(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 377 554**

(51) Int. Cl.:
H04W 12/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **03706803 .8**
(96) Fecha de presentación : **11.03.2003**
(97) Número de publicación de la solicitud: **1483930**
(97) Fecha de publicación de la solicitud: **08.12.2004**

(54) Título: **Método de actualización de un algoritmo de autenticación en un sistema informático.**

(30) Prioridad: **11.03.2002 EP 02075996**
07.06.2002 FR 02 07168

(45) Fecha de publicación de la mención BOPI:
28.03.2012

(45) Fecha de la publicación del folleto de la patente:
28.03.2012

(73) Titular/es: **GEMALTO, S.A.**
6, Rue de La Verrerie
92190 Meudon, FR
SCHLUMBERGER MALCO, Inc.

(72) Inventor/es: **Beaudou, Patrice y**
Dubois, Christophe

(74) Agente/Representante:
Isern Cuyas, María Luisa

DESCRIPCIÓN

Método de actualización de un algoritmo de autenticación en un sistema informático.

La presente invención se refiere a la actualización de un algoritmo de autenticación en un sistema informático.

La invención se aplica a un dispositivo cualquiera de tratamiento de datos que almacene un algoritmo de autenticación. La invención se aplica en particular a la tarjeta con chip.

La tarjeta con chip puede conectarse a cualquier sistema ya esté embarcado o no.

La invención se puede emplear en cualquier tipo de red de telecomunicación tal como el sistema de radiocomunicación digital celular de tipo GSM (Global System for Mobile communication), UMTS (Universal Mobile Telecommunication Service), GPRS (General Packet Radio Service), etc.

El ejemplo elegido para ilustrar la invención será él del teléfono móvil conectado a una tarjeta con chip de tipo SIM (Subscriber Identity Module).

Estado de la técnica

La gestión de la itinerancia (roaming en inglés) de un usuario en una red GSM (Global System for Mobile Communication) necesita emplear una identificación específica de este usuario.

El uso de un canal radio hace que las comunicaciones sean vulnerables a las escuchas y utilizaciones fraudulentas. El sistema GSM recurre por lo tanto:

- a la autentificación de cada usuario (o abonado) antes de autorizarle a acceder a un servicio,
- a la utilización de una identidad temporal,
- al cifrado (o encriptación) de las comunicaciones.

El sistema GSM utiliza actualmente cuatro tipos de códigos asociados al abonado:

- El código IMSI (International Mobile Subscriber Identity). Este código es la identidad internacional de un abonado. Esta identidad está inscrita en la tarjeta SIM;
- El código TMSI (Temporary Mobile Subscriber Identity) es una identidad temporal asignada por la red a un teléfono móvil y utilizado después para las transacciones por vía radio;
- El código MSISDN es el número internacional del abonado móvil conforme al plan E164 de la UIT (Unión internacional de Telecomunicaciones) y conocido por el abonado;
- El código MSRN (Mobile Station Roaming Number) es un número asignado temporalmente que permite, mediante una llamada telefónica normal, realizar el encaminamiento hacia un conmutador MSC donde se encuentra el abonado móvil solicitado.

Durante el abono, se asigna una clave Ki al abonado con el código IMSI. Esta pareja IMSI/Ki está almacenada al mismo tiempo en la tarjeta SIM del abonado y fuera de la tarjeta en particular en un centro de autenticación AuC (Authentication Center en inglés). Una pareja va unida íntimamente a uno o varios algoritmos de autenticación.

Recordemos que el centro de autenticación AuC es un centro de autenticación de los abonados de una red GSM. Recordemos, a título informativo, que una autenticación es un proceso que permite a la red comprobar que un abonado tiene autorización para utilizar la red controlando la presencia de una clave secreta en la tarjeta SIM.

Así, el documento US 6.212.372 “enseña la utilización de dos identificadores diferentes para acceder a un mismo servicio, estos identificadores diferentes pudiendo ser activados sucesivamente”.

El documento WO 93/07697 “enseña la utilización de un identificador y de un doble algoritmo de encriptación”.

Se puede almacenar también otra pareja en una segunda base de datos llamada HLR (Home Location Register). Esta base almacena la pareja MSISDN/IMSI asociada a cada abonado, compuesta por el número del abonado MSISDN y la identidad invariante IMSI.

