(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 387 073**

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06820602 .8**
(96) Fecha de presentación: **20.12.2006**
(97) Número de publicación de la solicitud: **1969880**
(97) Fecha de publicación de la solicitud: **17.09.2008**

(54) Título: **Sistema y método de autenticación dinámica multifactor**

(30) Prioridad:
21.12.2005 EP 05257924

(45) Fecha de publicación de la mención BOPI:
12.09.2012

(45) Fecha de la publicación del folleto de la patente:
12.09.2012

(73) Titular/es:
CRONTO LIMITED
198 HUNTINGDON ROAD
CAMBRIDGE CB3 0LB, GB

(72) Inventor/es:
DROKOV, Igor;
PUNSKAYA, Elena y
TAHAR, Emmanuel

(74) Agente/Representante:
de Elzaburu Márquez, Alberto

DESCRIPCIÓN

Sistema y método de autenticación dinámica multifactor.

La presente invención se refiere a un sistema y un método para autenticar dinámicamente a un usuario de un sistema de comunicaciones. El rápido crecimiento en las áreas de transacciones comerciales y bancarias en línea ha necesitado el desarrollo de diversos métodos de autenticación de usuarios de tales sistemas, impidiendo al propio tiempo el robo de identidades.

La vasta mayoría de métodos de autenticación actuales en línea utilizan lo que se conoce como autenticación estática monofactor. Este esquema implica que un usuario tenga alguna forma de identificación de entrada estática (ID) y de contraseña estática. Utilizando un navegador en un dispositivo de acceso local, tal como un ordenador personal, un usuario inicia una solicitud de autenticación con un dispositivo de autenticación remoto introduciendo primeramente una ID de entrada y una contraseña en una página web. El dispositivo de autenticación remoto varía entonces la combinación ID de entrada/contraseña y, si ésta es válida, produce alguna especie de señal de autenticación. Aunque sencillos de implementar, los esquemas de autenticación estática monofactor tienen graves inconvenientes y son muy vulnerables a dos tipos de ataques.

El primer tipo de ataque al que es propensa la autenticación estática monofactor es conocido como "phishing" (robo de identidad). En este escenario una tercera parte malévola crea primero un sitio web que está diseñado para parecer y funcionar como un sitio web en el que un usuario desearía introducir información de autenticación. Seguidamente, la tercera parte atrae al usuario hacia el sitio web falsificado. Este paso se realiza usualmente enviando un correo electrónico a un usuario que contiene un enlace al sitio web falsificado y que incluye un mensaje diseñado para presionar al usuario a que tome inmediatamente alguna forma de acción registrándose en su cuenta. El usuario introduce entonces su ID de entrada estática y su contraseña estática en el sitio web falsificado, proporcionando así involuntariamente un información de autenticación a la tercera parte.

El segundo tipo de ataque al que es propensa la autenticación estática monofactor se conoce como "registro de teclado". Este ataque, aunque más difícil de poner en acción, es considerablemente más efectivo que el "phishing" debido a que es virtualmente indetectable para incluso el más versado usuario de ordenadores. Este tipo de ataque cuida de que un usuario descargue involuntariamente una pieza de "programa espía" que está empaquetada con otra pieza de software que el usuario intenta descargar, o que es distribuida con un virus. El programa espía es una pieza de software que recoge furtivamente información del usuario, tal como pulsaciones de teclado e información perteneciente a sitios web que ha visitado un usuario, y envía periódicamente esta información a una tercera parte malévola. Tal información puede someterse después fácilmente a referencias cruzadas a fin de extraer la información de autenticación de un usuario.

Se ha desarrollado recientemente una autenticación bifactor para superar las debilidades asociadas con los sistemas de autenticación estática monofactor. La "tarjeta inteligente" fue el primero de tales sistemas en desarrollarse y está siendo utilizada actualmente en la mayoría de los países de Europa. Este sistema se basa en el uso de una tarjeta que comprende un microprocesador que contiene información necesaria para comunicarse con un lector de tarjetas inteligentes. Una vez que el lector de tarjetas inteligentes ha validado la propia tarjeta, un usuario introduce un número de identificación personal (PIN) en el lector y se envía la información a un dispositivo de autenticación remoto. Aunque esta solución es más segura que los sistemas de autenticación estática monofactor, las tarjetas inteligentes tienen ciertamente considerables desventajas. En primer lugar, las tarjetas inteligentes necesitan el uso de lectores de tarjetas inteligentes. Sin embargo, todo esto excluye el uso de un sistema de esta clase con dispositivos sencillos de acceso local tales como ordenadores personales. Asimismo, un usuario tiene que recordar un número PIN para cada tarjeta que esté en su posesión. Una solución a este problema es que un usuario tenga solamente un PIN para múltiples tarjetas inteligentes. Sin embargo, esta solución dejará ver que el PIN de usuario se emplea en una diversidad mucho más amplia de circunstancias, exponiendo así el PIN a más probabilidades de ser fraudulentamente utilizado. Si se interceptan una tarjeta y su PIN asociado, éstos pueden ser utilizados libremente por terceras partes malévolas.

Otra realización de un sistema de autenticación bifactor emplea parámetros biométricos de un usuario para proporcionar una segunda capa de autenticación. Por ejemplo, se han desarrollado sistemas que emplean el uso de un escáner de huella de pulgar para autenticar un usuario. Estos sistemas, aunque son seguros, son muy caros de implementar y, por tanto, no se despliegan actualmente a escala comercial. Asimismo, en situaciones en las que un usuario no es supervisado, es posible replicar huellas de pulgar a fin de contravenir estos sistemas. Por tanto, los sistemas basados en biometría no se prestan bien a una autenticación remota en línea.

Un reciente desarrollo en la materia de la autenticación de usuarios ha sido el advenimiento de la autenticación dinámica bifactor. Estos sistemas, de los que se piensa actualmente que son la más segura de todas las opciones económicamente viables, se basan en el uso de fichas que generan códigos de una manera pseudoaleatoria. Los usuarios de tales sistemas son provistos de su propia ficha que usualmente adopta la forma de un dispositivo electrónico que es lo bastante pequeño como para ser fijado a un llavero. El dispositivo electrónico utiliza un algoritmo para producir pseudoaleatoriamente una serie de códigos que se presentan al usuario. Por ejemplo, se

podría generar y presentar al usuario un nuevo código cada 60 segundos. Un dispositivo de autenticación remoto autentica el usuario basándose en una combinación de una ID de entrada, una contraseña y el código actual que aparece en la ficha. Así, cuando un usuario solicita autenticación, se introducen una ID de entrada, así como la contraseña y el código actual que aparece en la ficha. Sin embargo, estos sistemas siguen siendo vulnerables al phishing, ya que una tercera parte, una vez que haya capturado un código a través de un sitio web falsificado, podría tener hasta 60 segundos para entrar en el sitio web real o para autorizar realmente una transacción fraudulenta utilizando el nombre de entrada, la contraseña y el código actual que aparece en la ficha. Otras desventajas de este método de autenticación dinámica bifactor es la necesidad de que el usuario lleve consigo una ficha para cada institución con la que realiza transacciones, la voluminosidad de las propias fichas y los altos costes implicados en la fabricación de las fichas. Debido a esta desventaja, los sistemas de autenticación dinámica bifactor basados en fichas, aunque son bien conocidos, no son adecuados para su uso a amplia escala.

Lo que se necesita es un sistema mejorado para proporcionar autenticación dinámica bifactor.

El documento US-A-5668876 revela un método y un sistema para autenticar usuarios.

El documento WO-A-0117310 revela un sistema para mejorar la seguridad GSM para redes de datos en paquetes.

