(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 543 883**

(51) Int. CI.:

H04W 12/06 (2009.01)
H04L 29/06 (2006.01)
H04W 4/12 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **22.09.2010 E 10767951 (6)**

(97) Fecha y número de publicación de la concesión europea: **29.04.2015 EP 2481230**

(54) Título: **Método de autenticación, método de autorización de pago y equipos electrónicos correspondientes**

(30) Prioridad:

25.09.2009 IT MI20091640

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.08.2015

(73) Titular/es:

FERRARI, GIUSEPPE (100.0%)
Via Ripamonti 189
20141 Milan, IT

(72) Inventor/es:

COLOMBO, DANILO;
BERGANTINI, MARIO y
MINARDI, ALESSANDRO

(74) Agente/Representante:

RUO, Alessandro

DESCRIPCIÓN

Método de autenticación, método de autorización de pago y equipos electrónicos correspondientes

Campo de la invención

[0001] La presente invención se refiere a un método de autenticación, un método de autorización de pago y a equipos electrónicos correspondientes.

Estado de la técnica

[0002] En el campo de la seguridad informática, la autenticación se define como el proceso por el que un ordenador, un programa de software o un usuario verifica la correcta, o al menos presunta, identidad de otro ordenador, programa de software o usuario.

[0003] Actualmente existen muchos tipos de autenticación diferentes, con diversos niveles de seguridad y utilidad. Esto varía desde el clásico “nombre de usuario/contraseña”, a la combinación de aquellos con códigos personales de “un uso”, a los secuenciadores de códigos más recientemente usados por instituciones bancarias, también llamados “identificadores de seguridad”, que sustituyen a los códigos de “un uso”.

[0004] A partir de la solicitud de patente británica nº 2384396, se conoce un sistema de autenticación para transferir con seguridad información a través de mensajes de una red de comunicación móvil (por ejemplo, SMS de GSM); los mensajes se codifican total o parcialmente; tanto el usuario que origina la información como el usuario que recibe la información se autentican mediante un sistema de autorización que transfiere la información; la autenticación se lleva a cabo mediante el sistema de autorización basado en PIN recibidos por él desde ambos usuarios (etapa 322 en la Fig. 4A y etapa 350 en la Fig. 4B) y comparados (etapa 322 en la Fig. 4A y etapa 350 en la Fig. 4B) con PIN previamente almacenados de manera interna (etapa 308 en la Fig. 4A y etapa 328 en la Fig. 4B); el proceso de transferencia de información autenticada facilita que las claves públicas específicas de transacción se transfieran desde el sistema de autenticación al terminal de origen (mensaje 310 de la Fig. 4A) y desde el sistema de autenticación al terminal de recepción (mensaje 334 en la Fig. 4B).

Sumario de la invención

[0005] Aunque la solución descrita en la solicitud de patente antes mencionada es bastante fiable y segura, existe el riesgo de que la información de autenticación (es decir, los PIN) y la información de codificación (es decir, las claves públicas) puedan capturarse y recibir un uso incorrecto por parte de usuarios maliciosos, ya que se transmiten por el aire y se almacenan dentro del sistema de autenticación.

[0006] La presente invención es una solución diseñada para asegurar una autenticación más fiable y segura de una persona a través de un terminal de teléfono móvil para el uso de un servicio genérico.

[0007] El requisito de autenticación se aplica a todos los servicios que requieren el acceso a datos confidenciales, la segura comunicación de tales datos a terceras partes, y en general a todos los servicios que implican transferencias de cantidades de dinero u objetos valiosos o autorizaciones para tales transferencias en diversas capacidades. En este contexto, los ejemplos más comunes de actividades humanas que requieren autenticación mediante un sistema electrónico son: la compra de un bien en Internet, la solicitud de un certificado a una institución pública, el uso de un ordenador, la retirada de una cantidad de dinero de un cajero automático, la compra de un bien mediante una tarjeta de crédito o tarjeta de débito en un minorista normal, y la realización de una transacción bancaria por medio de Internet (llamada “Banca en línea”).

[0008] Las principales características técnicas de la presente invención se exponen en las reivindicaciones adjuntas para considerarse como una parte esencial de la presente descripción; otras características técnicas de la presente invención se exponen en la siguiente descripción detallada. El aspecto clave de la presente invención es un método de autenticación; otros aspectos hacen referencia a un método de autorización de pago basándose en tal método de autenticación y equipos electrónicos adaptados para tales métodos.

[0009] La presente invención tiene tres objetivos principales:

- el aislamiento de la información confidencial: evitar el intercambio de datos confidenciales (números PIN, claves criptográficas, …) durante el procedimiento de autenticación;
- una alta certeza, robustez y seguridad;
- una alta utilidad tanto para los usuarios en términos de operación (fácil de usar) y en términos de practicidad (siempre disponible en cualquier momento).

[0010] La solución de acuerdo con la presente invención se basa en el intercambio de información entre dos entidades:

- un “Usuario”, usuario de un servicio, es decir, la entidad, normalmente una persona, que desea autenticarse;
- un “Administrador”, que proporciona el servicio, es decir, la entidad con la que el Usuario pretende autenticarse para usar el servicio.

[0011] Una tercera entidad el “Intermediario” ubicada entre el Usuario y el Administrador, se ocupa de proporcionar el soporte de tecnología de la información necesario para el intercambio de información entre las otras dos entidades y para la autenticación del Usuario hacia el Administrador. En algunos contextos, el Intermediario y el Administrador pueden coincidir, pero es preferente mantener esta separación lógica para la conveniencia de la exposición.

[0012] La solución de acuerdo con la presente invención requiere normalmente la instalación de un programa de software en el terminal de teléfono móvil del Usuario, llamado “Cliente”; este programa de software se ocupa de controlar la comunicación con el Administrador y proporcionar al Usuario una interfaz adecuada teléfono-terminal. En su lugar, el Administrador tiene normalmente disponible una interfaz de tipo Web para todas sus operaciones; como alternativa, puede darse que el Administrador tenga un terminal de teléfono móvil con un Cliente que refleje completamente el del Usuario.

[0013] El flujo de información intercambiada entre las entidades antes definidas se realiza mediante mensajes de texto (mensajes de texto de teléfono y/o mensajes de texto informáticos) y se divide en dos secciones:

- la sección Administrador-Intermediario: en esta sección el transporte de información se realiza por medio del protocolo TCP/IP para la interfaz de tipo Web y por medio de SMS, MMS o el protocolo TCP/IP para el Cliente.
- la sección Intermediario-Usuario; en esta sección el transporte de información se realiza por medio de SMS, MMS o el protocolo TCP/IP (a través de, por ejemplo, una tecnología de mensajería instantánea) para el Cliente;

[0014] De acuerdo con la implementación más típica de la presente invención, se proporciona: un transporte SMS en la sección Intermediario-Usuario y un transporte TCP/IP en la sección Administrador-Intermediario.