Un problema reside en la puesta al día de un algoritmo almacenado en la tarjeta y en cualquier dispositivo de tratamiento de datos que almacene datos propios de los usuarios (el centro AuC, el registro HLR, la base VLR, etc.) en comunicación con la tarjeta. Dicha actualización requiere entre otras cosas modificar el algoritmo de autenticación de cada pareja IMSI/Ki, y de las parejas MSISDN/Ki, al mismo tiempo dentro de la tarjeta y fuera de la tarjeta en el centro AuC, en el registro VLR, en la base HLR, etc.

Una solución simplista puede consistir en descargar el nuevo algoritmo dentro de la tarjeta y fuera de ella en el centro AuC, en el registro VLR, en la base HLR, etc. Sin embargo, esta solución plantea un problema en términos de seguridad; no es factible transmitir este algoritmo en la red, más cuando este algoritmo es no-propietario.

La invención

Se pretende una actualización securizada de un algoritmo de autenticación.

Para alcanzar este objetivo, la invención se refiere a un proceso de actualización de un algoritmo de autenticación en al menos un dispositivo de tratamiento de datos apto para almacenar en una memoria de dicho dispositivo una identidad de abonado asociada a un algoritmo de autenticación, caracterizado porque comprende las siguientes etapas:

- Una etapa previa de almacenamiento, en una memoria del dispositivo, de un segundo algoritmo de autenticación inactivo.

- Una etapa de vuelco del primer algoritmo hacia el segundo algoritmo (Algo2) apta para inhibir el primer algoritmo y para activar el segundo.

Así, se ve que los algoritmos de autenticación están previamente almacenados en la tarjeta. Ello evita, durante la actualización, que tenga que circular un algoritmo de autenticación para una puesta al día.

La invención se entenderá mejor con la lectura de la descripción que sigue, la cual se da a título de ejemplo y con referencia a los dibujos adjuntos.

En los dibujos

La Figura 1 es una vista de un sistema informático en el que se puede aplicar la invención. En esta figura aparece el estado del sistema informático antes del vuelco de las cuentas.

La Figura 2 representa la misma vista que la Figura 1. En esta figura, el estado del sistema es el que se obtiene tras el vuelco de las cuentas.

Descripción detallada que ilustra la invención

Para simplificar la descripción, los mismos elementos llevan las mismas referencias.

En la Figura 1, para ilustrar la invención, se ha representado una arquitectura que comprende un sistema embarcado tal como un teléfono móvil (no representado) conectado a una tarjeta CARD. En nuestro ejemplo de realización, esta tarjeta es de tipo SIM.

En nuestro ejemplo ilustrado, el sistema embarcado comunica con un dispositivo de tratamiento de datos tal como un servidor SERV por medio de una red de telecomunicaciones RES.

En nuestro ejemplo, un operador OP gestiona las distintas tarjetas repartidas por la red. En particular, el operador administra las cuentas de los distintos abonados. En general, durante la personalización de la tarjeta, el operador asigna una pareja de datos a saber la clave Ki y el código IMSI asociado a al menos un algoritmo de autenticación y los carga en la tarjeta. La tarjeta almacena así una pareja IMSI/Ki para cada abonado. Esta pareja se almacena también en un centro de autenticación AuC.

Para simplificar la ilustración de la invención se ha elegido asociar a cada cuenta un único algoritmo de autenticación. Sin embargo, este ejemplo no es limitativo; varios algoritmos de autenticación podrían haberse asociado a una misma cuenta de abonado.

En nuestro ejemplo ilustrado, se almacena otra pareja MSISDN/IMSI en una base llamada HLR (Home Location Register).

El centro AuC y la base HLR pueden encontrarse indistintamente en un mismo servidor o en dos servidores diferentes. En nuestro ejemplo y con referencia a la Figura 1, se ha elegido almacenarlos en el mismo servidor SERV.

Tal como se ha indicado anteriormente, una actualización de un algoritmo de autenticación no es sencillo.

En nuestro ejemplo de realización, el proceso de actualización conforme a la invención necesita una tarjeta con chip apta para almacenar al menos dos cuentas C1 y C2. La tarjeta almacena una primera cuenta C1 de abonado asociada a al menos un primer algoritmo de autenticación Algo1 (A3A8). Esta primera cuenta se compone de la pareja IMSI1/KM. En nuestro ejemplo ilustrado, la tarjeta almacena también una segunda cuenta C2 asociada al mismo abonado A1 asociado a al menos un segundo algoritmo de autenticación Algo2 (A3A8). Esta segunda cuenta se compone de la pareja IMSI2/KÍ2. La invención no se limita al algoritmo de autenticación A3A8 conocido por el especialista en la técnica sino que puede aplicarse indistintamente a todo tipo de algoritmo de autenticación.