Para resolver los problemas asociados con formas de autenticación de la técnica anterior, la presente invención proporciona un método de autenticación de un usuario, comprendiendo el método los pasos de:

enviar una solicitud de autenticación a un dispositivo de autenticación remoto;

generar una primera pieza de información de autenticación;

generar, dentro del dispositivo móvil del usuario, una segunda pieza de información de autenticación que se basa al menos parcialmente en la primera pieza de información de autenticación recibida;

enviar la segunda pieza de información de autenticación al dispositivo de autenticación remoto;

validar la segunda pieza de información de autenticación; y, si la segunda pieza de información de autenticación es validada con éxito;

generar una señal de autenticación;

en donde la primera pieza de información de autenticación se recibe en el dispositivo móvil desde el terminal de acceso; caracterizado porque:

la primera pieza de información de autenticación se presenta como una imagen sobre unos medios de visualización del terminal de acceso y se captura desde éstos utilizando unos medios de adquisición óptica del dispositivo móvil; y

la primera pieza de información de autenticación contiene información transaccional relacionada con una transición que desea hacer el usuario.

El paso de generar la segunda pieza de información de autenticación puede hacerse utilizando la identidad internacional de equipo móvil (IMEI), una información relacionada con el módulo de identidad de abonado (SIM) o cualquier otra información específica del dispositivo móvil del usuario.

La segunda pieza de información de autenticación puede comprender datos biométricos.

La presente invención proporciona, además, un sistema para autenticar un usuario, comprendiendo el sistema:

unos medios emisores para enviar una solicitud de autenticación a un dispositivo de autenticación remoto;

unos medios generadores para generar una primera pieza de información de autenticación;

unos medios generadores para generar, dentro del dispositivo móvil de un usuario, una segunda pieza de información de autenticación que se basa al menos parcialmente en la primera pieza de información de autenticación recibida;

unos segundos medios emisores para enviar la segunda pieza de información de autenticación al dispositivo de autenticación remoto;

unos medios validadores para validar la segunda pieza de información de autenticación; y

unos medios generadores para generar una señal de autenticación si la segunda pieza de información de autenticación es validada con éxito por los medios validadores;

en donde el sistema está concebido de tal manera que la primera pieza de información de autenticación sea

recibida en el dispositivo móvil desde el terminal de acceso; y en donde el sistema está concebido de tal manera que la primera pieza de información de autenticación sea presentada como una imagen en unos medios de visualización del terminal de acceso y capturada desde éstos utilizando unos medios de adquisición óptica del dispositivo móvil; y la primera pieza de información de autenticación contiene información transaccional relacionada con una transición que desea hacer el usuario.

Preferiblemente, la primera pieza de información de autenticación contiene información transaccional relacionada con una transacción que desea hacer el usuario.

El sistema puede estar concebido de tal manera que la primera pieza de información de autenticación sea recibida en el dispositivo móvil desde el terminal de acceso.

El sistema puede estar concebido de tal manera que la primera pieza de información de autenticación sea capturada desde unos medios de visualización del terminal de acceso utilizando unos medios de adquisición óptica del dispositivo móvil.

El sistema puede estar concebido de tal manera que la información de autenticación sea capturada desde el terminal de acceso utilizando una cámara digital en el dispositivo móvil.

El sistema puede estar concebido de tal manera que los medios generadores generen la segunda pieza de información de autenticación utilizando la identidad internacional de equipo móvil (IMEI), una información relativa al módulo de identidad de abonado (SIM) o cualquier otra información específica del dispositivo móvil del usuario.

La segunda pieza de información de autenticación puede comprender datos biométricos.

El dispositivo móvil puede ser una ficha de hardware que comprenda:

unos medios de entrada óptica;

unos medios de procesamiento; y

unos medios de visualización.

Así, la presente invención proporciona varias ventajas con respecto a la técnica anterior. Una primera de estas ventajas es que la presente invención utiliza el poder de procesamiento cada vez mayor de los ubicuos dispositivos móviles para proporcionar una autenticación dinámica multifactor. El uso de dispositivos móviles ya ampliamente difundidos proporciona una disminución significativa en los costes de implementación y mantenimiento. Una segunda de estas ventajas es que se envía un segundo factor de autenticación de forma automática (por ejemplo, a través de BluetoothTM o SMS) o de forma semiautomática (por ejemplo, a través de un teléfono con cámara). Esto hace que el sistema de la presente invención sea mucho más fácil de utilizar y, por tanto, sea más comerciable. Además, debido al hecho de que el segundo factor de autenticación es ingresado en el dispositivo móvil de forma automática o semiautomática, el sistema puede generar mensajes con códigos más largos y con una mayor cantidad de información transaccional, proporcionando así una seguridad y utilizabilidad incrementadas.

En los dibujos:

la figura 1 es un diagrama que representa un sistema de autenticación de acuerdo con una primera realización de la presente invención;

la figura 2 es un diagrama que representa un sistema de autenticación de acuerdo con una segunda realización de la presente invención;

la figura 3 es un diagrama que representa el proceso de realización del paso S103 de la figura 2;

la figura 4 es un diagrama que representa el proceso de realización del paso S104 de la figura 2;

la figura 5 es un diagrama que representa un sistema de autenticación de acuerdo con una tercera realización de la presente invención;

la figura 6 es un diagrama que representa los procesos implicados en la realización de los pasos S203, S204 y S206 de la figura 5;

la figura 7 es un diagrama de la posible distribución de elementos de seguridad en un sistema de autenticación de acuerdo con la presente invención;

la figura 8 es un diagrama de un ejemplo de la presente invención; y

la figura 9 es un diagrama que representa una ficha de hardware de acuerdo con un ejemplo de la presente

invención.

Con referencia a la figura 1, el sistema de la presente invención comprende al menos un terminal de acceso 4. El terminal de acceso 4 puede ser un ordenador conectado en red, un terminal de punto de ventas (POS) o cualquier otro dispositivo conectado en red. El sistema comprende, además, un dispositivo de autenticación remoto 3, tal como un servidor de red. Finalmente, el sistema comprende al menos un dispositivo móvil 2, tal como un teléfono móvil, un buscapersonas o un asistente digital personal (PDA). Como alternativa, el dispositivo móvil podría ser una pieza dedicada de hardware.

Según una primera realización de la presente invención, un usuario 1 envía primeramente una solicitud de autenticación al dispositivo de autenticación remoto 3 a través del terminal de acceso 4. La solicitud de autenticación está asociada con una transacción específica que desea realizar el usuario 1. Tales transacciones pueden incluir operaciones relacionadas con servicios bancarios, transacciones de naturaleza comercial, escenarios de registro o cualquier otra transacción en la que, por alguna razón, tendría que ser autenticado un usuario 1. Como alternativa, se puede enviar una solicitud de autenticación al terminal de autenticación remoto 3 a través del dispositivo móvil 2. El dispositivo de autenticación remoto 3 genera entonces un mensaje que es enviado directamente al dispositivo móvil 2 utilizando un servicio de mensajes cortos (SMS), un servicio de mensajes multimedia (MMS) o cualquier otro medio inalámbrico de comunicación de datos (es decir, GPRS, 3G, etc.). En cualquier caso, se codifica y encripta preferiblemente el mensaje y éste puede incluir información relacionada con la transacción.

Si se le presenta el mensaje al usuario, el usuario 1 puede entonces ingresar el mensaje en el terminal de acceso 4 a fin de que éste sea enviado al dispositivo de autenticación remoto 3, o bien puede enviar el mensaje directamente al dispositivo de autenticación remoto 3 utilizando el dispositivo móvil 2. Como alternativa, en otro ejemplo de la presente invención se puede no mostrar el mensaje al usuario 1 y este mensaje puede ser enviado directamente al dispositivo de autenticación remoto 3.

En el ejemplo de un sistema en el que se le presenta el segundo mensaje al usuario 1, este usuario 1 tiene que ingresar el segundo mensaje en el terminal de acceso 4 a fin de que el segundo mensaje sea comunicado al dispositivo de autenticación remoto 3. Una vez recibido por el dispositivo de autenticación remoto 3, el segundo mensaje es entonces validado. Si se valida con éxito el segundo mensaje, se genera una señal de autenticación y ésta puede ser enviada al terminal de acceso 4 indicando que el usuario 1 ha sido autenticado por el dispositivo de autenticación remoto 3.

