(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 436 426**

(51) Int. CI.:

G06Q 20/32 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **03.10.2008 E 08807869 (6)**

(97) Fecha y número de publicación de la concesión europea: **11.09.2013 EP 2195769**

(54) Título: **Método basado en una tarjeta SIM para la realización de servicios con altas características de seguridad**

(30) Prioridad:

03.10.2007 EP 07117829

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.01.2014

(73) Titular/es:

POSTEMOBILE S.P.A. (100.0%)
Viale Europa 175
00144 Rome, IT

(72) Inventor/es:

FUCCI, FRANCESCO y
GIACCHI, ROBERTO

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Método basado en una tarjeta SIM para la realización de servicios con altas características de seguridad

La presente invención se refiere a un método para ejecutar transacciones seguras y de altas prestaciones bancarias, económicas, financieras y postales a través de un terminal telefónico móvil que comunica a través del aire con mensajes cifrados. La invención también se refiere a una tarjeta SIM y a un sistema capaz de implementar el método. La tarjeta SIM de la invención se inserta en el teléfono móvil y permite la comunicación usando las redes de GSM y UMTS, completamente extendidas sobre casi toda la superficie terrestre. El método de la invención posibilita la realización de servicios financieros, bancarios y postales, denominados en adelante en este documento como " VAS distintivo - Servicios de Valor Añadido" y ejemplificados a continuación en este documento en una lista no exhaustiva:

- recargar el crédito del teléfono prepago cargando a un instrumento de pago asociado (por ejemplo, tarjeta de crédito prepago, tarjeta de crédito post-pago, cuenta corriente o carta de pago postal).
- recargar el crédito del teléfono prepago de otro beneficiario cargando a un instrumento de pago asociado con el solicitante (por ejemplo, tarjeta de crédito prepago, tarjeta de crédito post-pago, cuenta corriente o carta de pago postal).
- petición de información acerca del balance de cuentas y lista de transacciones para un instrumento de pago tal como una tarjeta de crédito prepago y post-pago o una cuenta bancaria.
- transferencia de efectivo entre sus propios instrumentos de pago (por ejemplo, tarjeta de crédito prepago, tarjeta de crédito pos-pago o cuenta bancaria).
- transferencia de efectivo a otra organización financiera (por ejemplo, otro banco, diferente del asociado con los instrumentos de pago);
- pago de facturas con cartas de pago postal usando un instrumento de pago (por ejemplo, tarjeta de crédito pre-pago, tarjeta de crédito post-pago o cuenta bancaria);
- petición de servicios postales cargados a un instrumento de pago (por ejemplo el crédito prepago de la SIM, factura post-pago del teléfono, tarjeta de crédito pre-pago, tarjeta de crédito post-pago, cuenta bancaria o carta de pago postal). Ejemplos de servicios postales son: telegramas, seguimiento de entregas, tarjetas postales MMS y tickets SMS;
- micro-pagos y pagos electrónicos de objetos de consumo, con respecto a los suministradores de servicios y productos asociados, cargados a un instrumento de pago (por ejemplo, tarjeta de crédito prepago, tarjeta de crédito post-pago o cuenta bancaria).

El documento US 2005/0277432 se refiere a una SIM que tiene memoria, un procesador y la capacidad de interactuar con el usuario. La SIM tiene una aplicación de Intérprete Dinámico que extiende la funcionalidad de una aplicación STK (estructura de herramienta de SIM) posibilitando a un operador de red móvil para añadir menús dinámicos para una aplicación STK sobre el dispositivo de usuario. En consecuencia el desarrollador de una aplicación es capaz de optimizar el funcionamiento de una aplicación de STK dividiendo el almacenamiento de datos usados para ofrecer un menú sobre el dispositivo de usuario entre la SIM y el servidor de la aplicación dinámica sobre la red.

La comunicación "*…and Turks with mobile signature programme*" *Card Technology Today, abril de 2007* se refiere a una solución de identificación basada en la SIM para para implementar un programa de firma de móvil a gran escala, permitiendo a los usuarios realizar transacciones en línea seguras a través de su teléfono, en cualquier momento, en cualquier parte. La tarjeta SIM comprueba el código secreto, crea la firma digital y la envía al destinatario, por ejemplo el banco para posibilitar la transacción correspondiente sobre el banco de la cuenta bancaria. La tarjeta SIM crea las claves secretas por si misma cuando se realiza una petición de activación por el operador.

El método de la invención y la tarjeta SIM relacionada pueden garantizar para cada VAS distintivo los cinco requisitos de seguridad esenciales de una transacción financiera:

1. Privacidad: garantiza que el contenido y significado de la comunicación no se divulga a personas no autorizadas;
2. Integridad: asegura la detección por el receptor de cualquier interferencia con el mensaje original generado por el usuario;
3. Autenticación: asegura que todas las partes involucradas en una comunicación se reconocen con certeza;
4. Autorización: garantiza que la persona que solicita la realización de una operación está autorizada para hacerla dentro del contexto específico;
5. No denegación: garantiza que, una vez realizado un servicio, en particular una transacción, ni el receptor ni el usuario pueden denegar haber tomado parte en la misma. La memoria de la tarjeta SIM se divide en dos áreas lógicas reservadas para almacenar las aplicaciones de seguridad que implementan una combinación de algoritmos de huella electrónica, algoritmos de criptografía simétricos y asimétricos y algoritmos para la inicialización y memorización de claves de cifrado (proceso de claves incorporado). Además de este nivel de seguridad, dirigido al aseguramiento de la transferencia de datos, se ha creado un grado adicional de seguridad para acceder y autenticar las transacciones financieras usando un PIN de usuario gestionado con otros

algoritmos de seguridad.