En adelante, en la descripción, cada cuenta C1 y C2 será identificada por su código IMSI1 e IMSI2 respectivamente.

En nuestro ejemplo de realización, las cuentas IMSI1 e IMSI2 son gestionadas por el mismo operador OP. Según otro modo de realización, las cuentas en la tarjeta pueden ser gestionadas por operadores diferentes.

De la misma forma, en nuestro ejemplo, el centro AuC almacena la cuenta IMSI1 asociada al primer algoritmo Algo1 (A3A8) y la cuenta IMSI2 asociada al segundo algoritmo Algo2 (A3A8).

De la misma manera, en nuestro ejemplo, la base HLR almacena la pareja MSISDN/IMSI1 asociada a la primera cuenta y la pareja MSISDN/IMSI2 asociada a la segunda cuenta.

El proceso de puesta al día consiste en volcar la primer cuenta IMSI1 hacia la segunda IMSI2 en la tarjeta con chip, y llegado el caso, en el servidor SERV. En el ejemplo de realización, el servidor SERV está provisto de una funcionalidad que permite almacenar dos cuentas por abonado.

Para ello, antes del vuelco, la cuenta IMSI1 es activa, mientras que la cuenta IMSI2 es inactiva. La Figura 1 es una vista del sistema antes del vuelco de las cuentas. La Figura 2 es una vista del sistema después del vuelco.

En nuestro ejemplo de realización, las etapas de vuelco de las cuentas son las siguientes:

Etapa 1

El operador lanza un comando apto para realizar un vuelco de cuenta. Ventajosamente, este comando es un comando OTA (Over The Air) adecuado para activar una bandera en la tarjeta, teniendo la activación un efecto de vuelco de una cuenta hacia otra cuenta.

Una bandera se puede emplear sencillamente por medio de un bit. Por ejemplo, un bit en el estado 0 significa que la cuenta IMSI1 está inactiva y que la cuenta IMSI2 está activa. A la inversa, un bit en el estado 1 significa que la cuenta IMSI1 está activa y que la cuenta IMSI2 está inactiva.

Etapa 2

La tarjeta CARD recibe el comando y realiza un vuelco de cuenta, desde la cuenta IMSI1 hacia la cuenta IMSI2. En ese momento, en la tarjeta, la primera cuenta IMSI1 se vuelca desde el estado activo hacia el estado inactivo IMSI2 y la segunda cuenta se vuelca desde el estado inactivo hacia el estado activo.

Etapa 3

En nuestro ejemplo, para sincronizar el cambio de estado de las cuentas almacenadas en la tarjeta con las que están almacenadas en el servidor SERV, el teléfono que incluye la tarjeta emite un comando de autenticación hacia el servidor para que éste último efectúe un vuelco de las cuentas. Este comando de autentificación incluye el nuevo código IMSI2. En el servidor, la cuenta activa es la cuenta IMSI1. Cuando el servidor recibe el comando de autenticación, un programa es apto para identificar el nuevo código IMSI2. El servidor SERV realiza entonces un vuelco de algoritmo para garantizar una sincronización de la actualización de los algoritmos de autenticación con la tarjeta CARD.

En el servidor, todas las parejas (MSISDN/IMSI1 e IMSI1/KÍ1) asociadas al primer algoritmo Algo1 (A3A8) se convierten en inactivas mientras que todas las parejas (MSISDN/IMSI2 e IMSI2/KÍ2) asociadas al nuevo algoritmo Algo2 (A3A8) se convierten en activas. Como en la tarjeta, el vuelco se puede realizar activando una bandera.

Etapa 4

En esta fase del proceso, las dos cuentas IMSI1 e IMSI2 se han volcado a la vez en la tarjeta CARD y en el servidor SERV; el algoritmo de autenticación utilizado para la autenticación al mismo tiempo en la tarjeta CARD y en el servidor SERV es a partir de ahora el nuevo algoritmo Algo2 (A3AB).