En el ejemplo de un sistema en el que el segundo mensaje es devuelto automáticamente al dispositivo de autenticación remoto 3 desde el dispositivo móvil 2, el usuario 1 no necesita ingresar el mensaje en el terminal de acceso 4. Al igual que en el ejemplo anterior, una vez recibido por el dispositivo de autenticación remoto 3, el segundo mensaje es entonces validado. Si se valida con éxito el segundo mensaje, se envía una señal de autenticación al terminal de acceso 4 indicando que el usuario 1 ha sido autenticado por el dispositivo de autenticación remoto 3.

El segundo mensaje puede contener más información de autenticación. Tal información podría contener información biométrica, tal como una fotografía de la cara del usuario o una huella del pulgar, que podría ser procesada en el dispositivo móvil o bien, alternativamente, enviada en forma directa al servidor de autenticación y procesada y validada en éste. Otro ejemplo de datos biométricos podría consistir en un registro de la voz del usuario, nuevamente para análisis y validación en el dispositivo móvil o en el dispositivo de autenticación.

Con referencia a la figura 2, se describirá ahora una segunda realización de la presente invención. Cuando un usuario 1 desea ser autenticado para fines de una transacción específica, tal como una transacción bancaria o comercial, el usuario 1 ingresa su información personal en un terminal de acceso 4 (paso S101). La información puede ser un nombre del usuario 1 o un nombre de cuenta y una contraseña. El terminal de acceso 4 envía entonces la información personal del usuario 1 a un dispositivo de autenticación remoto 3 a través de una red de ordenadores (paso 102), junto con información perteneciente a la transacción específica que desea realizar el usuario 1. El dispositivo de autenticación remoto 3 valida entonces el nombre del usuario o el nombre de cuenta y la contraseña del usuario 1.

Haciendo ahora referencia a la figura 2 y la figura 3, si se validan con éxito el nombre del usuario 1 o de la cuenta y la contraseña, el dispositivo de autenticación remoto 3 produce entonces un mensaje que este dispositivo encripta y codifica a fin de asegurar una detección fiable. El mensaje puede basarse parcialmente en un código aleatoriamente generado, tal como un código alfanumérico, así como en una información transaccional relacionada con la transacción solicitada (por ejemplo, transferencia de £100 de la cuenta A a la cuenta B). La adición de información transaccional proporciona una signatura de transacción que asegura la integridad de la transacción contra ataques del tipo “hombre en medio” de tal manera que los atacantes no puedan cambiar el contenido de la transacción sin ser detectados, lo cual contrasta con sistemas que se basan solamente en contraseñas dinámicas (por ejemplo, fichas) que no están asociadas con ninguna forma de información de transacción.

Finalmente, el mensaje encriptado y codificado se incrusta en una señal de cobertura de modo que la señal original

y la señal modificada sean perceptualmente indistinguibles. La señal de cobertura podría ser una señal de sonido o una señal de imagen. La señal de imagen podría ser una sola imagen o una secuencia de imágenes formadoras de una señal de vidrio. La señal encriptada y codificada puede incrustarse en una señal de imagen de cobertura utilizando cualquier forma conocida de esteganografía o de marcación de agua digital. Como alternativa, el mensaje podría codificarse en un código visual en el que el propio código sea el objeto de datos primario y no se utilice ninguna señal de cobertura. Uno de varios ejemplos de esto es el uso de un código de barras. La señal modificada es enviada después al terminal de acceso 4 (paso S103).

Haciendo ahora referencia a la figura 2 y la figura 4 y en el caso en el que la señal modificada es una señal de imagen digital, se visualiza la señal modificada en la pantalla del terminal de acceso 4 de modo que esté claramente a la vista del usuario 1. El usuario 1 utiliza entonces la cámara de su dispositivo móvil 2 para capturar la imagen del terminal de acceso 4 (paso S104). Típicamente, la imagen modificada será enviada al terminal de acceso por medio de una red de ordenadores y visualizada para el usuario por un medio de un navegador web. Como alternativa, la imagen modificada puede ser enviada al terminal de acceso por medio de un correo electrónico.

En otro ejemplo de la invención la imagen modificada podría ser enviada al terminal de acceso y seguidamente impresa en un trozo de papel o cualquier otro medio que proporcione una representación visual de la señal. Como alternativa, la señal modificada podría ser enviada al usuario sobre un trozo de papel en forma de, por ejemplo, una letra.

Una vez que se captura la imagen modificada, el dispositivo móvil 2 puede autenticar el origen de la imagen. Utilizando un software instalado en el dispositivo móvil 2, se puede procesar después la imagen para extraer el mensaje codificado y encriptado.

En el caso en que la señal modificada es una señal de sonido digital, la señal modificada es reproducida por el terminal de acceso 4 de modo que resulte audible para el usuario 1. El usuario 1 utiliza entonces un micrófono de su dispositivo móvil 2 para capturar la señal de sonido digital reproducida (paso S104). Utilizando un software instalado en el dispositivo móvil 2, se procesa después el sonido para extraer el mensaje codificado y encriptado.

En uno u otro de los casos anteriores, se descodifica y desencripta el mensaje extraído. El código generado y la información transaccional son visualizados después para el usuario 1 (paso 105). Si el usuario 1 está satisfecho en cuanto al carácter correcto de la información transaccional, puede enviar el código resultante al terminal de acceso 4 (paso S106). Se envía después el código al dispositivo de autenticación remoto 3 a fin de que sea comparado con el código que se generó originalmente en el paso S102. Si el código concuerda con el código que se generó originalmente, se autentica con éxito el usuario 1. Esto puede hacerse, por ejemplo, enviando una señal de autenticación a una tercera parte, tal como un banco o un minorista en línea, o, alternativamente, enviando una señal de autenticación a un cliente local que opere en el terminal de acceso 4.

Con referencia ahora a la figura 5 y la figura 6, se describirá una tercera realización de la presente invención. En esta realización el usuario 1 ingresa información personal, tal como un nombre y contraseña del usuario 1, en el terminal de acceso 4 (paso S201). La información personal es enviada después al dispositivo de autenticación remoto 3 a través de una red de ordenadores (paso S204), junto con detalles de la transacción que intenta realizar el usuario 1.

Una vez recibidos por el dispositivo de autenticación remoto 3, se validan la contraseña y el nombre del usuario y, si el proceso de validación tiene éxito, se añade la información perteneciente a la transacción a un código aleatoriamente generado y se encripta, codifica e intercala el mensaje resultante. El mensaje encriptado y codificado resultante puede ser incrustado después en una señal de cobertura audible o visual. Si se incrusta el mensaje encriptado y codificado en una señal de imagen, se puede utilizar cualquier forma conocida de esteganografía o de marcación de agua digital.

Como alternativa, el mensaje podría codificarse en un código visual en el que el propio código sea el objeto de datos primario y no se utilice ninguna señal de cobertura. Uno de varios ejemplos de esto es el uso de un código de barras.

En los dos casos anteriores se envía después la señal modificada al terminal de acceso 4 (paso S203).

Haciendo ahora referencia a la figura 5 y a la figura 6 y en el caso en el que la señal modificada es una señal de imagen digital, la señal de cobertura en la que se incrusta el mensaje codificado y encriptado puede ser una imagen que contenga información transaccional visual relacionada con la transacción que ha sido solicitada por el usuario 1 (por ejemplo, "£1.222 a cta. 42455434". La imagen puede ser encriptada a fin de entregarla con seguridad al terminal de acceso. La señal modificada es visualizada en la pantalla del terminal de acceso 4 de modo que esté claramente a la vista del usuario 1. El usuario 1 utiliza entonces la cámara de su dispositivo móvil 2 para capturar la imagen del terminal de acceso 4 (paso S204). Utilizando un software instalado en el dispositivo móvil 2, se procesa luego la imagen a fin de extraer el mensaje codificado y encriptado, el cual es visualizado para el usuario 1. En una realización alternativa se podría utilizar para todos los pasos de procesamiento un circuito integrado (IC) dedicado

instalado en el dispositivo móvil.