El conjunto y la combinación de estas aplicaciones técnicas, desarrolladas directamente en la tarjeta SIM en la etapa de fabricación permiten realizar servicios con un acceso simple y seguro.

La invención actual proporciona un instrumento capaz de realizar funciones que siguen siendo hasta la fecha específicas de los sistemas bancarios y/o postales.

El método de la invención permite a un usuario registrado realizar operaciones y solicitar servicios bancarios y financieros de forma confortable y segura desde su terminal móvil.

La tarjeta SIM del método de la presente invención, además de las funciones usuales (llamadas telefónicas, intercambio de mensajes, WAP y navegación de Internet) permite funciones bancarias / financieras que hasta la fecha implican la presencia física del usuario en una oficina postal, en un banco o delante de un terminal de ordenador conectado a la Internet. Cualquiera que tenga un terminal móvil de la segunda o tercera generación, una suscripción telefónica con el operador de la tarjeta SIM y un instrumento de pago (por ejemplo, una tarjeta de crédito prepago o post-pago, cuenta bancaria asociada con la tarjeta SIM) puede realizar operaciones financieras en cualquier momento, en un modo seguro y con unas pocas y simples etapas, enviando mensajes cifrados.

La memoria de la tarjeta SIM está básicamente dividida en dos áreas:

a) un área primera dedicada a la red, gestionada con seguridad por el operador de telefonía móvil y ocupada por el sistema operativo y por la estructura del sistema de ficheros, por el área de sistema necesaria para las comunicaciones de voz y SMS, por la agenda del teléfono y por los mismos mensajes de texto SMS.
b) un área segunda dedicada a albergar el "VAS distintivo", como componentes esenciales: los algoritmos de seguridad, el código de los Servicios de Valor Añadido distintivo (VAS), y la herramienta dinámica de SIM (DSTK). La DSTK asegura una actualización dinámica de los servicios VAS para cada cliente transfiriendo la lógica de aplicación a demanda desde un componente servidor dedicado y remoto llamado Plataforma del Servidor Sobre el Aire (OTA), véase también a continuación.

El método de la invención implementa las siguientes funciones para la gestión de la seguridad: generación dinámica de claves asimétricas; creación, modificación y verificación del PMPIN; cifrado y descifrado de las transferencias de datos; firma digital. Un objeto de la invención es un método para la realización de servicios de valor añadido VAS con un nivel muy alto de seguridad por medio de la comunicación por un complemento sobre una tarjeta SIM, teniendo dicha tarjeta SIM una memoria M dividida en dos áreas independientes, una para gestionar los servicios de telefonía básica y la otra para almacenamiento seguro y aseguramiento de los datos propietarios, posibilitando la aplicación de cifrado para un VAS, tales áreas son:

a) un área primera dedicada a la red, gestionada en un modo seguro también con respecto al operador de telefonía móvil y ocupada por el sistema operativo y por la estructura del sistema de ficheros, por el área de sistema necesario para las comunicaciones de voz y SMS, por la agenda del teléfono y por los mismos mensajes de texto SMS.
b) un área segunda dedicada a albergar los VAS, que tiene como componentes esenciales: el complemento para la realización de los algoritmos de seguridad, que son una combinación de algoritmos de huella electrónica, algoritmos de criptografía simétrica y asimétrica y algoritmos para la inicialización y memorización de las claves de cifrado; el código de los servicios de valor añadido VAS, un código de verificación como un prueba de posesión POP, una herramienta de SIM dinámica DSTK; comprendiendo dicho método las siguientes fases:

a) inicialización de un sistema de cifrado en una primera vía de acceso:

i) entrada de un código de verificación PoP como una prueba de posesión, emitido durante la compra de dicha tarjeta SIM;
ii) generación de un código PIN de órdenes a asociar con cada servicio confidencial con respecto al sistema central;
iii) generación, directamente sobre la tarjeta SIM, de un par de claves asimétricas, una privada y una pública, a usar para una firma digital;
iv) envío de la clave pública a través de un mensaje de cifrado a una autoridad de certificación CA, para crear un certificado digital a archivar y usar para todas las comunicaciones posteriores;

b) uso del sistema de cifrado para el envío de mensajes con relación a los servicios mediante:

i) petición del servicio navegando por el menú de servicios sobre la tarjeta SIM e introducción de los datos y la información necesaria para el funcionamiento;
ii) introducción del PIN de órdenes para autorizar el servicio;
iii) producción de un resumen del mensaje mediante un algoritmo de huella electrónica;

iv) firma de dicho resumen a través de un algoritmo asimétrico;
v) cifrado de la firma digital y del mensaje inicial a través de un algoritmo AES;
vi) envío del mensaje cifrado a través de mensajes de texto SMS binarios y a través de una plataforma de comunicación OTA de la petición de servicio a los sistemas centrales;
vii) descifrado del mensaje de texto SMS mediante una llamada a la CA para la validación del usuario y la corrección del mensaje y la réplica posterior desde la CA para la autorización de la realización del servicio.