[0015] La información intercambiada entre el Usuario y el Administrador se divide en dos tipos: “Datos de Control” y “Datos de Servicio”.

[0016] Los Datos de Control se codifican siempre preferentemente por medio de claves criptográficas asimétricas (clave pública + clave privada) en cada etapa del procedimiento de autenticación, asegurando de esta manera la confidencialidad y la autenticación.

[0017] La criptografía asimétrica, también conocida como criptografía de par de claves, criptografía de clave pública/privada, o también criptografía de clave pública, es un tipo de criptografía donde los pares de claves se asocian con las entidades implicadas en la comunicación:

- la clave privada, personal y secreta, se usa para descodificar un texto codificado;
- la clave pública, que tiene que distribuirse, se usa para codificar un texto dirigido a una entidad que tiene la clave privada correspondiente.

[0018] Los Datos de Servicio pueden estar “sin codificar”, al menos que se especifique lo contrario.

[0019] Ventajosamente, los mensajes son independientes del tipo de transporte usado. Preferentemente, cada mensaje de texto usado durante la autenticación se transporta usando un único mensaje te texto de teléfono, en particular un SMS.

Breve descripción de los dibujos

[0020] La presente invención así como sus características técnicas y ventajas se entenderán mejor a partir de la siguiente descripción al considerarla junto con los dibujos adjuntos en los que:

La Fig. 1 es un diagrama de bloques útil para entender un procedimiento de registro de acuerdo con la presente invención,
La Fig. 2 es un diagrama de bloques útil para entender un procedimiento de autenticación de acuerdo con la presente invención, y
La Fig. 3 es un diagrama de bloques útil para entender un procedimiento de pago de acuerdo con la presente invención que incorpora el procedimiento de autenticación de la Fig. 2.

Descripción detallada de la invención

[0021] Dicha descripción y dichos dibujos son únicamente explicativos y no limitativos.

[0022] De acuerdo con el ejemplo descrito a continuación, existe un servicio, en lo sucesivo el “Servicio de Autenticación”, que puede usarse mediante un usuario, en lo sucesivo el “Usuario” (marcado con un 7 en las

figuras), para certificar su identidad a cualquier proveedor de servicios, en lo sucesivo el “Administrador” (véase el elemento 21 en las figuras); el servicio de autenticación se proporciona mediante una entidad, en lo sucesivo, el “Intermediario” (véase el elemento 9 en las figuras); por tanto, básicamente, están implicadas tres entidades: el Usuario, el Administrador y el Intermediario; cada una de estas entidades se asocia con al menos un equipo electrónico (marcados con 8, 9 y 21 en las figuras), en particular, el Usuario se asocia con un terminal de teléfono móvil que tiene un número de teléfono móvil, normalmente un teléfono móvil (marcado con un 8 en las figuras), que permite implementar la invención.

[0023] Debe apreciarse que en un entorno de implementación real y típico existe un número de usuarios, un número de administradores y un intermediario.

[0024] Se proporcionan tres procedimientos: un procedimiento de suscripción que permite al Usuario suscribirse al Servicio de Autenticación, un procedimiento de registro que permite que el Usuario comience a usar el Servicio de Autenticación, y un procedimiento de autenticación que permite que el Administrador autentique al Usuario.

Procedimiento de Suscripción

[0025] En la suscripción para el Servicio de Autenticación, el Usuario proporciona (directa o indirectamente) al Intermediario, entre otros datos, su propio número de teléfono móvil, es decir, el “Número de Teléfono del Usuario”; el Usuario recibe (directa o indirectamente) del Intermediario un código personal, llamado “Código de Usuario”, que le identificará a él únicamente en el contexto del Servicio de Autenticación, y un programa de software, llamado “Cliente” (más precisamente “Cliente Usuario”), que se instalará en su terminal de teléfono móvil; este programa de software está provisto de una clave, llamada “Clave de Registro”; esta clave se genera a través de, por ejemplo, un algoritmo de base aleatorio, es inequívoca y puede usarse solo una vez durante el registro en el Servicio de Autenticación; los datos del Usuario, es decir, el número de teléfono móvil, el Código de Usuario, la Clave de Registro,… se almacenan en una “Base de Datos” accesible mediante el Intermediario para uso futuro; este es el procedimiento de suscripción.

[0026] Una vez que se ha completado el procedimiento de suscripción, puede comenzar el procedimiento de registro.

Procedimiento de Registro

[0027] El Usuario, para poder beneficiarse del Servicio de Autenticación, realiza las siguientes etapas:

1) instalar el Cliente en un teléfono móvil del Usuario (asociado con el Número de Teléfono Móvil, por ejemplo, a través de la tarjeta SIM del Usuario);
2) configurar en el Cliente un código privado, llamado PIN [Número de Identificación Personal]; este código no lo crea ni el Intermediario ni el Administrador, sino que lo crea el Usuario en el momento del registro y por lo tanto solo lo conoce él.

[0028] El Cliente, después de la configuración del PIN por el Usuario, realiza las siguientes etapas:

1) generar un par de “clave pública-clave privada” (es decir, claves de Usuario);
2) codificar la “clave privada de Usuario” usando el PIN como clave de codificación;
3) guardar la clave privada de Usuario, codificada de esta manera, dentro del teléfono móvil del Usuario;
4) enviar al Intermediario un “Mensaje de Registro” que contenga al menos la “clave pública de Usuario” generada y codificada por medio de la “clave de Registro”.

[0029] El Intermediario, tras recibir el Mensaje de Registro, realiza las siguientes etapas:

1) validar el Mensaje de Registro recibido basándose al menos en el número de teléfono móvil del remitente (que debería corresponderse con el Número de Teléfono del Usuario) y la Clave de Registro;
2) generar un par de “clave pública-clave privada” (es decir, claves de Intermediario), tales claves de Intermediario pueden asociarse con este Usuario específico o pueden asociarse con más de un usuario;
3) asociar, en su Base de Datos, la “clave privada de Intermediario” generada localmente con la clave pública de Usuario recibida desde el Usuario; tal Base de Datos se construye y se administra para asegurar el cumplimiento de la legislación existente sobre la protección de datos personales así como para asegurar la seguridad e integridad de los datos;
4) enviar al Usuario un “Mensaje de Validación de Registro” que contenga al menos la “clave pública de Intermediario” generada, codificada por medio de la Clave de Registro.

[0030] El Cliente, en el teléfono móvil del Usuario, tras recibir el Mensaje de Validación de Registro, guarda la clave pública de Intermediario dentro del teléfono móvil del Usuario y emite una señal de procedimiento completado.

