(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 456 815**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06F 21/35 (2013.01)
G06F 21/36 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **30.10.2007 E 07858853 (0)**

(97) Fecha y número de publicación de la concesión europea: **08.01.2014 EP 2220840**

(54) Título: **Procedimientos de autenticación de los usuarios en sistemas de procesamiento de datos**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.04.2014

(73) Titular/es:

TELECOM ITALIA S.P.A. (100.0%)
Piazza degli Affari 2
20123 Milano, IT

(72) Inventor/es:

GHIRARDI, MAURIZIO

(74) Agente/Representante:

PONTI SALES, Adelaida

DESCRIPCIÓN

Procedimientos de autenticación de los usuarios en sistemas de procesamiento de datos.

Antecedentes de la invención

[0001] La presente invención se refiere en general al campo de los sistemas de procesamiento de datos o sistemas informáticos, y de las redes de datos. La invención se refiere más particularmente a procedimientos y sistemas para la autenticación de los usuarios en los sistemas de procesamiento de datos y redes de datos.

Descripción de la técnica relacionada

[0002] Con el término "autenticación" el proceso está destinado en general a como dos o más entidades, por ejemplo, una unidad de procesamiento de datos "cliente" y una unidad de procesamiento de datos "servidor" en un sistema de "cliente-servidor", pueden comprobar mutuamente su identidad.

[0003] Son conocidos varios procedimientos de autenticación de un usuario en un sistema de ordenador, que prevén la evaluación de la identidad del usuario explotando por ejemplo una o más de entre las siguientes metodologías de verificación:

- Algo que es el propio usuario (por ejemplo, mediante la explotación de los datos biométricos, tales como las huellas dactilares, la impronta vocal, el modelo de la retina, la secuencia de ADN o la caligrafía u otros identificadores biométricos del usuario);
- Algo que el usuario tiene o posee (por ejemplo, una tarjeta de identificación o un dispositivo de hardware - "token" -, por ejemplo, una clave de hardware o una "tarjeta inteligente" a acoplar a su propio ordenador, posiblemente a través de un dispositivo de lectura adecuado);
- Algo que el usuario conoce (por ejemplo, una contraseña, una palabra clave y / o un "PIN" - número de identificación personal - o un "nombre de usuario").

[0004] En el pasado, para la autenticación de un usuario este último paradigma fue el explotado principalmente: el usuario, para autenticarse en el sistema de procesamiento de datos, tenía que suministrar una combinación de nombre de usuario y contraseña.

[0005] Hoy en día, la cuestión de la autenticación de un usuario se necesita aún más que antes, como consecuencia del continuo aumento de los servicios puestos a disposición en línea a través de las redes de datos (por ejemplo, los servicios bancarios, servicios de comercio de acciones o bonos, los servicios de mensajería electrónica - "e-mail" -, "Really Simple Syndication" - RSS - servicios, grupos de noticias, etc), de los que puede disfrutar un usuario a través de una red informática (Internet, intranet de la empresa y "extranet"), y, recientemente, también los servicios de entretenimiento que implican la distribución sometida al pago de los contenidos basados en las tecnologías TDT (Televisión Digital Terrestre) e IPTV (Internet Protocol Television).

[0006] Por lo tanto, se han desarrollado mecanismos de autenticación que son más seguros y más fuertes en comparación con los mecanismos normales basados en nombre de usuario y contraseña, tales como, por ejemplo, las soluciones basadas en la detección biométrica o aquellas basadas en tokens de hardware o tarjetas inteligentes, acompañadas con software específico ("One Time Password" - OTP -, certificados digitales y análogos).

[0007] En "Authentication Using Multiple Communication Channels" por Shintaro Mizuno, Kohji Yamada, Kenji Takahashi, NTT Información Platform Sharing Laboratories, Proceedings de los 2005 workshops on Digital identity management, 2005, Fairfax, VA, USA, 11 Noviembre - 11, 2005, páginas 54 - 62, se describe un mecanismo de autenticación "solicitud de acceso-respuesta" que hace uso de un código de barras bidimensional. El sitio del proveedor de servicios envía a un ordenador del usuario, conectado a través de Internet, un código de barras que incluye una “Solicitud de acceso”; usando un teléfono celular, el usuario lee el código de barras bidimensional que se muestra en la pantalla del ordenador, utilizando de nuevo el teléfono móvil, se envía la “Solicitud de acceso”, por una red de telefonía móvil, al proveedor de servicios, a través de un servidor de autenticación, que entonces se re-envía al teléfono móvil con una firma del proveedor de servicios.