El par de claves asimétricas es preferiblemente de 1024 bit.

El mensaje cifrado que contiene la clave pública y la petición de certificado está preferiblemente en la normativa de seguridad PKCS Nº 10.

El resumen del mensaje se produce preferiblemente por medio de un algoritmo de huella digital SHA-1.

El resumen se firma preferiblemente por medio de un algoritmo asimétrico RSA con una clave de 1024 bits.

La firma digital y el mensaje inicial se cifran preferiblemente por medio de un algoritmo AES de clave asimétrica, más preferiblemente de 128 bits.

El método permite ventajosamente la flexibilidad y diferenciación del nivel de seguridad como una función del servicio solicitado, permitiendo la asociación del nivel de seguridad más apropiado como una función del secreto, la confidencialidad y el valor financiero.

De hecho, además del criterio de seguridad usado para la transmisión de los datos que posibilita los servicios de seguridad a realizar, el sistema tiene un nivel de seguridad adicional para acceder a los servicios por el usuario. Esto se obtiene gestionando sobre la tarjeta SIM un código PIN específico adicional para autorizar los servicios (PMPIN), usado tanto para lanzar los mecanismos de la firma electrónica como el cifrado de los datos y para poder solicitar y confirmar las operaciones de órdenes sobre el instrumento de pago.

Por lo tanto es posible fijar en las especificaciones de seguridad un nivel único y un nivel doble: el nivel doble requiere la introducción del PMPIN dos veces durante algunas iteraciones de servicios de petición / respuesta, por ejemplo las transacciones (fase de petición y fase de confirmación de la transacción); el nivel único requiere la introducción del PMPIN una vez (fase de confirmación).

La presente invención se describirá por medio de ejemplos no limitativos.

Descripción de los dibujos

Fig. 1 - diagrama del proceso de generación de la tarjeta SIM.
Fig. 2 - representación esquemática del mecanismo del primer acceso al VAS distintivo.
Fig. 3 - diagrama de la gestión de seguridad en las comunicaciones.
Fig. 4 - diagrama de comunicaciones en el servicio de micro-pagos.
Fig. 5 - diagrama de uso del VAS distintivo.

Macroprocesos de generación de la tarjeta SIM y activación de los servicios

1) Producción de la tarjeta SIM

La primera fase del proceso es la de la generación de las tarjetas SIM sobre la que están presentes los siguientes:

- una clave simétrica específica para cada SIM, asociada con su ICCID (ID de la tarjeta del circuito integrado), una clave obtenida con un algoritmo certificado en un modo seudoaleatorio para asegurar la imposibilidad de regeneración de la secuencia de claves generadas;
- un código de verificación PoP (prueba de posesión), usado solo para el primer acceso, para garantizar que el primer usuario que crea el PMPIN es la persona que ha comprado la SIM y que conoce el código secreto inicial recibido con el empaquetado de la misma SIM.

2) Envío de códigos

Como se ha mencionado anteriormente, el algoritmo para el cálculo aleatorio de las claves también se certifica (de acuerdo con la normativa FIPS 140). Sobre la base de la norma, el vendedor de la SIM (vendedor de la SIM) genera una clave simétrica para cada SIM producida y crea un fichero de salida con las correspondencias de claves simétricas - ICCID. El fichero de salida contiene internamente las claves simétricas en una forma cifrada (por medio de un conjunto predefinido de otras claves simétricas usadas exclusivamente para este propósito) y se envía, a través de una comunicación cifrada, a la CA para cada lote de producción.

Una vez recibido, la CA procesa el fichero y mantiene la asociación dentro de sus sistemas (a su vez certificados y asegurados) para todas las tarjetas SIM producidas con objeto de usar las claves simétricas de las tarjetas SIM durante el cifrado, el descifrado y la verificación de la firma digital de una SIM específica (ICCID), como apoyo para el suministro de servicios.

El proceso de generación de la tarjeta SIM se ilustra en la Figura 1.

3) Primer acceso

En la activación de red de la SIM, el portafolio de los servicios bancarios y postales se configura (en remoto y a través de la OTA) de acuerdo con el perfil de usuario.

En el primer acceso a uno de estos servicios, el usuario, después de haber introducido la PoP, se guía durante la generación del PIN de órdenes PMPIN y el proceso de generación de las claves simétricas se lanza a continuación a través del mecanismo sobre la SIM de la GeneraciónClaveIncorporada (OBKG). Se solicitará el PMPIN para autorizar todos los servicios bancarios y financieros que están relacionados con un instrumento de pago.

Después de la verificación del PMPIN, la SIM cifra, firma y envía la información para las comunicaciones de seguridad, a los sistemas finales del proveedor de los servicios bancarios y postales. La información de seguridad enviada por la aplicación sobre la SIM es:

- la clave pública del cliente, clave transferida a través de la normativa PKCS Nº 10
- el identificador específico de la SIM (ICCID).

La Figura 2 es una representación esquemática de lo que se describe.

4) Uso de los servicios

Posteriormente a la creación de la SIM y la activación de los servicios bancarios y postales, la comunicación entre el terminal y los extremos de salida del proveedor tiene lugar a través de mensajes de texto SMS firmados y cifrados.