En el caso en el que la señal modificada sea una señal de audio digital, la señal de cobertura en la que se incrusta el mensaje codificado y encriptado puede ser una señal de audio conteniendo información transaccional audible, tal como una voz mecanizada que lea la frase "£1.222 a cuenta 42455434". La señal de audio modificada es reproducida después por el terminal de acceso 4 de modo que resulte audible para el usuario 1. El usuario 1 utiliza entonces el micrófono de su dispositivo móvil 2 para capturar la señal de sonido digital reproducida (paso S204). Utilizando un software instalado en el dispositivo móvil 2, se procesa luego el sonido a fin de extraer el mensaje codificado y encriptado, el cual es seguidamente reproducido de modo que resulte audible para el usuario 1. Como alternativa, el mensaje podría serle presentado al usuario en forma de texto.

Seguidamente, en los dos casos anteriores, se le proporciona al usuario 1 del dispositivo móvil 2 la oportunidad de aceptar la transacción que está siendo descrito en el mensaje o de rechazarla.

El software del dispositivo móvil 2 descodifica y desencripta el mensaje y, si la transacción es aceptada por el usuario, éste firma el mensaje antes de enviarlo al dispositivo de autenticación remoto 3. Como alternativa, el software del dispositivo móvil simplemente firma de manera digital el mensaje, sin descodificarlo ni desencriptarlo, y envía después el mensaje firmado al dispositivo de autenticación remoto 3.

Si se rechaza la transacción, el mensaje codificado y encriptado es enviado al dispositivo de autenticación remoto 3 sin firmarlo digitalmente. Como alternativa, el mensaje encriptado no podría ser enviado en absoluto y el dispositivo de autenticación tendría una función de tiempo límite que cancelaría cualquier solicitud de autenticación que durara más que un periodo de tiempo fijo. El dispositivo móvil 2 puede enviar el mensaje al dispositivo de autenticación remoto 3 a través de cualquier forma conocida de comunicación móvil (por ejemplo, SMS, MMS o GPRS estándar o 3G).

Se podría añadir también al mensaje firmado otra información específica del dispositivo móvil (tal como una ID del operador de la red). Con referencia a la figura 8, un ejemplo de la presente invención vería que el dispositivo de autenticación 3 y el terminal de acceso 4 están conectados a través de la Internet o alguna otra red de comunicación de datos. En este ejemplo, el dispositivo de autenticación 3 utilizaría información contenida en una cabecera de paquete del protocolo de Internet para determinar la dirección del protocolo de Internet del terminal de acceso 4. Una vez hecho esto, el dispositivo de autenticación verifica la localización del dispositivo móvil 2. Utilizando esta información, el dispositivo de autenticación 3 puede determinar la ubicación de las localizaciones geográficas de tanto el dispositivo móvil 2 como el terminal de acceso 4.

Si la localización geográfica del dispositivo móvil 2 y la localización geográfica del terminal de acceso 4 son las mismas, el dispositivo de autenticación 3 proseguirá con el método de autenticación. Sin embargo, si las localizaciones geográficas son diferentes, el dispositivo de autenticación 3 no proseguirá con el proceso de autenticación y no se autenticará el usuario. En un ejemplo alternativo el servidor de autenticación continuará con la autenticación del usuario, pero producirá una señal de notificación de fallo de localización geográfica que se puede utilizar después para alertar a una tercera parte sobre el hecho de que el dispositivo móvil 2 parece estar en una localización geográfica diferente con respecto a la del dispositivo de autenticación. La concordancia anterior de localizaciones geográficas puede materializarse en cualquier momento ante el usuario, si éste es autenticado con éxito.

En otro ejemplo más sencillo se puede determinar y utilizar para validación la locación geográfica de solamente el dispositivo móvil 2. Este ejemplo de la invención sería particularmente adecuado para una aplicación en la que esté restringida cierta actividad en línea dentro de localizaciones geográficas específicas (por ejemplo, juego en línea en los Estados Unidos).

Haciendo referencia nuevamente a las figuras 5 y 6, una vez que se recibe el mensaje por el dispositivo de autenticación 3, se desencripta, descodifica y luego valida el mensaje firmado. Si el mensaje firmado es validado con éxito por el dispositivo de autenticación remoto 3, se autentica con éxito el usuario 1. Esto puede hacerse, por ejemplo, enviando una señal de autenticación a una tercera parte, tal como un banco o un minorista en línea, o, como alternativa, enviando una señal de autenticación a un cliente local que opere en el terminal de acceso 4.

En cada realización de la presente invención el mensaje que ha sido descodificado y desencriptado por el dispositivo móvil puede ser enviado al dispositivo de autenticación 3 cualquier número de veces durante cualquier periodo de tiempo. Por ejemplo, la presente invención podría utilizarse para distribuir un código PIN a un usuario de modo que el usuario pudiera enviar después el código PIN al dispositivo de autenticación 3 cualquier número de veces de tal manera que el usuario pudiera ser autenticado siempre que lo deseara.

Haciendo ahora referencia a la figura 3, se describirá seguidamente una posible distribución de elementos de seguridad del sistema de autenticación de acuerdo con la presente invención. Cuando interactúa con un terminal de acceso 4, un usuario 1 puede utilizar una tarjeta magnética personalizada o tarjeta inteligente 5. Los detalles de estas tarjetas podrían ser registrados con el dispositivo de autenticación remoto 3 y podrían constituir, junto con una

contraseña que se registraría también en el dispositivo de autenticación remoto 3, el primer factor de autenticación.

La seguridad entre el dispositivo de autenticación remoto 3 y el dispositivo móvil 2 se puede implementar de diversas maneras. Un ejemplo es una criptografía asimétrica en la que se almacenaría una clave criptográfica pública en el dispositivo de autenticación remoto 3 y se almacenaría una clave privada en el dispositivo móvil 2.

Además, la información relativa a un módulo de identidad de abonado (SIM) específico en el dispositivo móvil 2 podría ser almacenada en el dispositivo de autenticación remoto 3 y utilizada como clave para encriptar el mensaje aleatoriamente registrado.

Finalmente, el número de identidad internacional de equipo móvil (IMEI) del dispositivo móvil 2 podría ser almacenado en el dispositivo de autenticación remoto 3 y utilizado como clave para encriptar el mensaje aleatoriamente generado. Así, solamente el dispositivo móvil 2 con ese IMEI específico podría desencriptar el mensaje.

Haciendo ahora referencia a la figura 9, aunque el dispositivo móvil de la presente invención puede ser un teléfono móvil, puede ser también una ficha de hardware dedicado que, por ejemplo, comprenda un módulo de cámara 10 u otros medios de captura óptica, un microcontrolador 8 para procesar la entrada de información a través del módulo de cámara 10, unos medios de memoria 9 y un módulo de visualización 11 para presentar información al usuario. El dispositivo móvil puede comprender también un escáner de huella dactilar 7 para escanear al menos una parte de una huella dactilar del usuario. El escáner de huella dactilar puede utilizarse también como disparador para accionar al menos una parte del dispositivo móvil.