Las etapas descritas anteriormente corresponden a un ejemplo de realización particular no limitativo. La etapa 3 podría aplicarse de manera diferente:

- Por ejemplo, no hace falta crear dos cuentas IMSI1 e IMSI2. La tarjeta puede almacenar una única cuenta y dos algoritmos de autenticación Algo1 y Algo2. El operador puede simplemente emitir simultáneamente un comando hacia la tarjeta y hacia el servidor para realizar un vuelco del primer algoritmo Algo1 hacia el segundo algoritmo Algo2 en la tarjeta y en el servidor; ventajosamente, se pueden prever claves Ki diferentes para cada algoritmo Algo1 y Algo2.

- O, el operador puede emitir un comando sólo hacia el servidor. En la tarjeta, la cuenta activa sigue siendo la cuenta IMSI1. Posteriormente, cuando el teléfono que incluye la tarjeta intenta autentificarse ante el servidor SERV, éste recibe el código IMSI1 asociado al primer algoritmo Algo1 y se da cuenta de que la cuenta actualmente utilizada en la tarjeta no es la cuenta IMSI2. El servidor lanza por lo tanto un comando apto para realizar un vuelco de las cuentas en la tarjeta. Una vez realizado el vuelco, se puede prever que el teléfono que incluye la tarjeta emita hacia el servidor un mensaje informando que el vuelco se ha realizado correctamente. Al recibo de este mensaje, las cuentas se vuelcan desde la cuenta IMSI1 hacia la cuenta IMSI2 en el servidor. Después del vuelco de las cuentas en el servidor SERV, el servidor pide entonces a la tarjeta que se autentifique con el nuevo algoritmo Algo2 asociado a la nueva cuenta IMSI2.

- O, el operador encargado del vuelco puede descargar en la tarjeta, y eventualmente en el servidor, un programa apto para activarse con retardo por ejemplo según una fecha definida cuya función consiste en realizar un vuelco de una cuenta hacia otra cuenta.

- O, el operador puede delegar también la operación de vuelco en uno o varios agentes inteligentes aptos para realizar el vuelco de las cuentas. Por ejemplo, se podría asignar a cada agente un conjunto de tarjetas. En este ejemplo, el operador transmite un comando a todos o parte de los agentes para que emitan hacia la tarjeta un comando COM que tiene las mismas características que las que se describen anteriormente.

- El vuelco de las cuentas en el servidor se puede realizar de otra forma. La tarjeta se autentifica ante el servidor utilizando el nuevo código IMSI2 asociado al nuevo algoritmo Algo2. Sin embargo, el algoritmo Algo2 utilizado en la tarjeta no es el mismo que el algoritmo activo en el servidor SERV. Por consiguiente, la autenticación fracasa; este fracaso puede servir de desencadenante al vuelco de los algoritmos en el servidor.

En la Etapa 3, el vuelco puede no realizarse inmediatamente. Cuando la bandera está activada, se puede prever que el vuelco efectivo de una cuenta hacia otra sólo se efectúe después de la realización de un evento tal como la reinicialización (Arranque/Parada) de la tarjeta, o durante la ejecución del comando de refrescamiento REFRESCH utilizando por ejemplo un modo entre:

- Reset.

- Full File Change Notification.

- o File Change Notification si la tarjeta contiene un archivo EF(IMSI) que incluye el nuevo código IMSI.

Para más detalles sobre estos modos, nos remitiremos a los textos de las especificaciones ETSI TS 11.14, TS 31.111 y TS 102 223 conocidos por el especialista en la técnica.

Se debe observar que la actualización de un algoritmo de autenticación ocasiona una modificación de las parejas IMSI/KI y MSISDN/IMSI. Una modificación no necesita siempre modificar los dos elementos que constituyen una pareja. Una modificación puede afectar a un único elemento. Por ejemplo, una modificación de un algoritmo puede afectar sólo al elemento IMSI de la pareja IMSI/Ki.

De forma general, la invención se refiere a un proceso que comprende las siguientes etapas:

- Una etapa previa de almacenamiento, en una memoria del dispositivo, de un segundo algoritmo de autenticación (Algo2) inactivo.

- Una etapa de vuelco del primer algoritmo (Algo1) hacia el segundo algoritmo (Algo2), apto para inhibir el primer algoritmo (Algo1) y activar el segundo (Algo2).

Ventajosamente, la etapa de vuelco se realiza por iniciativa de una entidad exterior (OP) a dicho dispositivo. En nuestro ejemplo de realización, esta entidad es un operador OP. En nuestro ejemplo, el operador tiene la operación de vuelco bajo su control.