Antes de la comunicación se realizan las dos fases siguientes sucesivas:

1. Firma electrónica con la clave privada de usuario siguiendo la introducción del PMPIN.
2. Cifrado del texto con la clave de criptografía simétrica asociada con el usuario.

Del mismo modo la comunicación de respuesta entre los sistemas finales del proveedor del servicio y el terminal se basa en el mismo mecanismo. En este caso, el cifrado de la comunicación involucra el cifrado del texto con la clave simétrica asociada con la SIM, garantizando que la información sensible sobre el resultado de los servicios, en particular las transacciones son confidenciales y accesibles solamente por el usuario de la SIM.

La Figura 3 es una representación esquemática de la gestión de la seguridad de las comunicaciones.

Ejemplo de uso de una VAS distintiva

La Figura 4 es un diagrama de las comunicaciones en el servicio de micro-pagos.

Se decidió analizar el servicio de transferencias de efectivo entre instrumentos de pago (por ejemplo la tarjeta de crédito post-pago y prepago). El servicio consiste de una transferencia de efectivo desde la tarjeta de un pagador a la tarjeta de un beneficiario, identificado por el número de teléfono móvil.

Las sencillas etapas que tiene que realizar el pagador para llevar a cabo la operación indicada son las siguientes:

1. seleccionar el servicio introduciendo el menú de la SIM;
2. teclear la cantidad a pagar;
3. introducir el número de teléfono del beneficiario, obteniéndolo también desde la agenda del teléfono.
4. introducir el PMPIN.

El pagador y el beneficiario reciben un mensaje que indica el resultado de la operación.

Después de introducir el PMPIN durante la confirmación (punto 4), se solicitan los algoritmos del complemento de seguridad, sobre la tarjeta SIM, que permiten la firma digital y el cifrado del mensaje.

La Figura 5 ilustra el proceso como se describe a continuación:

1. se firma el mensaje y se cifra siguiendo la llamada al complemento de seguridad sobre el terminal móvil;

2. el mensaje se envía a la plataforma del proveedor del VAS distintivo (en este ejemplo el Servicio Postal Móvil);
3. el proveedor del VAS distintivo reconoce una petición del servicio distintivo y lo redirige a la CA (en este ejemplo el Servicio Postal Italiano) para su descifrado y verificación de la firma digital;
4. posteriormente el mensaje se descifra; una vez descifrado el mensaje se redirige a los sistemas de pago para su verificación y el cálculo del coste de la operación;
5. se devuelve un mensaje de confirmación que contiene toda la información solicitada;
6. la respuesta se cifra una vez de nuevo una vez y se devuelve al usuario

La Figura 5 no muestra el flujo inverso, este flujo repite las etapas del flujo directo.

La intención es subrayar cómo la comunicación entre los diversos componentes del sistema permanece en cualquier caso transparente al usuario que simplemente tiene que elegir el beneficiario, el tipo de VAS distintivo que desea usar, posiblemente la suma a pagar y enviar el mensaje. Como consecuencia de estas acciones el usuario recibirá sobre su propio terminal un mensaje de confirmación que contiene el código de la operación realizada por el mismo. En el caso de una transacción financiera también se envía un mensaje adicional de notificación del crédito de la cuenta corriente al beneficiario de la transferencia.

REIVINDICACIONES

1. Método para la realización de servicios de valor añadido VAS con un nivel muy alto de seguridad por medio de comunicación por el complemento sobre una tarjeta SIM, teniendo dicha tarjeta SIM una memoria M dividida en dos áreas independientes, una para la gestión de los servicios de telefonía básica y otra para el almacenamiento seguro y aseguramiento de datos propietarios, posibilitando la aplicación de cifrado para un VAS, tales áreas son:

a) un área primera dedicada a la red, gestionada en un modo seguro también con respecto al operador de telefonía móvil y ocupada por el sistema operativo y por la estructura del sistema de ficheros, por el área de sistema necesaria para las comunicaciones de voz y SMS, por la agenda del teléfono y por los mismos mensajes de texto SMS.
b) un área segunda dedicada a albergar los VAS, que tiene como componentes esenciales: el complemento para la realización de los algoritmos de seguridad, que son una combinación de algoritmos de huella electrónica, algoritmos de criptografía simétrica y asimétrica y algoritmos para la inicialización y memorización de las claves de cifrado; el código de los servicios de valor añadido (VAS); un código de verificación como un prueba de posesión POP, una herramienta de SIM dinámica DSTK; comprendiendo dicho método las siguientes fases:

a) inicialización de un sistema de cifrado en un primer acceso por medio de:

i) entrada de un código de verificación como una prueba de posesión PoP, emitido durante la compra de dicha tarjeta SIM;
ii) generación de un código PIN de órdenes a asociar con cada uno de los servicios confidenciales con respecto al sistema central;
iii) generación, directamente sobre la tarjeta SIM, de un par de claves asimétricas, una privada y una pública, a usar para la firma digital;
iv) envío de la clave pública a través de un mensaje cifrado a una autoridad de certificación (CA), para crear un certificado digital a archivar y usar para todas las comunicaciones posteriores;

b) uso del sistema de cifrado para el envío de mensajes relativos a los servicios por medio de:

i) petición del servicio navegando por el menú de servicios sobre la tarjeta SIM e introducción de los datos y la información requerida para el funcionamiento;
ii) introducción del PIN de órdenes para autorizar el servicio;
iii) producción de un resumen del mensaje mediante un algoritmo de huella electrónica;
iv) firma de dicho resumen por medio de un algoritmo asimétrico;
v) cifrado de la firma digital y del mensaje inicial por medio de un algoritmo AES;
vi) envío del mensaje cifrado a través de mensajes de texto SMS binarios y por medio de la plataforma de comunicación OTA de la petición de servicio al sistema central;
vii) descifrado del mensaje de texto SMS mediante una llamada a la CA para la validación del usuario y de la corrección del mensaje y la respuesta posterior desde la CA para la autorización de la realización del servicio.