[0008] En J.M. McCune et al., "Seeing-Is-Believing: Using Chamber Phones for Human-Verifiable Authentication", Proceedings de the 2005 IEEE Symposium on Security y Privacy, 8-11 de Mayo, 2005, The Claremont Resort, Oakland, California, USA, páginas 110 - 124, se presenta un sistema que utiliza códigos de barras bidimensionales y teléfonos móviles con cámara para implementar un canal de identificación visual; el teléfono móvil tiene que ser capaz de utilizar la cámara integrada para reconocer los códigos de barras bidimensionales. El procedimiento utiliza el código de barras bidimensional para transferir a un dispositivo móvil una huella numérica (hash) que servirá para verificar una clave de autenticación que se intercambie de otra forma (comunicación por infrarrojos, bluetooth) para establecer una conexión segura con una aplicación compatible con TCG (donde TCG significa Trusted Computing Group, una organización que promueve estándares abiertos para fortalecer las plataformas de procesamiento de datos contra ataques de software).

[0009] El documento WO 2005/116909 da a conocer un aparato para obtener información que puede utilizarse para autenticar una entidad, comprendiendo el aparato: medios de captación dispuestos para capturar una imagen; un procesador de imágenes dispuesto para procesar la imagen con el fin de recuperar un bloque de texto cifrado codificado en la imagen, y un procesador de datos dispuesto para descifrar el bloque de texto cifrado con el fin de obtener la información que puede ser utilizada para autenticar la entidad. Se proporciona el uso de un par de claves de cifrado públicas -privadas.

[0010] El documento EP- A- 1713230 da a conocer un procedimiento para la configuración de una línea de comunicación segura entre un usuario y un proveedor de servicios utilizando un canal de comunicación no seguro dentro de una red insegura, que comprende los pasos de transmitir un token de identidad de una estación de usuario a una estación de proveedor de servicios ambas acopladas a la red insegura; tras la recepción del token de identidad, provocar la creación de una dirección URL secreta por la estación de proveedor de servicios; transmitir la URL secreta dentro de un canal lateral seguro a la estación de usuario; obtener, dentro de la estación de usuario, la dirección URL secreta, y establecer una nueva trayectoria de comunicación en la red insegura que une el usuario y la estación de proveedor de servicio en base a dicha dirección URL secreta. Además de descartar un *man-in-the-middle*, al negarle el acceso a los datos de flujo, también es posible detenerlo negándole el acceso al contenido del flujo de datos. Este acceso puede ser negado por el uso de un libro de códigos de una sola vez con la semántica sólo conocida por el usuario y el proveedor del servicio de autenticación.

[0011] El documento EP- A- 1713230 describe un dispositivo de seguridad para transacciones en línea entre el ordenador del proveedor de servicios y un operador equipado con un ordenador. El dispositivo comprende un sensor foto-eléctrico que se aplica a la pantalla del ordenador para identificar una señal de matriz desde el ordenador del proveedor que a continuación se procesa para generar un código y medios de comunicación que permiten que sea accesible por el operador. El dispositivo también cuenta con un sensor biométrico, en particular un sensor de huella digital con el que se introducen los datos relativos al operador. Se proporcionan unos medios de cifrado entre el sensor foto-eléctrico y los medios de comunicación que aseguran que el código determinado a partir de la pantalla sólo es accesible si la huella dactilar coincide con la almacenada en la tarjeta. El dispositivo de seguridad tiene tamaño de tarjeta de crédito y tiene una fuente de alimentación independiente.

Resumen de la invención

[0012] El solicitante ha observado que las tecnologías descritas anteriormente son bastante complejas y su coste puede crecer de forma exponencial con respecto al grado de seguridad y fiabilidad que se les pide.

[0013] Por ejemplo, en las soluciones basadas en el uso de tokens de hardware, hay en el servidor un reloj extremadamente preciso que es capaz de "sincronizarse" con el del dispositivo del usuario; las discordancias en la sincronización hacen que tanto el dispositivo de usuario como el proceso de autenticación sean inutilizables.

[0014] La técnica descrita en el artículo de Mizuno y otros tiene el problema de la necesidad de una conexión a una red de telefonía móvil, algo que no siempre es posible.

[0015] El procedimiento descrito en el artículo de McCune y otros no se utiliza para la autenticación del usuario, sino más bien para aplicaciones o dispositivos con los que se pretende establecer una conexión de datos y que utiliza algún tipo de comunicación por radio o por cable. La seguridad sólo está vinculada a la posesión del terminal.