En nuestro ejemplo, el operador que emite el comando de vuelco es un operador que gestiona una cuenta activa en la tarjeta. Sin embargo, se puede prever que existan arreglos particulares entre operadores autorizándose mutuamente a realizar vuelcos de cuentas en la tarjeta; en este contexto, se puede prever que el operador que emite el comando de vuelco sea el operador de una cuenta inactiva en la tarjeta. De forma más general, la etapa de vuelco es iniciada, preferentemente, por cualquier persona/entidad autorizada para hacerlo.

Preferentemente, la etapa de almacenamiento de los algoritmos se realiza en un lugar seguro, por ejemplo durante la personalización de tarjeta.

El modo de vuelco se puede aplicar de otra forma. Por ejemplo, hemos visto que el operador encargado del vuelco puede descargar en el dispositivo un programa apto para activarse con retardo. Así, el vuelco puede efectuarse al mismo tiempo en la tarjeta, y en cualquier dispositivo afectado por una actualización del algoritmo de autenticación.

Hemos visto que la sincronización de la puesta al día de los algoritmos de autenticación en la tarjeta y en el servidor puede realizarse de distintas formas. Ventajosamente, se almacena una segunda cuenta C2 que incluye un código IMSI2, distinto del código IMSI1, asociado al algoritmo Algo2. Tras la etapa de vuelco de las cuentas en el dispositivo en cuestión, este último transmite el código IMSI2 hacia la totalidad o parte de los dispositivos de tratamiento de datos que necesiten un vuelco de algoritmos. La función de este código IMSI2 consiste en particular a informar a los dispositivos de tratamiento de datos que necesiten un vuelco de algoritmos de que ha tenido lugar un vuelco. Ello asegura una sincronización de la actualización de los algoritmos en el sistema informático. A la recepción del código (IMSI2) asociado al segundo algoritmo (Algo2), dicho dispositivo receptor realiza un vuelco de algoritmo del primer algoritmo (Algo1) hacia el segundo algoritmo (Algo2).

La sincronización puede realizarse de otra forma. Hemos visto también en nuestro ejemplo, que tras el vuelco, dicho dispositivo puede transmitir simplemente un comando hacia otro dispositivo de tratamiento de datos que necesite un vuelco de cuentas.

Ventajosamente, al final del vuelco, se reutiliza el espacio de memoria que almacena los datos asociados a la cuenta desactivada. Por ejemplo, tras el vuelco, los datos asociados a la cuenta desactivada se borran de la memoria. Este borrado libera así espacio en la memoria.

Hemos visto en lo que antecede que, durante la primera etapa, las dos cuentas IMSI1 e IMSI2 creadas en la tarjeta pertenecen al mismo abonado A1. Se debe observar que un abonado puede reunir un grupo de usuarios que utilizan la misma cuenta.

Hemos visto también, en nuestro ejemplo de realización, que el vuelco consiste en desactivar en un primer tiempo la primera cuenta IMSI1 y en activar en un segundo tiempo la segunda cuenta IMSI2.

De ello resulta un dispositivo de tratamiento de datos, en particular una tarjeta con chip, caracterizado porque comprende:

- medios de memoria que almacenan un segundo algoritmo de autenticación (Algo2),
- y porque comprende un microcontrolador programado para realizar, por iniciativa de un operador (OP), una etapa de vuelco del primer algoritmo (Algo1) hacia el segundo algoritmo (Algo2).

La invención se refiere asimismo a un programa de ordenador para un dispositivo de tratamiento de datos, que comprende instrucciones de código para la ejecución de la etapa de vuelco definida anteriormente.

Finalmente, la invención se refiere a un programa de ordenador para un dispositivo de tratamiento de datos, que comprende instrucciones de códigos para, después de la etapa de vuelco del primer algoritmo hacia el segundo, identificar el algoritmo utilizado por un dispositivo emisor con el código (IMSI2) recibido de dicho dispositivo emisor.

Nos damos cuenta de que la invención ofrece numerosas ventajas:

Se reduce mucho el coste en tiempo de tal aplicación. En efecto, la tarjeta se vende con los dos algoritmos. Un primer algoritmo para una utilización corriente; y un segundo algoritmo para una futura utilización. El operador mismo elige el momento deseado para realizar la migración. Un simple comando permite efectuar el vuelco hacia un número elegido de tarjetas con chip. El operador por lo tanto tiene la posibilidad, si así lo desea, de realizar una migración a la unidad es decir una tarjeta tras otra.