2. Método de acuerdo con la reivindicación 1 en el que el par de claves asimétricas es de 1024 bit.

3. Método de acuerdo con la reivindicación 1 o 2, en el que el mensaje cifrado de la clave pública está en la normativa de seguridad PKCS Nº 10.

4. Método de acuerdo con una de las reivindicaciones 1 a 3 en el que el resumen del mensaje se produce por medio de un algoritmo de huella electrónica SHA - 1.

5. Método de acuerdo con una de las reivindicaciones 1 a 4 en el que el resumen se firma por medio de un algoritmo asimétrico de RSA con una clave de 1024 bits.

6. Método de acuerdo con una de las reivindicaciones 1 a 5 en el que el cifrado de la firma digital y del mensaje inicial tiene lugar a través de un algoritmo AES de clave simétrica.

7. Método de acuerdo con la reivindicación 6, en el que el algoritmo AES de clave simétrica es de 128 bits.

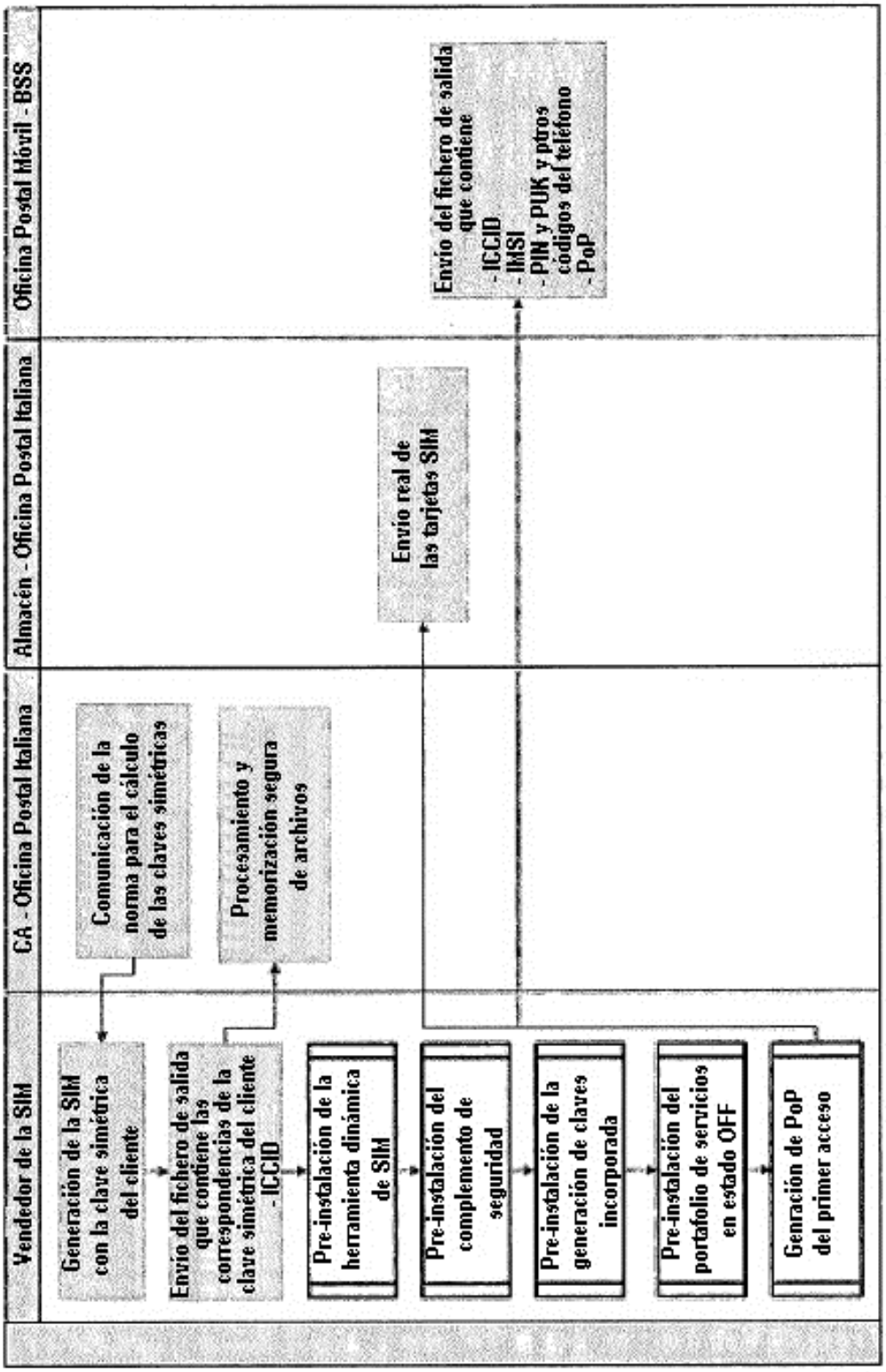
Vendedor de la SIM
CA - Oficina Postal Italiana
Almacén - Oficina Postal Italiana
Oficina Postal Móvil - BSS
Generación de la SIM con la clave simétrica del cliente
Comunicación de la norma para el cálculo de las claves simétricas
Envío del fichero de salida que contiene las correspondencias de la clave simétrica del cliente - ICCID
Procesamiento y memorización segura de archivos
Pre-instalación de la herramienta dinámica de SIM
Envío real de las tarjetas SIM
Envío del fichero de salida que contiene
- ICCID
- IMSI
- PIN y PUK y ptros códigos del teléfono
- PoP
Pre-instalación del complemento de seguridad
Pre-instalación de la generación de claves incorporada
Pre-instalación del portafolio de servicios en estado OFF
Genración de PoP del primer acceso