REIVINDICACIONES

1. Un método de autenticación de un usuario (1), comprendiendo el método los pasos de:

enviar una solicitud de autenticación a un dispositivo de autenticación remoto (3);

generar una primera pieza de información de autenticación;

generar, dentro del dispositivo móvil del usuario, una segunda pieza de información de autenticación que se basa al menos parcialmente en la primera pieza de información de autenticación recibida;

enviar la segunda pieza de información de autenticación al dispositivo de autenticación remoto;

validar la segunda pieza de información de autenticación; y, si se valida con éxito la segunda pieza de información de autenticación,

generar una señal de autenticación;

en donde la primera pieza de información de autenticación es recibida en el dispositivo móvil (2) desde un terminal de acceso (4); **caracterizado** porque:

la primera pieza de información de autenticación es presentada como una imagen sobre unos medios de visualización del terminal de acceso (4) y capturada desde éstos utilizando unos medios de adquisición óptica del dispositivo móvil (2); y

la primera pieza de información de autenticación contiene información transaccional relacionada con una transición que desea hacer el usuario (1).

2. El método de la reivindicación 1, en el que se captura la información de autenticación del terminal de acceso (4) utilizando una cámara digital del dispositivo móvil (2).

3. El método de cualquiera de las reivindicaciones anteriores, en el que el paso de generación de la segunda pieza de información de autenticación se efectúa utilizando la identidad internacional de equipo móvil, IMEI, una información relacionada con el módulo de identidad de abonado, SIM, o cualquier otra información específica del dispositivo móvil (2) del usuario (1).

4. El método de cualquiera de las reivindicaciones anteriores, en el que la segunda pieza de información de autenticación comprende datos biométricos.

5. Un sistema de autenticación de un usuario, comprendiendo el sistema:

unos medios emisores para enviar una solicitud de autenticación a un dispositivo de autenticación remoto (3);

unos medios generadores para generar una primera pieza de información de autenticación;

unos medios generadores para generar, dentro del dispositivo móvil de un usuario (1), una segunda pieza de información de autenticación que se basa al menos parcialmente en la primera pieza de información de autenticación recibida;

unos medios emisores para enviar la segunda pieza de información de autenticación al dispositivo de autenticación remoto;

unos medios validadores para validar la segunda pieza de información de autenticación; y

unos medios generadores para generar una señal de autenticación si la segunda pieza de información de autenticación es validada con éxito por los medios validadores;

en donde el sistema está concebido de tal manera que la primera pieza de información de autenticación es recibida en el dispositivo móvil (2) desde un terminal de acceso; y

en donde el sistema **se caracteriza** porque está concebido de tal manera que la primera pieza de información de autenticación es presentada como una imagen sobre unos medios de visualización del terminal de acceso (4) y capturada desde éstos utilizando unos medios de adquisición óptica del dispositivo móvil (2); y la primera pieza de información de autenticación contiene información transaccional relacionada con una transacción que desea hacer el usuario.

6. El sistema de la reivindicación 5, en el que el sistema está concebido de tal manera que se captura la información

de autenticación del terminal de acceso (4) utilizando una cámara digital del dispositivo móvil (2).

7. El sistema de cualquiera de las reivindicaciones 5 ó 6, en el que el sistema está concebido de tal manera que los medios generadores generan la segunda pieza de información de autenticación utilizando la identidad internacional de equipo móvil, IMEI, una información relacionada con el módulo de identidad de abonado, SIM, o cualquier otra información específica del dispositivo móvil (2) del usuario (1).

8. El sistema de cualquiera de las reivindicaciones 5 a 7, en el que la segunda pieza de información de autenticación comprende datos biométricos.

9. El sistema de cualquiera de las reivindicaciones 5 a 8, en el que el dispositivo móvil (2) es una ficha de hardware que comprende:

unos medios de entrada óptica (10);

unos medios de procesamiento (8); y

unos medios de visualización (11).