[0031] En este momento el Usuario se registra en el Servicio de Autenticación.

[0032] Debe apreciarse que, dependiendo de la implementación de la presente invención, el procedimiento de suscripción y el procedimiento de registro pueden ocurrir justo uno después del otro.

[0033] También debe apreciarse que, dependiendo de la implementación de la presente invención, estos procedimientos pueden ocurrir después del equipo electrónico del Intermediario o a través de una conexión segura con el equipo electrónico del Intermediario; en estos casos, el procedimiento de registro puede simplificarse mucho ya que la comunicación entre el Usuario y el Intermediario puede considerarse completamente o altamente segura.

Procedimiento de Autenticación

[0034] El procedimiento de Autenticación se activa mediante el Usuario que, teniendo la necesidad, solicita un servicio al Administrador.

[0035] El Usuario comunica su propio Código de Usuario, además de la información sobre el servicio solicitado, al Administrador. Debe apreciarse que en algunos casos tal comunicación no es electrónica tal como en el caso de la compra de un bien a través de una tarjeta de crédito o tarjeta de débito a un minorista normal y que en algunos casos tal comunicación puede corresponderse con el Usuario introduciendo directamente información en el equipo electrónico del Administrador, tal como en el caso de, por ejemplo, la retirada de una cantidad de dinero de un cajero automático, y que en algunos casos tal comunicación puede corresponderse con el Usuario introduciendo indirectamente información en el equipo electrónico del Administrador tal como en el caso de por ejemplo la compra de un bien en Internet.

[0036] El Administrador, tras recibir la solicitud de servicio, envía al menos el Código de Usuario recibido y posiblemente la información sobre el servicio solicitado al Intermediario.

[0037] Debe apreciarse que esto se realiza normalmente mediante un programa de software llamado “Cliente” (más precisamente “Cliente Administrador”), que se ejecuta en el equipo electrónico asociado con el Administrador. Puede ser que no solo el equipo electrónico del Usuario sino también el equipo electrónico del Administrador sean terminales de teléfono móvil; este es el caso de, por ejemplo un vendedor callejero ambulante.

[0038] Después, el Intermediario realiza las siguientes etapas del procedimiento:

1) recibir el Código de Usuario identificar al Usuario y el Número de Teléfono del Usuario;
2) generar una “Clave de Autenticación; esta clave puede generarse mediante el Usuario a través de, por ejemplo, un algoritmo de base aleatorio, puede ser única y puede proporcionarse para un único uso dentro de la transacción actual (es decir, tiene un uso temporal);
3) enviar el “Mensaje de Solicitud de Autenticación” al Usuario (más precisamente, al terminal de teléfono móvil asociado con el Número de Teléfono Móvil, es decir, al teléfono móvil del Usuario). Tal mensaje consiste en dos partes: una primera parte que contiene, si y cuando sea necesario “Datos de Servicio” y una segunda parte que contiene la Clave de Autenticación, codificada por medio de la “clave pública de Usuario” y opcionalmente firmada de manera digital.

[0039] El Cliente Usuario, en el teléfono móvil del Usuario, recibe el Mensaje de Solicitud de Autenticación y realiza las siguientes etapas:

1) avisar a la persona que usa actualmente el teléfono móvil del Usuario de la presencia de una “Solicitud de Autenticación”;
2) proporcionar los Datos de Servicio a esa persona, tras la solicitud, y preguntarle si pretende autenticarse o no en el servicio (es decir usarlo);
3) pedir un PIN tras una respuesta positiva de esa persona;
4) extraer la “clave privada de Usuario” y descodificar la segunda parte del Mensaje de Solicitud de Autenticación por medio del PIN recibido desde esa persona (es decir, introducido por ella) obteniendo de esta manera la Clave de Autenticación;
5) enviar al Intermediario un mensaje de respuesta a la Solicitud de Autenticación, que contenga la Clave de Autenticación (o de manera equivalente unos datos derivados de la misma) codificada por medio de la “clave pública de Intermediario”.

[0040] El Intermediario recibe la respuesta a la Solicitud de Autenticación y realiza las siguientes etapas:

1) descodificar la Clave de Autenticación a través de la clave privada de Intermediario;
2) validar la Clave de Autenticación recientemente descodificada (o de manera equivalente unos datos derivados de la misma);
3) en caso de una validación con un resultado positivo, enviar un “Mensaje de Autenticación Confirmada” al Usuario y al Administrador; en caso de una validación con resultado negativo, enviar un “Mensaje de

Autenticación Denegada” al Usuario y al Administrador.

[0041] El procedimiento de autenticación está ahora completado.

Criptografía y PIN

[0042] Como ya se ha dicho, el tipo preferente de criptografía a usar para implementar la presente invención, particularmente para el procedimiento de autenticación, es la criptografía asimétrica. De cualquier manera, la criptografía simétrica puede usarse total o parcialmente durante el procedimiento de autenticación incluso con una seguridad y fiabilidad reducidas; adicionalmente, los mensajes de texto pueden dividirse en partes en las que cada una de estas partes puede codificarse o no codificarse, es decir, puede haber mensajes de texto no codificados y/o mensajes de texto totalmente codificados y/o mensajes de texto parcialmente codificados dependiendo de su contenido y/o de las entidades implicadas en el intercambio, pero también dependiendo de las circunstancias específicas y la implementación de la presente invención.

[0043] Si se usa criptografía asimétrica, el enfoque preferente es ECC [Criptografía de Curva Elíptica]; en este caso, las curvas preferentes van desde P-160 a P-256. Este enfoque puede usarse ventajosamente también para firmar digitalmente información y/o mensajes.

[0044] Si se usa criptografía simétrica, el enfoque preferente es AES [Estándar de Codificación Avanzada]; en este caso, los tamaños de clave preferentes van desde 128 a 256 bits.

[0045] Como ya se ha dicho, se usa un PIN como clave criptográfica para codificar y descodificar la clave privada de Usuario. Si el Administrador se asocia con una terminal de teléfono móvil, pueden existir claves de Administrador y la clave privada de Administrador puede almacenarse dentro del terminal de teléfono móvil del Administrador codificada por medio de un “PIN del Administrador”.

[0046] Preferentemente, cualquier PIN debería ser bastante corto, por ejemplo de 4 a 8 dígitos, para que una persona pueda recordarlo fácilmente; en este caso, usar el PIN directamente como una clave criptográfica puede no ser suficientemente seguro; por tanto, una función de resumen criptográfico se aplica ventajosamente al PIN proporcionando una secuencia de bits (que tiene una longitud preferentemente de 128 a 256) lo suficientemente larga para usarse como una clave criptográfica segura. La familia preferente de funciones de resumen criptográfico es SHA [Algoritmo de Resumen criptográfico Seguro], en particular de 128 bits a 256 bits.