Fig. 1

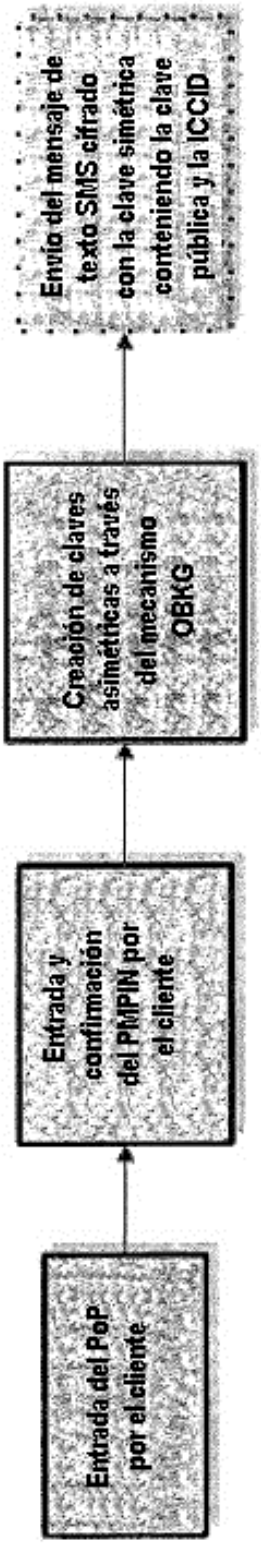
Entrada del PoP por el cliente
Entrada y confirmación del PMPIN por el cliente
Creación de claves asimétricas a través del mecanismo OBKG
Envío del mensaje de texto SMS cifrado con la clave simétrica conteniendo la clave pública y la ICCID

Fig. 2

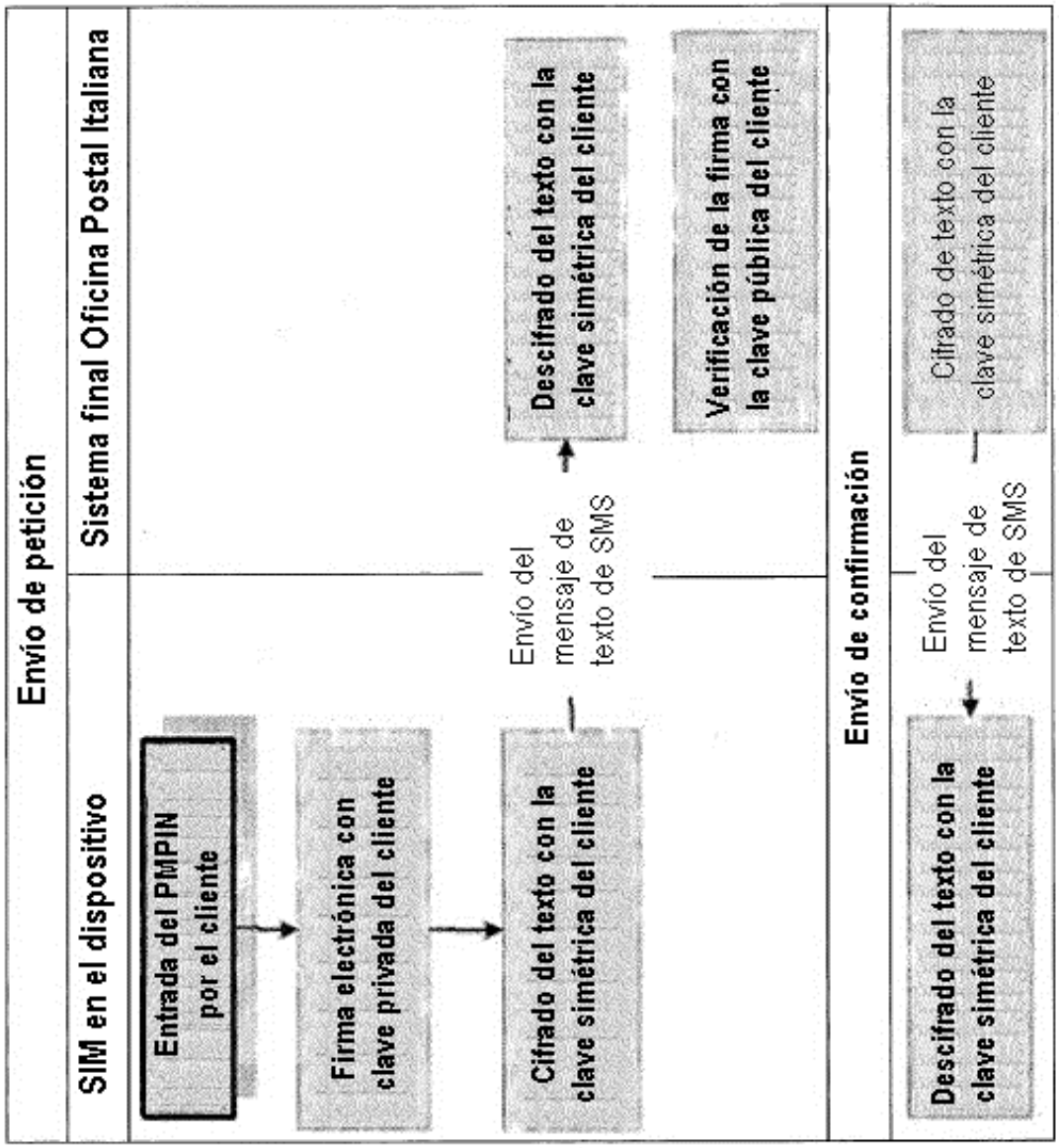
Envío de petición
SIM en el dispositivo
Sistema final Oficina Postal Italiana
Entrada del PMPIN por el cliente
Firma electrónica con clave privada del cliente
Cifrado del texto con la clave simétrica del cliente
Envío del mensaje de texto de SMS
Descifrado del texto con la clave simétrica del cliente
Verificación de la firma con la clave pública del cliente
Envío de confirmación
Descifrado del texto con la clave simétrica del cliente
Envío del mensaje de texto de SMS
Cifrado de texto con la clave simétrica del cliente