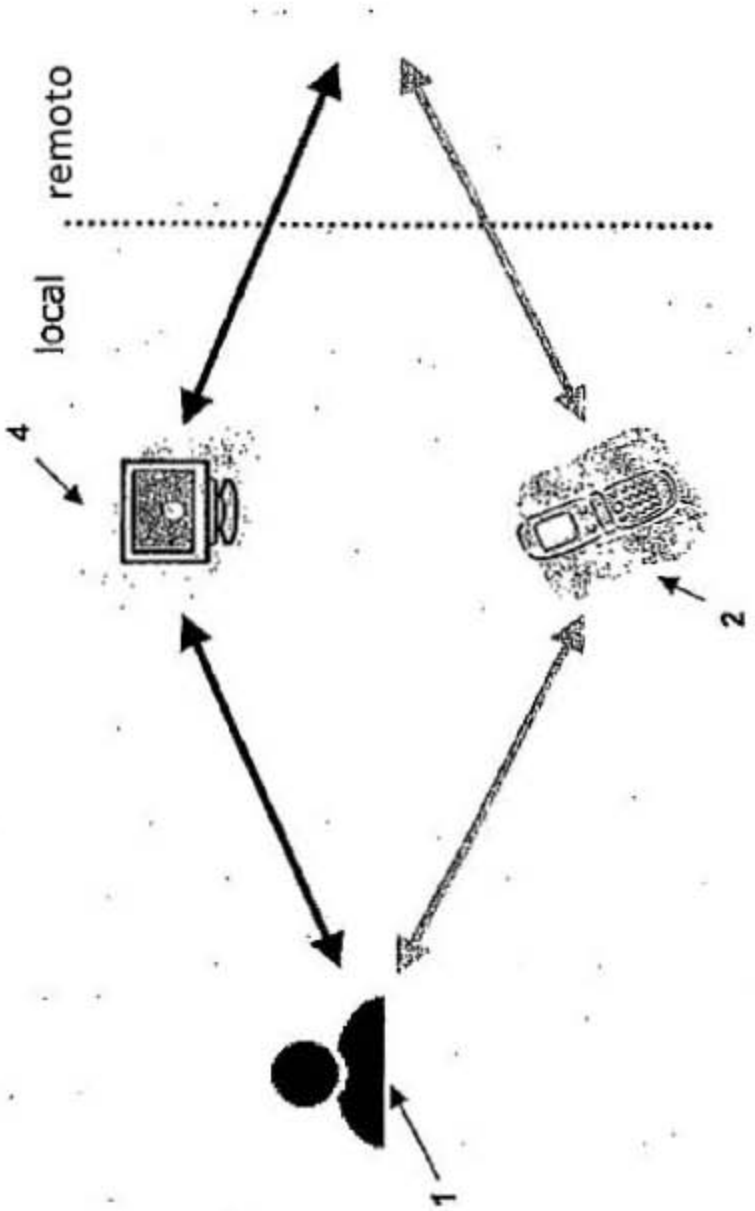

FIGURA 1

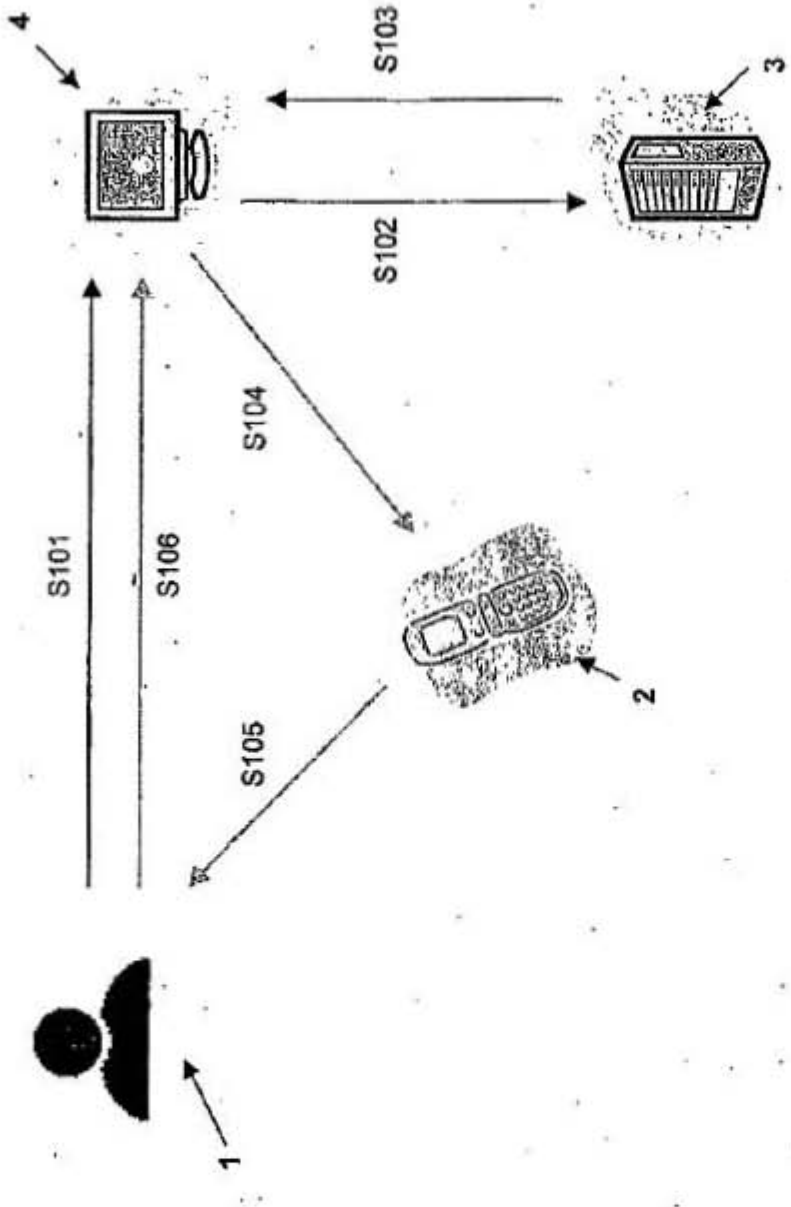

FIGURA 2

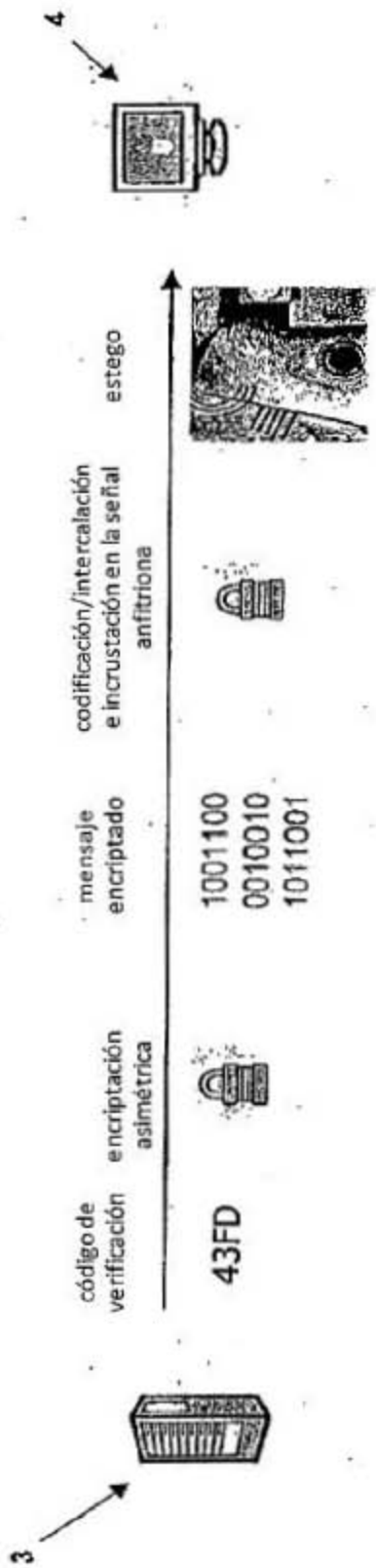

FIGURA 3

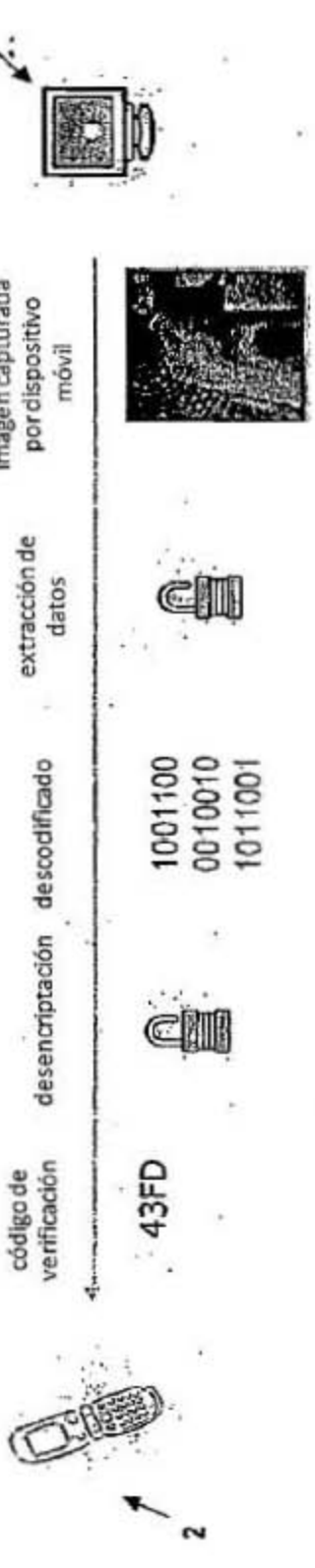

FIGURA 4

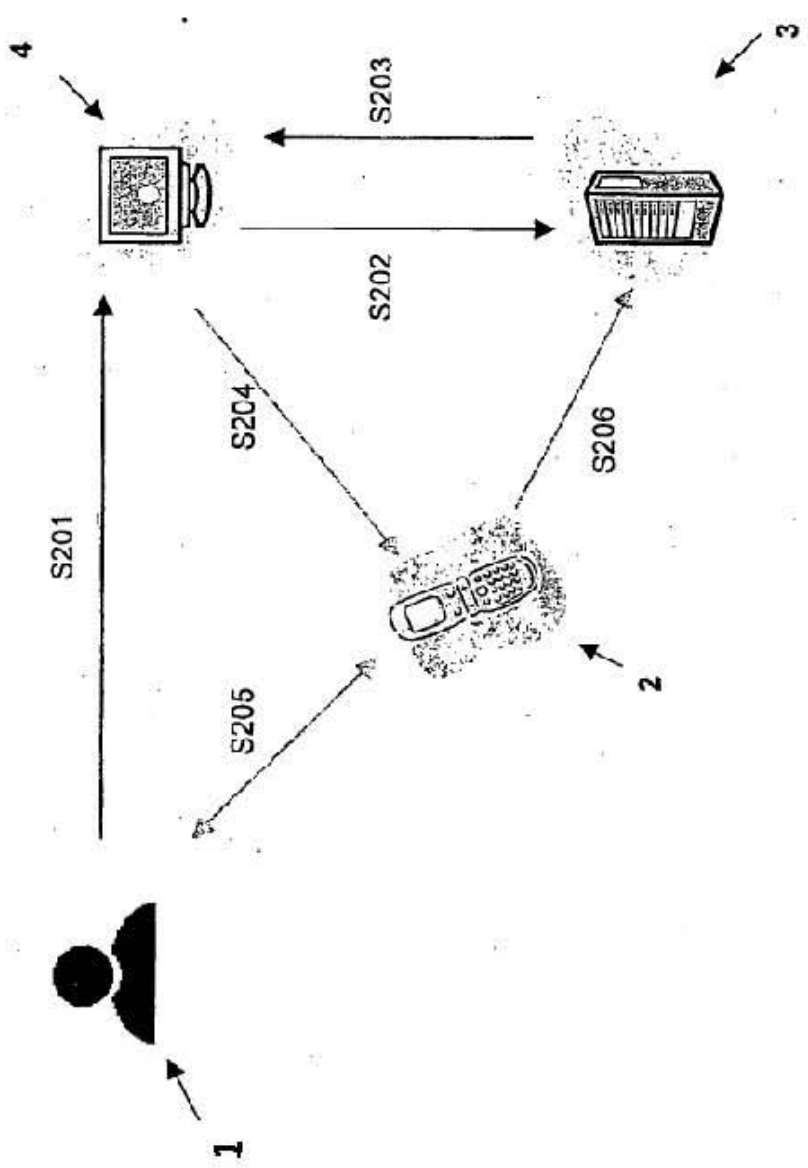

FIGURA 5

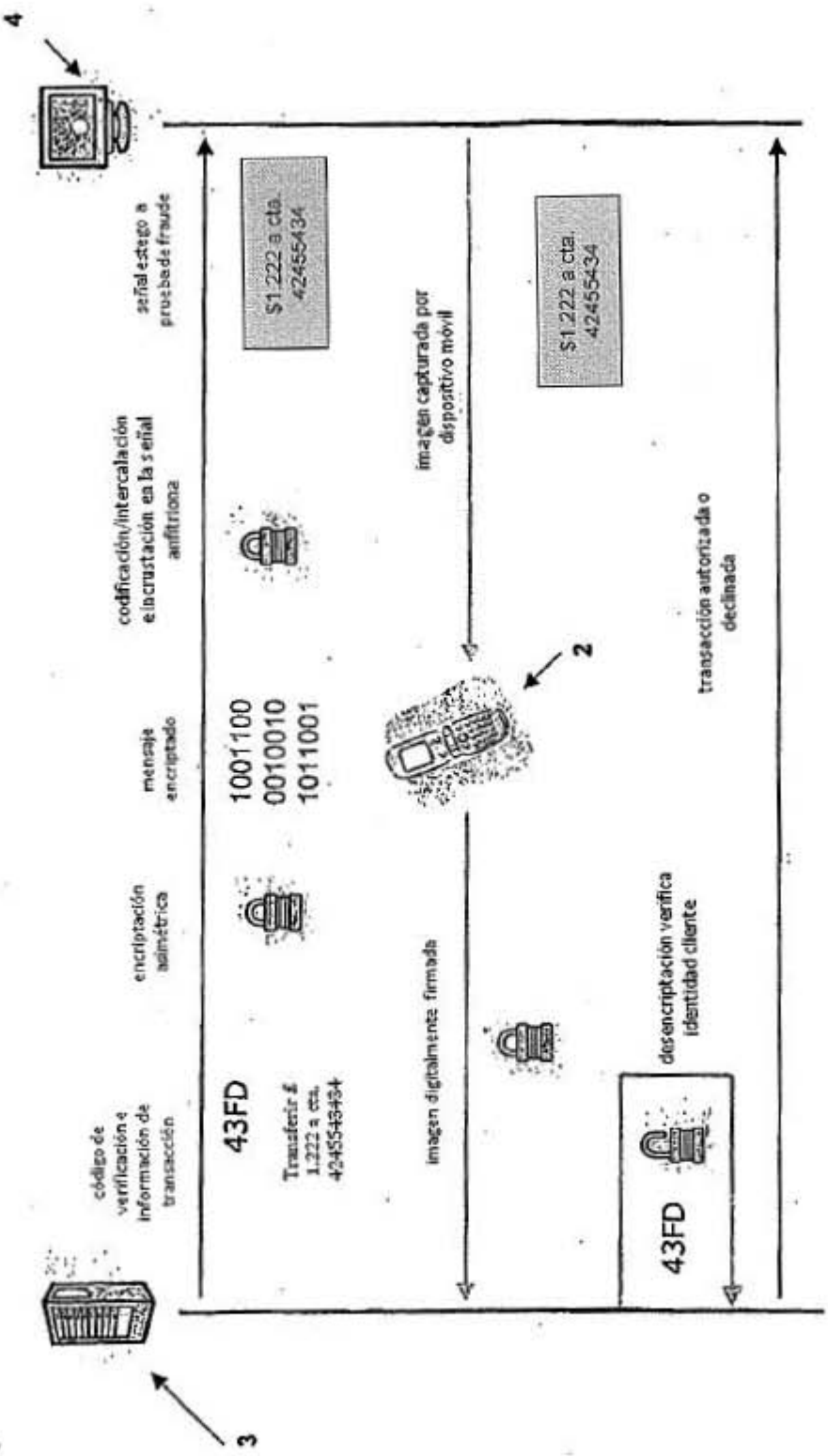
4
señal estego a prueba de fraude
codificación/intercalación e incrustación en la señal anfitriona
$1.222 a cta. 42455434