Procedimiento de Autorización de Pago

[0047] El procedimiento de autorización de pago puede considerarse una aplicación del procedimiento de autenticación descrito anteriormente; en este caso, el término Comprador sería más apropiado que Usuario y el término Vendedor sería más apropiado que Administrador.

[0048] Para implementar tal procedimiento en un entorno práctico donde los sistemas de pago electrónicos ya existen, es ventajoso proporcionar una cuarta entidad, en lo sucesivo el “Pagador”, asociada con al menos un equipo electrónico (marcado como 123 en la Fig. 3), que se ocupa del pago, es decir, de la transferencia de dinero de la cuenta bancaria del Usuario a la cuenta bancaria del Administrador (tras la autenticación de, es decir, autorización por, el Usuario); se establece que el Pagador se comunique con el Intermediario, pero no con el Usuario ni el Administrador; tanto el Usuario como el Administrador deben suscribirse y registrarse en el servicio para que los datos necesarios para gestionar la autorización y el pago estén disponibles para el Intermediario y el Pagador de acuerdo con sus necesidades y de acuerdo con la implementación específica; la suscripción y el registro pueden tener lugar de la misma manera tanto para el Usuario como para el Administrador, por ejemplo, tal como se ha descrito anteriormente y puede implicar solo (o casi únicamente) al Intermediario o tanto al Intermediario como al Pagador, dependiendo de la implementación.

[0049] Debe apreciarse que este procedimiento puede implementarse para que sea aplicable no solo a pagos de un comprador a un vendedor sino también a transferencias de dinero entre personas; de acuerdo con la implementación, los suscriptores pueden actuar como un “Usuario”/”Comprador” o “Administrador”/”Vendedor” dependiendo del momento.

[0050] Las principales diferencias entre el procedimiento de autenticación y el procedimiento de autorización de pago son las siguientes:

- la primera parte del Mensaje de Solicitud de Autenticación es necesaria ya que debe contener al menos la cantidad del pago;
- una tercera parte del Mensaje de Solicitud de Autenticación es necesaria ya que debe contener un código que identifica al Administrador, es decir, el beneficiario del pago;
- los códigos de identificación del Usuario y del Administrador así como al menos la cantidad del pago deben comunicarse al Pagador mediante el Intermediario;

- normalmente el número de teléfono móvil del Usuario (y el del Administrador) se almacena internamente en el Pagador y no en el Intermediario, por tanto, tras la Solicitud de Autenticación (es decir, un Solicitud de Pago), el Intermediario debería recopilar esta información del Pagador;
- la Clave de Autenticación se genera mediante el Pagador y es un código de transacción financiera único para el Pagador; por tanto, tras la Solicitud de Autenticación (es decir, una Solicitud de Pago), el Intermediario debería recopilar esta información del Pagador;
- en caso de una autenticación confirmada (es decir, autorización de pago mediante el Usuario), se envía un "Mensaje de Solicitud de Pago" del Intermediario al Pagador y se hace referencia a este código de transacción financiera;
- el Mensaje de Autorización Confirmada (que en este caso significa "pago confirmado") o Mensaje de Autenticación Denegada (que en este caso significa "pago denegado") se envía del Intermediario al Usuario y al Administrador solo después de recibir un "Mensaje de Resultado del Pago" del Pagador en respuesta al "Mensaje de Solicitud de Pago".

[0051] El procedimiento de autorización de pago de acuerdo con la presente invención puede aplicarse también a los pagos relacionados con comercio electrónico.

[0052] En el caso de comercio electrónico, de acuerdo con una primera posibilidad, el Administrador/Vendedor vende sus propios productos/servicios y el equipo electrónico del Administrador/Vendedor es un ordenador del Administrador/Vendedor conectado a Internet, que recibe información del Usuario/Comprador y se comunica con el equipo electrónico del Intermediario. Los códigos de identificación del Usuario/Comprador, es decir, la entidad que aporta el dinero y del Administrador/Vendedor, es decir, la entidad que recibe el dinero, así como al menos la cantidad de pago deben comunicarse al Pagador.

[0053] En el caso de comercio electrónico, de acuerdo con una segunda posibilidad, el Administrador/Vendedor vende productos/servicios a una Tercero (tal como por ejemplo "eBay") y el equipo electrónico del Administrador/Vendedor es un ordenador del Administrador/Vendedor conectado a Internet, que recibe información del Usuario/Comprador y se comunica con el equipo electrónico del Intermediario. Los códigos de identificación del Usuario/Comprador, es decir, la entidad que aporta el dinero, así como al menos la cantidad del pago deben comunicarse apropiadamente al Pagador; por tanto, la suscripción y el registro deben realizarse mediante el Usuario/Comprador y el Tercero, mientras que el Administrador/Vendedor tiene una relación preferente con el Intermediario.

Realización de la Fig. 1

[0054] En la Fig. 1, el Usuario 7 configura (flecha 1) un PIN en el Cliente instalado en el teléfono móvil 8. Ya que el Usuario crea el PIN, este solo lo conoce él. El Cliente, después de la configuración del PIN por el Usuario, genera un par de "clave pública - clave privada", codifica (flecha 2) la clave privada generada usando el PIN como clave de codificación y guarda la clave privada 11 codificada de esta manera dentro del teléfono móvil 8. Finalmente, codifica (flecha 2) la clave pública generada, codificada mediante la Clave de Registro, y envía (flecha 3) un mensaje de registro que contiene la clave pública 10 codificada de esta manera al equipo electrónico del Intermediario 9.

[0055] El equipo electrónico del Intermediario 9, tras recibir el mensaje de registro, valida el mensaje de registro recibido, basándose en el número de teléfono móvil del remitente y la Clave de Registro; genera un par de "clave pública - clave privada"; asocia (flecha 4) en su base de datos 12 la clave privada generada de esta manera, es decir, la "clave privada de Intermediario" con la clave pública de Usuario; envía (flecha 5) un mensaje de validación de registro, que contiene la clave pública de Intermediario, codificado por medio de la "Clave de Registro", al equipo electrónico del Usuario 8.

[0056] El Cliente, en el teléfono móvil 8 del Usuario, tras recibir el mensaje de validación de registro, guarda la "clave publica de Intermediario" proporcionada por el equipo electrónico del Intermediario dentro del teléfono móvil 8 que emite (flecha 6) una señal de procedimiento completado. En este punto, el Usuario se registra en el Servicio de Autenticación.