Hemos visto también que una vez realizado el vuelco y que el nuevo algoritmo Algo2 está activo, la cuenta asociada al antiguo algoritmo Algo1 puede borrarse liberando así espacio en la memoria. Esta liberación de espacio en la memoria, en particular en la tarjeta con chip, es una ventaja importante considerando los imperativos materiales extremos en términos de memoria.

La invención permite no sustituir todas las tarjetas actualmente utilizadas por nuevas tarjetas que almacenan la nueva versión del algoritmo de autenticación.

La invención permite evitar la asignación de un nuevo número de teléfono a cada abonado cuya pareja IMSI/Ki necesita ser almacenada en un nuevo centro de autenticación AuC; el usuario conserva entonces la misma tarjeta, el mismo número de teléfono en todos los casos hipotéticos.

La invención permite que el operador evita gastos financieros considerables. Se observa que la invención es interesante para el operador ya que éste utiliza un único centro de autenticación para poner al día los algoritmos de autenticación. El operador no se ve obligado a comprar nuevos equipos para realizar la migración. El precio de tal aplicación una vez más es muy reducido.

REIVINDICACIONES

1. Proceso de actualización de un algoritmo de autenticación en al menos un dispositivo de tratamiento de datos (CARD, SERV) apto para almacenar en una memoria de dicho dispositivo (CARD, SERV) una identidad de abonado (IMSI1) asociada a un algoritmo de autenticación (Algo1), **caracterizado** porque comprende las siguientes etapas:

- Una etapa previa de almacenamiento, en una memoria del dispositivo, de un segundo algoritmo de autenticación (Algo2) inactivo, asociado a un segundo código IMSI2, distinto de la identidad de abonado IMSI1.

- Una etapa de vuelco del primer algoritmo (Algo1) hacia el segundo algoritmo (Algo2) apta para inhibir el primer algoritmo (Algo1) y para activar el segundo (Algo2).

2. Proceso según la reivindicación 1, **caracterizado** porque la etapa de vuelco se realiza por iniciativa de una entidad exterior (OP) a dicho dispositivo.

3. Proceso según la reivindicación 1 ó 2, **caracterizado** porque, para realizar la operación de vuelco, la entidad exterior a dicho dispositivo (OP) transmite un comando (COM) a distancia hacia dicho dispositivo (CARD) para realizar el vuelco del primer algoritmo (Algo1) hacia el segundo algoritmo (Algo2).

4. Proceso según la reivindicación 1 ó 2, **caracterizado** porque para realizar la operación de vuelco, la entidad exterior a dicho dispositivo descarga en el dispositivo un programa apto para activarse con retardo, cuya función consiste en realizar un vuelco del primer algoritmo (Algo1) hacia el segundo algoritmo (Algo2).

5. Proceso según la reivindicación 1, **caracterizado** porque, durante la etapa previa de almacenamiento, se almacena un segundo código IMSI2, distinto del código IMSI1 y asociado al algoritmo Algo2, y porque después de la etapa de vuelco de las cuentas en dicho dispositivo (CARD), dicho dispositivo transmite el código IMSI2 hacia la totalidad o parte de los dispositivos de tratamiento de datos (SERV) que necesiten un vuelco de algoritmos, dicho código (IMSI2) asociado al segundo algoritmo informando a estos últimos del vuelco de algoritmo para asegurar una sincronización de la actualización de los algoritmos.

6. Proceso según la reivindicación 5, **caracterizado** porque a la recepción del código (IMSI2) asociado al segundo algoritmo (Algo2), dicho dispositivo receptor realiza un vuelco de algoritmo del primer algoritmo (Algo1) hacia el segundo algoritmo (Algo2).

7. Proceso según la reivindicación 1, **caracterizado** porque al final del vuelco, se reutiliza el espacio de memoria que almacena los datos asociados a la cuenta desactivada.

8. Dispositivo de tratamiento de datos, en particular una tarjeta con chip, apto para almacenar una identidad de abonado (IMSI1) y asociado a un algoritmo de autenticación (Algo1), **caracterizado** porque comprende:

- medios de memoria que almacenan un segundo algoritmo de autenticación (Algo2), asociado a un segundo código IMSI2, distinto de la identidad de abonado IMSI1,

- y porque comprende un microcontrolador programado para realizar, una etapa de vuelco del primer algoritmo (Algo1) hacia el segundo algoritmo (Algo2) apto para inhibir el primer algoritmo (Algo1) y para activar el segundo (Algo 2).