imagen capturada por dispositivo móvil
$1.222 a cta. 42455434
2
transacción autorizada o declinada
mensaje encriptado
1001100
0010010
1011001
encriptación asimétrica
43FD
Transferir $ 1.222 a cta. 42455434
imagen digitalmente firmada
desencriptación verifica identidad cliente
43FD
código de verificación e información de transacción
3

FIGURA 6

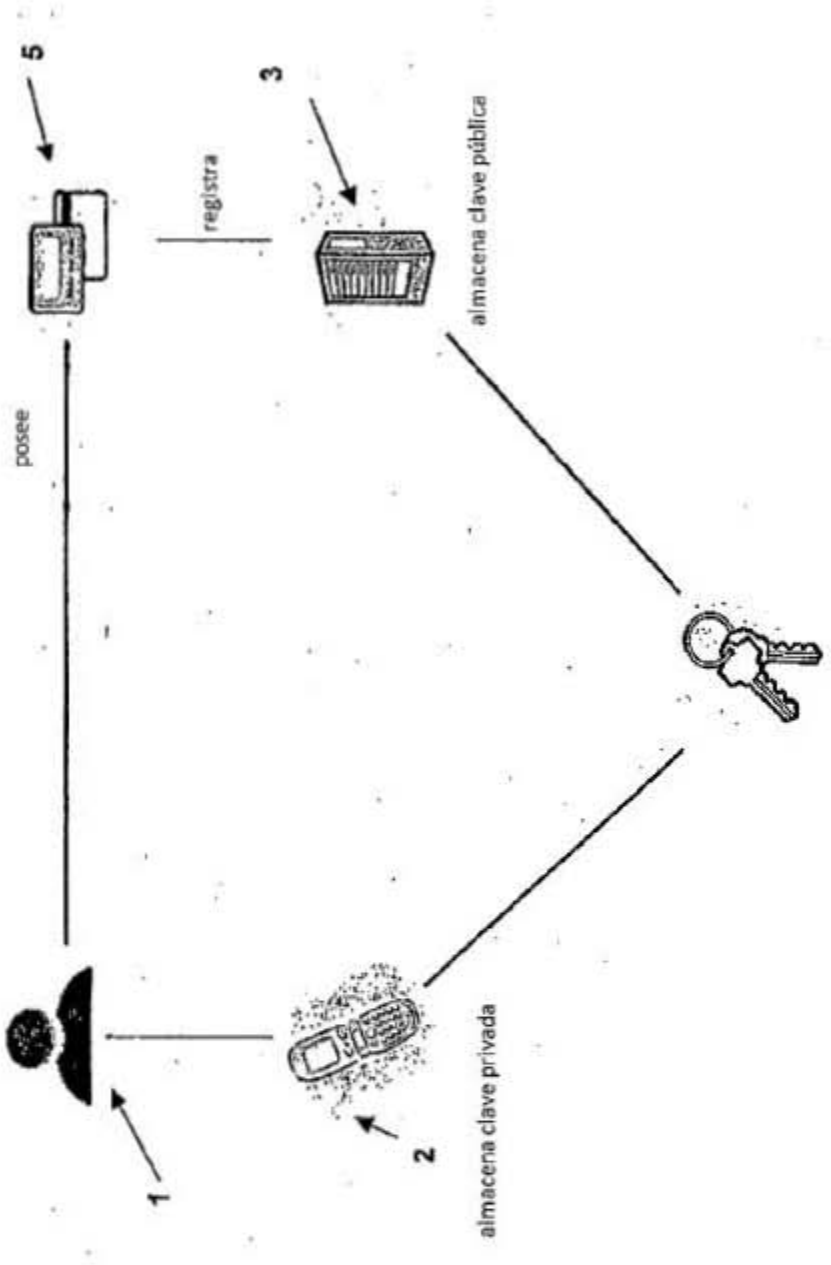
5
3
registra
almacena clave pública
posee
1
2
almacena clave privada