Realización de la Fig. 2

[0057] En la Fig. 2, el equipo electrónico del Administrador 21 comunica (flecha 13) el Código de Usuario al equipo electrónico del Intermediario 9; el equipo electrónico del Intermediario 9 facilita generar 14 la Clave de Autenticación temporal 22, que solo puede usarse una vez; el equipo electrónico del Intermediario 9 envía (flecha 15) el Mensaje de Solicitud de Autenticación al equipo electrónico del Usuario 8.

[0058] El Cliente, en el teléfono móvil 8 del Usuario, recibe el Mensaje de Solicitud de Autenticación. Por tanto, avisa (flecha 17) a la persona que está usando actualmente el teléfono móvil 8, que como norma debería corresponderse con el Usuario 7, sobre la presencia de una Solicitud de Autenticación y, tras la solicitud del Usuario, presenta (flecha 17) los Datos de Servicio contenidos en el Mensaje de Solicitud de Autenticación y pregunta (flecha 17) al Usuario 7 si pretende autenticarse o no en el servicio; el Cliente pide (flecha 17) un PIN tras una respuesta

positiva del Usuario 7 y el Usuario 7 proporciona (flecha 16) un PIN que debería corresponderse con el PIN proporcionado por el Usuario 7 en el registro.

[0059] A través del PIN recibido (si es correcto), el Cliente puede extraer y descodificar la clave privada de Usuario y, a través de la clave privada de Usuario recién descodificada, puede descodificar la segunda parte del Mensaje de Solicitud de Autenticación, obteniendo de esta manera la Clave de Autenticación.

[0060] El Cliente en el teléfono móvil 8 del Usuario envía (flecha 18) al equipo electrónico del Intermediario 9 un mensaje de respuesta a la Solicitud de Autenticación, que contiene la Clave de Autenticación, codificado por medio de la clave pública de Intermediario.

[0061] El equipo electrónico del Intermediario 9, tras recibir la respuesta a la Solicitud de Autenticación, descodifica la Clave de Autenticación a través de la clave privada de Intermediario, valida la Clave de Autenticación, y, en caso de que la validación tenga un resultado positivo, envía (flecha 19) un mensaje de Autenticación Confirmada al equipo electrónico del Administrador 21, y normalmente el mismo mensaje de Autenticación Confirmada al equipo electrónico del Usuario 8. En el caso de la validación con resultado negativo, envía un mensaje de Autenticación Denegada al Usuario y al Administrador.

[0062] El Procedimiento de Autenticación está ahora completado.

[0063] Tal como debería ser aparente a partir de lo que se acaba de describir, la presente invención tiene las siguientes ventajas:

- ningún dato confidencial se transmite durante el procedimiento de autenticación y la Clave de Autenticación puede seleccionarse para usarse solo una vez; en particular, el PIN no lo genera una entidad, lo elige el Usuario, nunca se almacena permanentemente dentro del equipo electrónico del Usuario y nunca se transmite fuera del equipo electrónico del Usuario;
- el uso de mensajes de texto codificados mediante criptografía asimétrica asegura la seguridad, robustez y fiabilidad; además, como la autenticación siempre se solicita al Usuario mediante el Administrador, la solicitud siempre se dirige al terminal de teléfono móvil del Usuario, evitando de manera eficaz cualquier tipo de fraude;
- el procedimiento de autenticación estipula únicamente escribir el PIN para que lo complete el Usuario; esto facilita las operaciones en el teléfono móvil, ya que no existe necesidad de, por ejemplo, escribir mensajes de texto directamente; el uso del teléfono móvil y SMS permite el uso de la presente invención en cualquier contexto en la vida diaria de hoy en día y en cualquier momento y en cualquier parte del mundo.

Realización de la Fig. 3

[0064] Debe apreciarse que en la Fig. 3 se usan números de referencia similares a los usados en la Fig. 2; en particular, los elementos correspondientes (o casi correspondientes) están marcados con el mismo número, pero aumentados en 100.

[0065] En la Fig. 3, el equipo electrónico del Administrador/Vendedor 121 envía (flecha 113) una solicitud de pago al equipo electrónico del Intermediario 109 que contiene los datos de pago, su código de identificación y el código de identificación del Usuario/Comprador; el equipo electrónico del Intermediario 109 comprueba la autenticidad de esta solicitud descodificándola por medio de la clave privada de Intermediario y, si la comprobación da un resultado positivo, solicita (flecha 124) una comprobación de los datos recibidos al equipo electrónico del Pagador 123 (esta es la interfaz con un circuito de pago ya existente que no se muestra en la figura).

[0066] El equipo electrónico del Pagador 123 proporciona una respuesta (flecha 125) con un resultado positivo o negativo; si el resultado es positivo, el equipo electrónico del Pagador 123 coloca en la respuesta el número de teléfono móvil del Usuario/Comprador y un Código de Transacción Financiera (correspondiente a la Clave de Autenticación ya mencionada); este código es único y puede usarse solo una vez para identificar con seguridad una transacción financiera del circuito de pago.

[0067] Una vez que el equipo electrónico del Intermediario 109 ha recibido la información necesaria desde el equipo electrónico del Pagador 123, el equipo electrónico del Intermediario 109 envía (flecha 114/115) al equipo electrónico 108 del Usuario/Comprador del Usuario/Comprador 107 un Mensaje de Solicitud de Autorización de Pago; este mensaje comprende dos partes: una primera parte que contiene datos de pago (al menos la cantidad de pago) y una segunda parte que contiene el Código de Transacción Financiera, codificado por medio de la clave pública de Usuario/Comprador y posiblemente firmado digitalmente por el Intermediario. El Cliente en el equipo electrónico 108 del Usuario/Comprador del Usuario/Comprador 107 recibe el Mensaje de Solicitud de Autorización de Pago, comprueba la firma (si existe) y realiza las siguientes etapas:

- presentar (flecha 117) la solicitud al Usuario/Comprador 107;
- después de la solicitud (flecha 116) del Usuario/Comprador 107, presentar (flecha 117) los datos de pago (extraídos del Mensaje de Solicitud de Autorización de Pago recibido) al Usuario/Comprador 107 y pedir (flecha

117) al Usuario/Comprador 107 la autorización para pagar;
- tras una respuesta positiva (flecha 16) del Usuario/Comprador 107, solicitar (flecha 117) un PIN;
- a través de un PIN correcto recibido del Usuario/Comprador 107, descodificar la segunda parte del Mensaje de Solicitud de Autorización de Pago recibido, obteniendo de esta manera el Código de Transacción Financiera;
- enviar (flecha 118) al equipo electrónico del Intermediario 109 una respuesta a la solicitud de autorización de pago que contenga al menos el Código de Transacción Financiera, codificada por medio de la clave pública de Intermediario y posiblemente firmada de manera digital por el Usuario/Comprador.