9. Programa de ordenador almacenado en un dispositivo de tratamiento de datos, que comprende instrucciones de código para la ejecución de la etapa de vuelco definida en la reivindicación 1 cuando se ejecuta en el dispositivo de tratamiento de datos.

10. Programa de ordenador almacenado en un dispositivo de tratamiento de datos, que comprende instrucciones de códigos para, después de la etapa de vuelco del primer algoritmo hacia el segundo tal como se define en la reivindicación 1, identificar el algoritmo utilizado por un dispositivo emisor con el código (IMSI2), tal como se define en la reivindicación 5, recibido de dicho dispositivo emisor cuando es ejecutado en el dispositivo de tratamiento de datos.

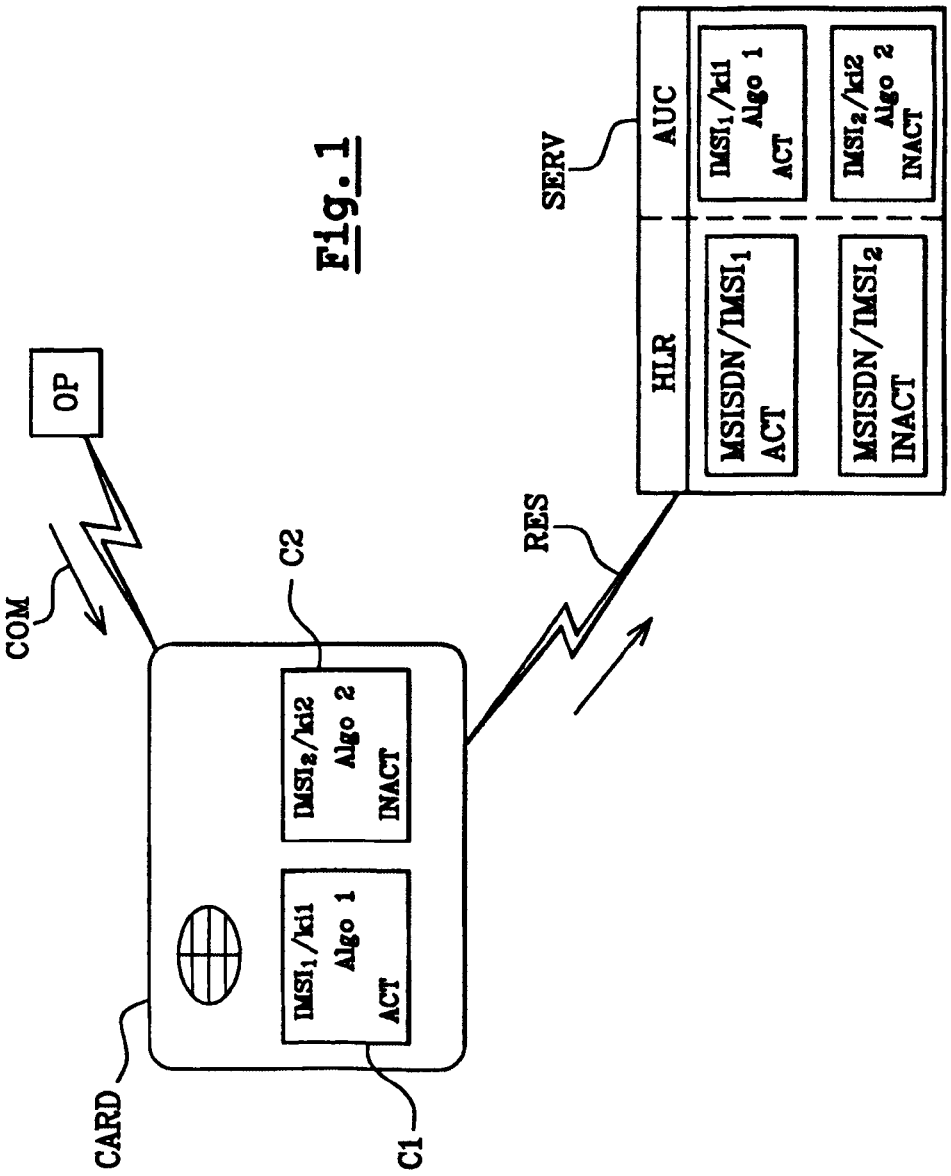
OP
COM
C2
RES
SERV
AUC
HLR
IMSI1/ki1
Algo 1
ACT
IMSI2/ki2
Algo 2
INACT
MSISDN/IMSI1
ACT
MSISDN/IMSI2
INACT
CARD
C1