FIGURA 7

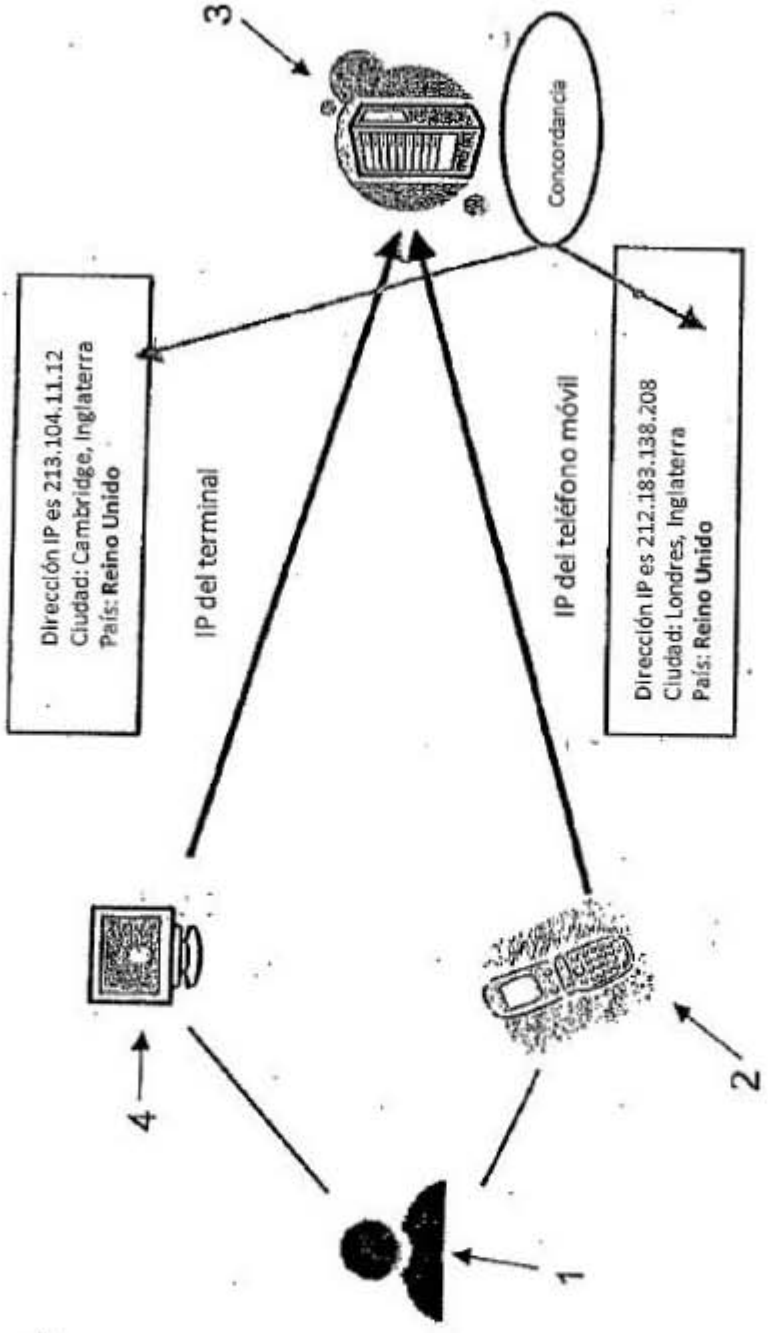
3
Concordancia
Dirección IP es 213.104.11.12
Ciudad: Cambridge, Inglaterra
País: Reino Unido
IP del terminal
IP del teléfono móvil
Dirección IP es 212.183.138.208
Ciudad: Londres, Inglaterra
País: Reino Unido
4
2
1

FIGURA 8

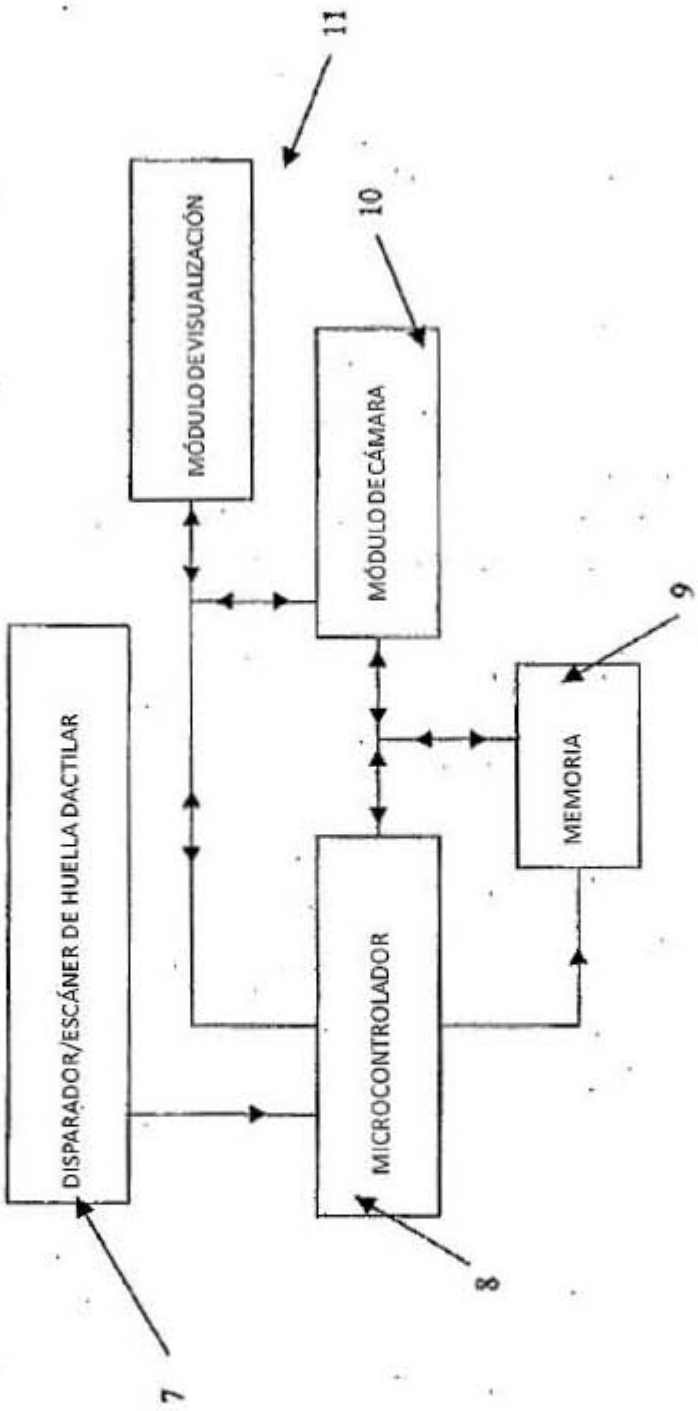
11
MÓDULO DE VISUALIZACIÓN
10
MÓDULO DE CÁMARA
9
MEMORIA
DISPARADOR/ESCÁNER DE HUELLA DACTILAR
MICROCONTROLADOR
7
8

FIGURA 9