[0068] El equipo electrónico del Intermediario 109, tras la recepción de la respuesta a la solicitud de autorización de pago desde el equipo electrónico 108 del Usuario/Comprador, comprueba la firma (si existe) y realiza las siguientes etapas:

- descodificar el Código de Transacción Financiera por medio de la clave privada de Intermediario;
- validar la respuesta a la solicitud de autorización de pago, por ejemplo, mediante la comparación del Código de Transacción Financiera enviado al Usuario/Comprador y el Código de Transacción Financiera recibido desde el Usuario/Comprador;
- en caso de un resultado positivo de la validación, enviar (flecha 126) al equipo electrónico del Pagador 123 un Mensaje de Solicitud de Pago que contenga los datos de pago y/o el Código de Transacción Financiera.

[0069] El equipo electrónico del Pagador 123, tras la recepción del Mensaje de Solicitud de Pago desde el equipo electrónico del Intermediario 109, realiza todas las etapas necesarias para llevar a cabo el pago (no se describen en el presente documento ya que son típicas de los circuitos de pago conocidos) y envía (flecha 127) al equipo electrónico del Intermediario 109 un Mensaje de Resultado del Pago que contiene información referente al resultado del pago que podría ser positivo o negativo (por ejemplo, en el caso de que el Usuario/Comprador no tenga suficiente dinero en su cuenta bancaria).

[0070] El equipo electrónico del Intermediario 109, tras la recepción del Mensaje de Resultado del Pago desde el equipo electrónico del Pagador 123, envía un Mensaje de Pago Confirmado o un Mensaje de Pago Denegado tanto (flecha 120) al equipo electrónico del Usuario/Comprador como (flecha 119) el equipo electrónico del Administrador/Vendedor. El procedimiento de autorización de pago (y también el pago) está ahora completado.

REIVINDICACIONES

1. Método de autenticación de un Usuario (7) mediante un Administrador (21) en el que dicho Usuario está asociado con un equipo electrónico en la forma de un terminal de teléfono móvil (8) en el que está cargado un programa de software, estando adaptado dicho programa de software para almacenar dentro de dicho terminal de teléfono móvil una clave criptográfica codificada por medio de un PIN, en el que dicho Administrador está asociado con un equipo electrónico, en el que el método proporciona un Intermediario (9) asociado con un equipo electrónico adaptado para comunicarse con dicho equipo electrónico del Usuario y dicho equipo electrónico del Administrador mediante mensajes de texto y para almacenar un número de teléfono móvil del Usuario, y proporciona las siguientes etapas:

A) el equipo electrónico del Administrador envía al equipo electrónico del Intermediario un mensaje de texto que contiene al menos un código de identidad del Usuario,
B) el equipo electrónico del Intermediario identifica al Usuario y el número de teléfono móvil del Usuario y envía al equipo electrónico del Usuario un mensaje de texto que contiene al menos una clave de autenticación, estando codificado dicho mensaje de texto,
C) el equipo electrónico del Usuario recibe dicho mensaje de texto desde el equipo electrónico del Intermediario, lo descodifica por medio de dicha clave criptográfica después de haber obtenido dicho PIN desde una persona que usa el terminal de teléfono móvil del Usuario, y envía otro mensaje de texto codificado al equipo electrónico del Intermediario que contiene al menos dicha clave de autenticación,
D) el equipo electrónico del Intermediario recibe dicho otro mensaje de texto codificado desde el equipo electrónico del Usuario, lo descodifica, y realiza una comparación entre la clave de autenticación enviada al equipo electrónico del Usuario y la clave de autenticación recibida desde el equipo electrónico del Usuario, y
E) el equipo electrónico del Intermediario envía un mensaje de texto, que contiene al menos el resultado de dicha comparación o información que se deriva de la misma, a al menos el equipo electrónico del Administrador;
en el que dicho terminal de teléfono móvil usa dicho PIN solo para la codificación y descodificación interna de dicha clave criptográfica tras haberlo recibido de una persona que usa el terminal de teléfono móvil del Usuario en cada caso;
por donde el Administrador autentica al Usuario basándose en dicho resultado recibido o en información derivada del mismo.

2. Método de autenticación de acuerdo con la reivindicación 1, en el que los mensajes de texto intercambiados entre el equipo electrónico del Usuario y el equipo electrónico del Intermediario son mensajes de texto de teléfono, en particular SMS y/o MMS.

3. Método de autenticación de acuerdo con la reivindicación 1 o 2, en el que el Administrador está asociado con un equipo electrónico en la forma de un terminal de teléfono móvil y los mensajes de texto intercambiados entre el equipo electrónico del Administrador y el equipo electrónico del Intermediario son mensajes de texto de teléfono, en particular SMS y/o MMS.

4. Método de autenticación de acuerdo con la reivindicación 1 o 2, en el que el Administrador está asociado con un equipo electrónico en la forma de un terminal de usuario informático y los mensajes de texto intercambiados entre el equipo electrónico del Administrador y el equipo electrónico del Intermediario son mensajes de texto informáticos, transportados en particular usando el protocolo TCP/IP.

5. Método de autenticación de acuerdo con la reivindicación 2 o 3, en el que cada uno de dichos mensajes de texto se corresponde únicamente con un SMS o MMS.

6. Método de autenticación de acuerdo con cualquiera de las reivindicaciones anteriores, en el que dicho PIN comprende preferentemente de 4 a 8 dígitos y en el que para la codificación y descodificación de dicha clave criptográfica se aplica una función de resumen criptográfico a dicho PIN que proporciona una secuencia de bits que tienen una longitud preferentemente de 128 a 256.

7. Método de autenticación de acuerdo con cualquiera de las reivindicaciones anteriores, en el que los mensajes de texto intercambiados entre el equipo electrónico del Intermediario y el equipo electrónico del Usuario están codificados.

8. Método de autenticación de acuerdo con cualquiera de las reivindicaciones anteriores, en el que los mensajes de texto intercambiados entre el equipo electrónico del Intermediario y el equipo electrónico del Administrador están codificados.

9. Método de autenticación de acuerdo con las reivindicaciones 7 y/u 8, en el que los mensajes de texto están codificados mediante Criptografía de Curva Elíptica.

10. Método de autenticación de acuerdo con cualquiera de las reivindicaciones anteriores, en el que el equipo electrónico del Usuario está adaptado para gestionar claves públicas y privadas de Usuario, para almacenar la clave privada de Usuario y preferentemente una clave pública de Intermediario, usándose dichas claves para codificar y

descodificar mensajes de texto hacia y/o desde dicho equipo electrónico del Intermediario.