Fig.1

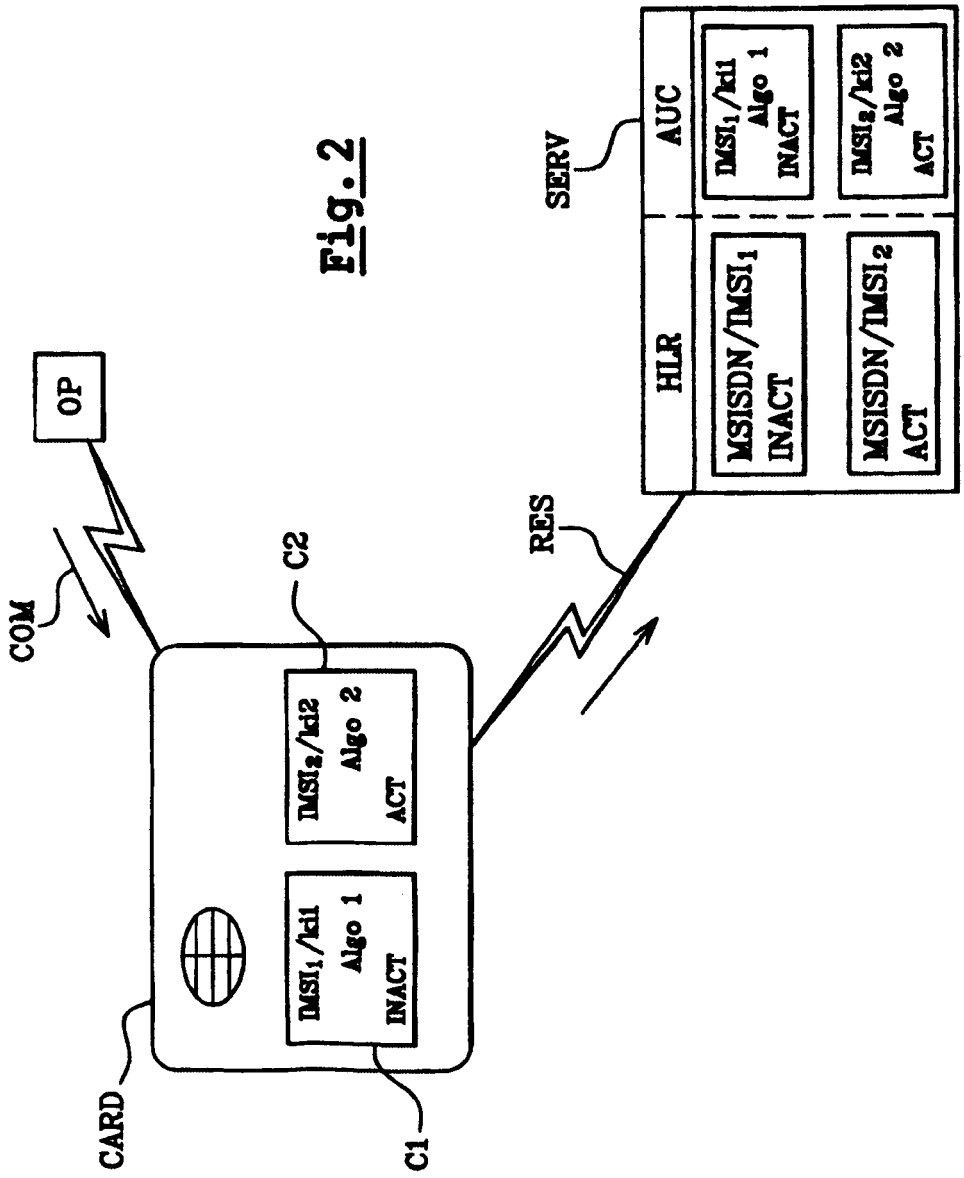
OP
COM
CARD
C1
C2
IMSI1/ki1
Algo 1
INACT
IMSI2/ki2
Algo 2
ACT
RES
SERV
AUC
HLR
IMSI1/ki1
Algo 1
INACT
IMSI2/ki2
Algo 2
ACT
MSISDN/IMSI1
INACT
MSISDN/IMSI2
ACT

Fig.2