Fig. 3

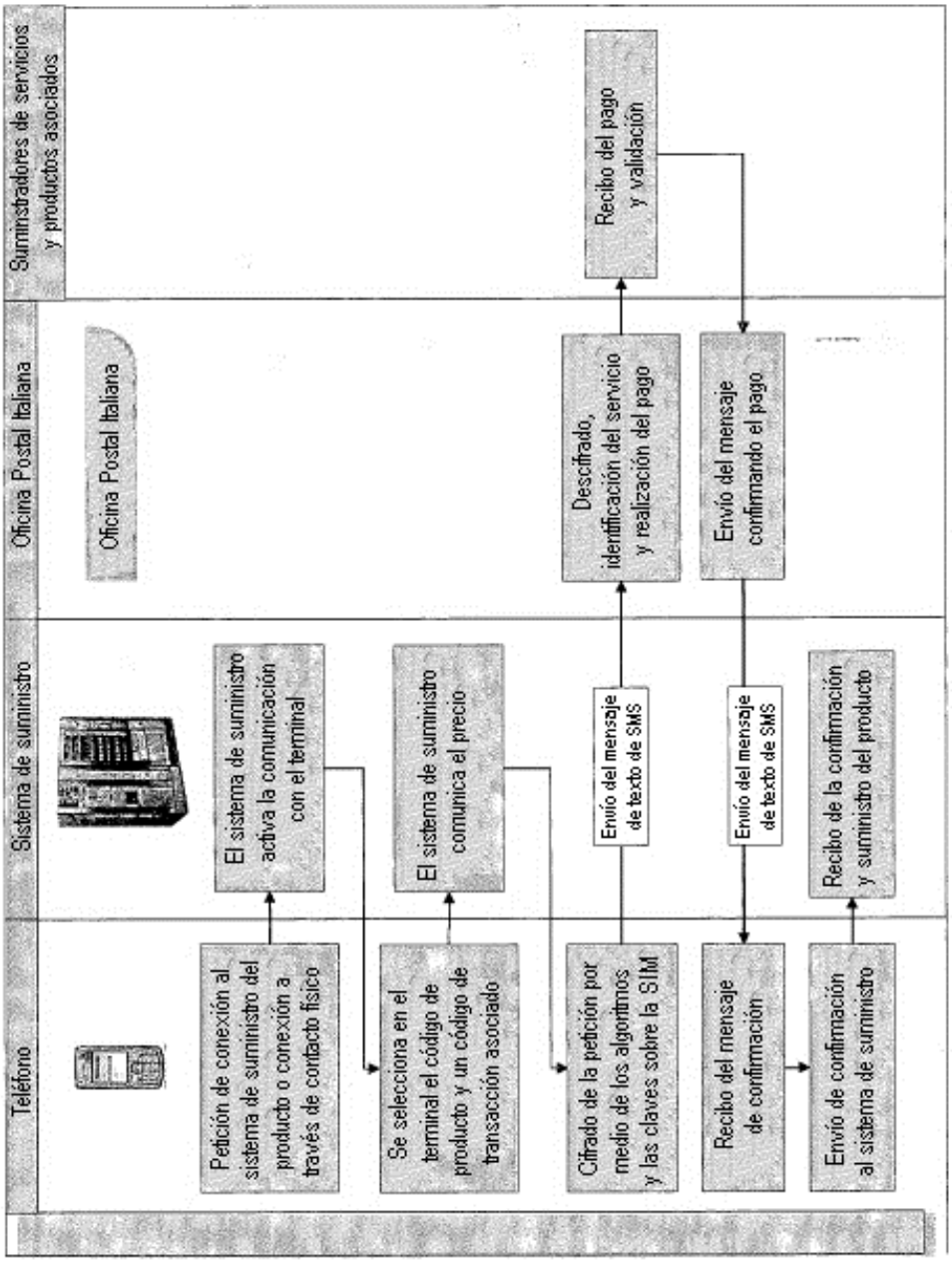
Teléfono
Sistema de suministro
Oficina Postal Italiana
Suministradores de servicios y productos asociados
Oficina Postal Italiana
Petición de conexión al sistema de suministro del producto o conexión a través de contacto físico
El sistema de suministro activa la comunicación con el terminal
Se selecciona en el terminal el código de producto y un código de transacción asociado
El sistema de suministro comunica el precio
Cifrado de la petición por medio de los algoritmos y las claves sobre la SIM
Envío del mensaje de texto de SMS
Descifrado, identificación del servicio y realización del pago
Recibo del pago y validación
Recibo del mensaje de confirmación
Envío del mensaje de texto de SMS
Envío del mensaje confirmando el pago
Envío de confirmación al sistema de suministro
Recibo de la confirmación y suministro del producto