11. Método de autenticación de acuerdo con cualquiera de las reivindicaciones anteriores, en el que el equipo electrónico del Administrador está adaptado para gestionar claves públicas y privadas de Administrador, para almacenar la clave privada de Administrador y preferentemente una clave pública de Intermediario, usándose dichas claves para codificar y descodificar mensajes de texto hacia y/o desde dicho equipo electrónico del Intermediario.

12. Método de autenticación de acuerdo con cualquiera de las reivindicaciones anteriores, en el que el equipo electrónico del Intermediario está adaptado para gestionar claves públicas y privadas de Intermediario, para almacenar la clave privada de Intermediario y preferentemente una clave pública de Usuario y/o una clave pública de Administrador, usándose dichas claves para codificar y descodificar mensajes de texto hacia y/o desde dicho equipo electrónico del Usuario y/o dicho equipo electrónico del Administrador.

13. Método de autenticación de acuerdo con cualquiera de las reivindicaciones anteriores, en el que las comunicaciones entre el equipo electrónico del Usuario, el equipo electrónico del Intermediario y el equipo electrónico del Administrador pueden comprender el intercambio de mensajes de texto no codificados y/o mensajes de texto totalmente codificados y/o mensajes de texto parcialmente codificados, dependiendo tales características de los mensajes de texto de su contenido y/o de las entidades implicadas en el intercambio.

14. Método de autenticación de acuerdo con cualquiera de las reivindicaciones anteriores, en el que en la etapa E el equipo electrónico del Intermediario envía el mensaje de texto también al equipo electrónico del Usuario.

15. Método de autenticación de acuerdo con cualquiera de las reivindicaciones anteriores, que proporciona además un procedimiento de registro preliminar durante el que al menos ocurren las siguientes etapas:

- dicha clave criptográfica se codifica por medio de un PIN y se almacena dentro del terminal de teléfono móvil del Usuario, y
- dicho número de teléfono móvil del Usuario se almacena mediante el equipo electrónico del Administrador.

16. Método de autenticación de acuerdo con cualquiera de las reivindicaciones anteriores, en el que en la etapa A el mensaje de texto contiene además al menos una referencia a un producto o servicio solicitado por el Usuario al Administrador, en la etapa B el mensaje de texto contiene además al menos una referencia a un producto o servicio solicitado por el Usuario al Administrador, y en la etapa C el otro mensaje de texto codificado contiene además información referente a una autorización de pago de acuerdo con datos de una persona que usa el terminal de teléfono móvil del Usuario.

17. Método para autorizar el pago de un Usuario a un Administrador, que comprende el método de autenticación de acuerdo con la reivindicación 16 y proporciona además un Pagador asociado al menos con un equipo electrónico adaptado para comunicarse con dicho equipo electrónico del Intermediario, en el que después de la etapa D y antes de la etapa E, el equipo electrónico del Intermediario envía una solicitud de pago al equipo electrónico del Pagador de acuerdo con el resultado de dicha comparación, y recibe un resultado del pago del equipo electrónico del Pagador, y en el que en la etapa E, el mensaje de texto contiene al menos dicho resultado del pago.

18. Método de autorización de pago de acuerdo con la reivindicación 17, en el que en la etapa B el equipo electrónico del Intermediario obtiene dicha clave de autenticación del equipo electrónico del Pagador, siendo dicha clave de autenticación un código de transacción financiera único para el Pagador.

19. Equipo electrónico que comprende características técnicas que hacen que esté adaptado para funcionar como Intermediario de acuerdo con cualquiera de las reivindicaciones 1 a 18.

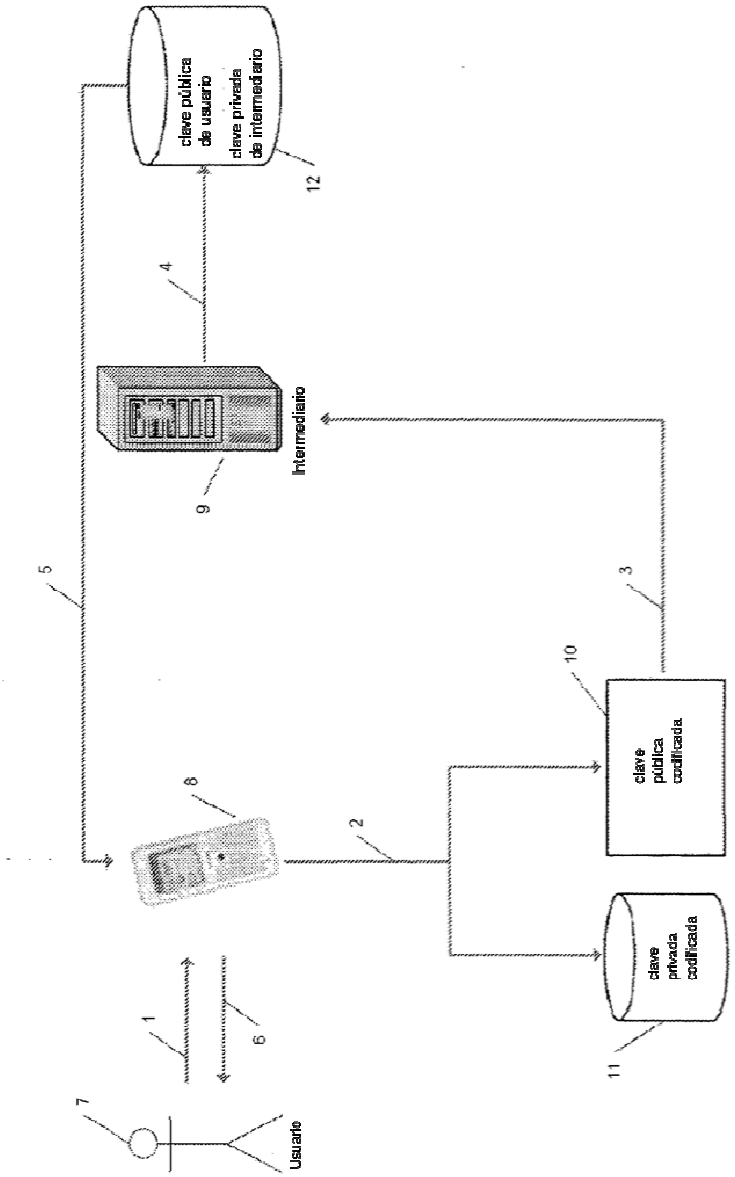
clave pública de usuario
clave privada de intermediario
12
4
Intermediario
9
5
3
10
clave pública codificada
8
2
clave privada codificada
11
1
6
7
Usuario

