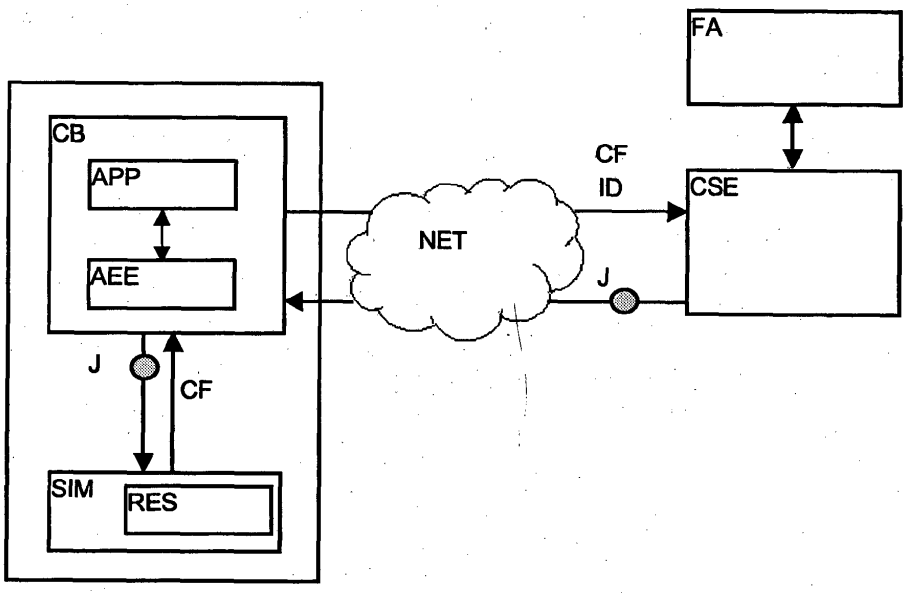

Fig.1

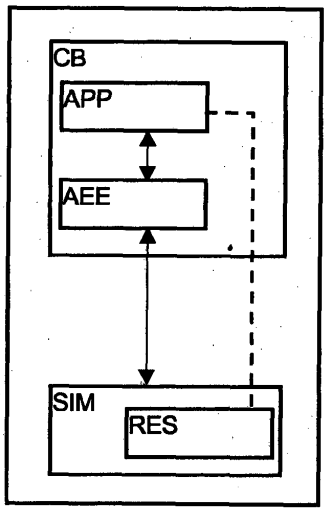

Fig. 2