Fig.4

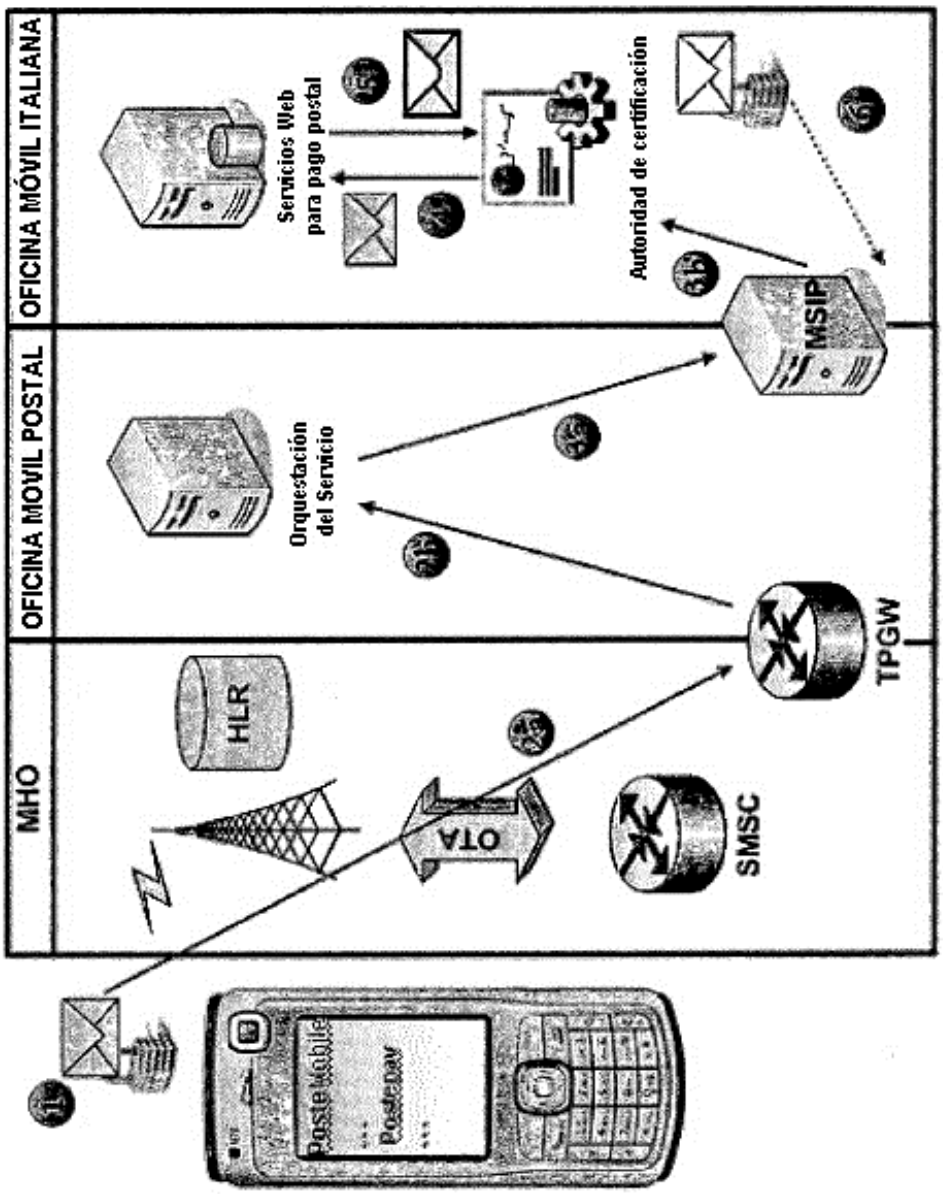
MHO
OFICINA MOVIL POSTAL
OFICINA MÓVIL ITALIANA
HLR
OTA
SMSC
TPGW
MSIP
Orquestación del Servicio
Servicios Web para pago postal
Autoridad de certificación
Postepay

Fig.5