Fig. 1

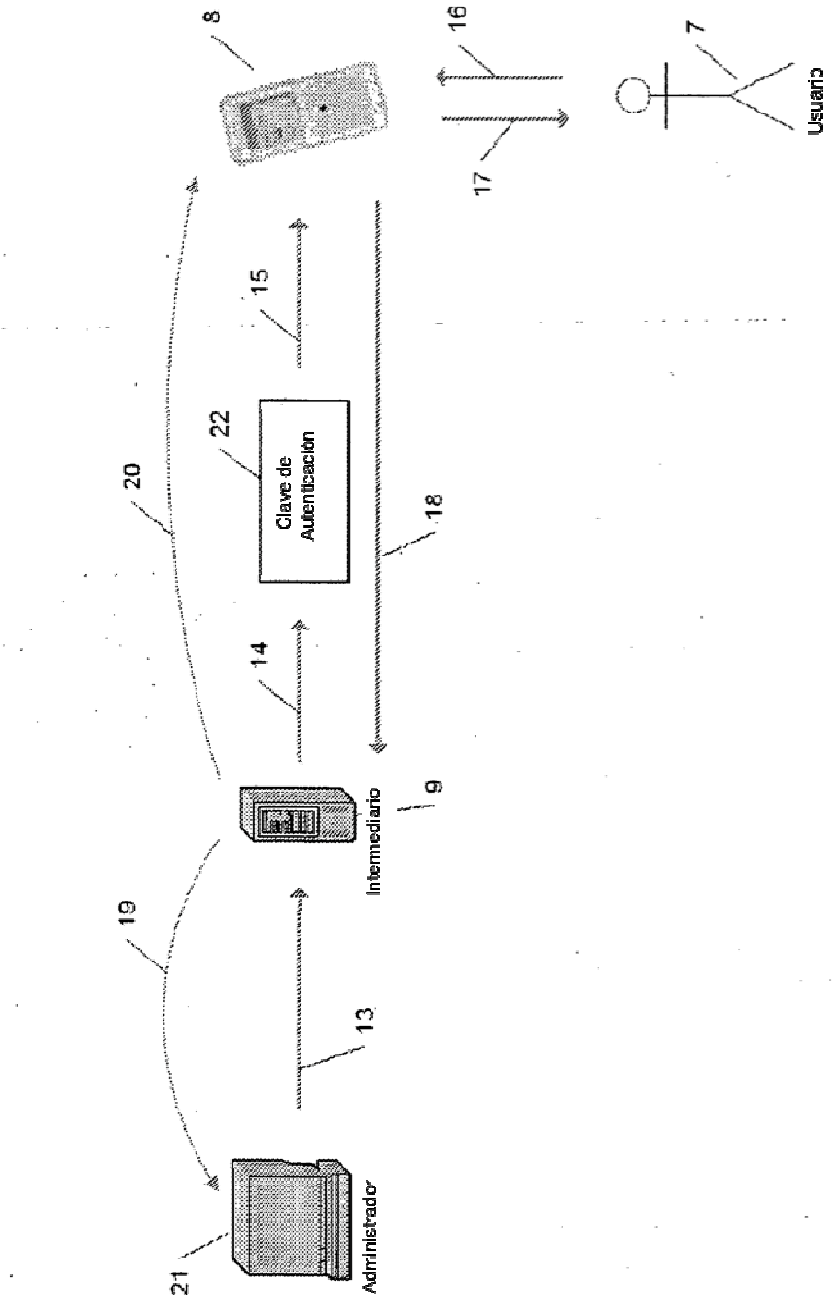
8
16
17
7
Usuario
15
22
Clave de Autenticación
20
18
14
9
Intermediario
19
13
Administrador
21

Fig. 2

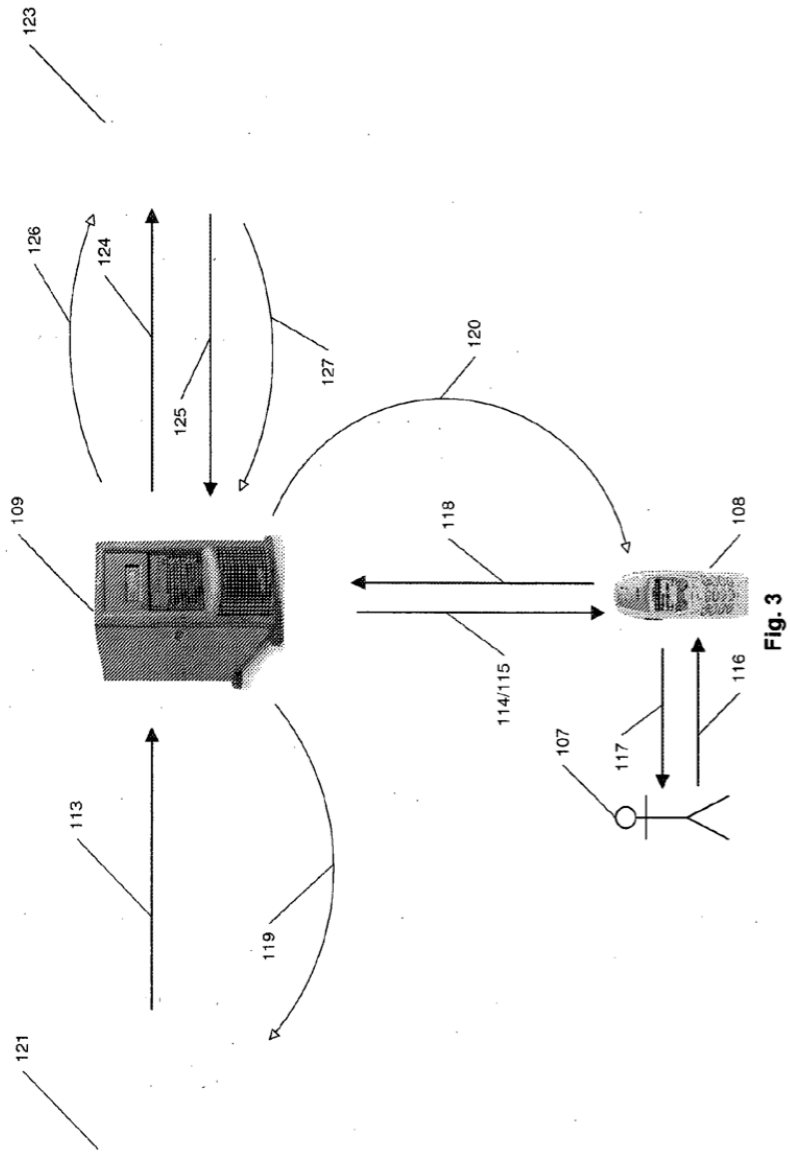
123
126
124
125
127
120
109
118
108
114/115
116
107
117
113
119
121

Fig. 3