[0016] Por lo tanto, el solicitante ha observado que existe la necesidad de poner a disposición una nueva metodología de autenticación del usuario, que tenga un alto grado de seguridad y un coste de ejecución inferior en comparación con las soluciones actualmente disponibles.

[0017] El solicitante ha encontrado una metodología que es segura y que al mismo tiempo tiene un bajo coste de implementación; dicha metodología explota un mecanismo de autenticación del tipo "Solicitud de acceso-Respuesta".

[0018] Para los propósitos de la presente invención, Para los propósitos de la presente invención "Solicitud de acceso- Respuesta " se entiende un mecanismo en el que un sujeto / entidad que desea autenticar a otra entidad, y la entidad autenticadora intentan compartir capacidades basadas en metodologías de procesamiento de datos (por ejemplo,, capacidades de cifrado / descifrado, capacidades hash, capacidades de codificación / descodificación) o información (por ejemplo, nombre de usuario, PIN, llaves de cifrado o de hash) que permiten el reconocimiento mutuo; dichos mecanismos "Solicitud de acceso- Respuestas " son, por ejemplo, explotados en el CHAP (Solicitud de acceso Handshake Autentication Protocol) o protocolos Kerberos, o en la autenticación en las redes de telefonía móvil de segunda y tercera generación. Particularmente, para los fines de la presente invención, por “Solicitud de acceso” se entiende información enviada al sujeto que tiene que ser autenticado, que se correlaciona de manera unívoca con el sujeto a ser autenticado, y que el sujeto a ser autenticado explota para mostrar que posee una capacidad determinada, la generación de la "Respuesta" correcta esperada por la entidad autenticadora.

[0019] En particular, el envío al usuario de la autenticación “Solicitud de acceso” por el sistema de procesamiento de datos, por ejemplo un servidor de autenticación, en el que el usuario desea autenticarse se hace, por ejemplo, en forma gráfica, por ejemplo, en forma de código de barras bidimensional. El contenido del gráfico “Solicitud de acceso” enviado al usuario puede, si se desea, protegerse utilizando técnicas de cifrado y/o técnicas de autenticación de información.

[0020] Para generar la "respuesta" a devolver al servidor de autenticación, el usuario utiliza un dispositivo con capacidades de captura de imagen que es distinto del ordenador a través del cual el usuario tiene que introducir la información necesaria para su autenticación. Por ejemplo, este dispositivo puede ser, ventajosamente, un teléfono móvil equipado con una cámara o cámara de vídeo, un dispositivo cada vez más difundido hoy en día, con software adecuado o firmware adaptado instalado para el reconocimiento y el procesamiento de la " Solicitud de acceso " recibida en forma gráfica.

[0021] La "respuesta" enviada por el usuario en respuesta como resultado de la transformación de la "Solicitud de acceso" recibida no contiene suficiente información para permitir recuperar la "Solicitud de acceso" a partir de la cual se ha calculado, y no puede ser utilizada por un atacante con el propósito de interferir en la comunicación entre el servidor de autenticación y el usuario o *vice versa.*

[0022] Una ventaja de la solución propuesta es que, para su funcionamiento, no requiere cobertura de radio, en particular por una red de telefonía móvil, ya que explota una lectura "óptica" de la información. Otra ventaja es que no se basa en un reloj interno para producir la información de autenticación que tiene que ser introducida.

[0023] Preferentemente, la información de autenticación producida por el servidor de autenticación, es decir, la "Solicitud de acceso" y la "respuesta" esperada como respuesta del usuario, tiene una validez temporal limitada, para evitar cualquier posible reutilización fraudulenta de estas.

[0024] Preferentemente, el servidor de autenticación puede implementar mecanismos adaptados para deshabilitar el usuario después de un número limitado, por ejemplo igual a tres, de intentos fallidos consecutivos de autenticación.

[0025] Una ventaja de la solución propuesta es que los costes de gestión se reducen en comparación con otros procedimientos de autenticación, ya que utilizan dispositivos y soluciones de software no especializados existentes.

[0026] De acuerdo con un aspecto de la presente invención, se proporciona un procedimiento de autenticación de usuarios en sistema de procesamiento de datos. El procedimiento incluye:

- generar una “Solicitud de acceso” unívocamente asociada con un usuario a autenticar;
- procesar la “Solicitud de acceso” para generar un código de respuesta esperado, para compararlo con un código de respuesta que el usuario tiene que suministrar para su autenticación;
- codificar la “Solicitud de acceso” generada para obtener una imagen representable mediante un dispositivo de representación adaptado para mostrar la imagen al usuario;
- enviar la imagen que contiene la “Solicitud de acceso” al usuario;
- representar la imagen que contiene la “Solicitud de acceso” al usuario mediante el dispositivo de representación;
- mediante un dispositivo de usuario equipado con un dispositivo de captura de imágenes, capturar ópticamente la imagen representada;
- mediante el dispositivo de usuario, procesar la imagen capturada para extraer de la imagen capturada la “Solicitud de acceso”, y subsecuentemente procesar la “Solicitud de acceso” obtenida para generar el código de respuesta;
- recibir el código de respuesta del usuario y compararlo con el código de respuesta esperado; y
- en caso de comparación positiva, autenticar el usuario, en el que una de entre dichas acciones de generar la “Solicitud de acceso” y el código de respuesta esperado, y dicha acción de procesar la imagen capturada que genera dicho código de respuesta explota una información secreta unívocamente asociada con el usuario.

[0027] Dicha generación de un código de respuesta esperado puede incluir asociar con el código de respuesta esperado un límite temporal de validez, y dicha recepción del código de respuesta del usuario y compararlo con el código de respuesta esperado incluye estimar si el código de respuesta del usuario se recibe dentro de dicho límite temporal de validez.

[0028] Dicha generación de la “Solicitud de acceso” puede incluir generar una secuencia de bits sustancialmente aleatoria.

[0029] Dicha generación de la “Solicitud de acceso” puede incluir además codificar la secuencia de bits sustancialmente aleatoria en una primera cadena de caracteres alfanuméricos que la representa unívocamente.

[0030] Dicha codificación de la “Solicitud de acceso” puede incluir además codificar la primera cadena de caracteres alfanuméricos, y codificar la primera cadena de caracteres alfanuméricos codificada para obtener la imagen representable mediante el dispositivo de representación.

[0031] Dicha generación del código de respuesta esperado puede incluir cifrar la secuencia de bits sustancialmente aleatoria con dicha información secreta o calcular una huella numérica de la secuencia de bits sustancialmente aleatoria con dicha información secreta.

[0032] Dicha generación del código de respuesta esperado puede incluir además codificar la secuencia de bits sustancialmente aleatoria cifrada, o la huella numérica de la secuencia de bits sustancialmente aleatoria, para obtener una segunda cadena de caracteres alfanuméricos y almacenar la cadena obtenida.

[0033] Dicho procesamiento de la imagen capturada para extraer de la imagen capturada la “Solicitud de acceso” y generar el código de respuesta can en particular incluye:

- descodificar la primera cadena de caracteres alfanuméricos para obtener la secuencia de bits sustancialmente aleatoria;
- cifrar la secuencia de bits sustancialmente aleatoria con dicha información secreta para obtener otra secuencia de bits sustancialmente aleatoria cifrada, o calcular una huella numérica de la secuencia de bits sustancialmente aleatoria con dicha información secreta;
- codificar la secuencia adicional de bits sustancialmente aleatoria cifrada, o la huella numérica de la secuencia de bits sustancialmente aleatoria, para obtener la segunda cadena de caracteres alfanuméricos, constituyendo dicha segunda cadena de caracteres alfanuméricos el código de respuesta.

[0034] Dicha generación de la “Solicitud de acceso” puede comprender cifrar la secuencia de bits sustancialmente aleatoria con dicha información secreta, y posiblemente codificar la secuencia de bits sustancialmente aleatoria cifrada en una primera cadena de caracteres alfanuméricos, y codificar la primera cadena de caracteres alfanuméricos para obtener la imagen representable mediante el dispositivo de representación.

[0035] Dicha generación del código de respuesta esperado puede incluir codificar la secuencia de bits sustancialmente aleatoria en una segunda cadena de caracteres alfanuméricos y almacenar la segunda cadena obtenida.

[0036] Dicho procesamiento de la imagen capturada para extraer de la imagen capturada la “Solicitud de acceso” y generar el código de respuesta puede incluir:

- descodificar la primera cadena de caracteres alfanuméricos para obtener la secuencia de bits sustancialmente aleatoria cifrada;
- descifrar la secuencia de bits sustancialmente aleatoria cifrada con dicha información secreta para obtener la secuencia de bits sustancialmente aleatoria;
- codificar la secuencia de bits sustancialmente aleatoria para obtener la segunda cadena de caracteres alfanuméricos, constituyendo dicha segunda cadena de caracteres alfanuméricos el código de respuesta.

[0037] Dicha codificación de la “Solicitud de acceso” generada para obtener una imagen puede incluir generar un código de barras bidimensional.

[0038] Dicha autenticación del usuario puede incluir permitir al usuario acceder, mediante un terminal de procesamiento de datos del usuario conectado a una red de datos, un servicio puesto a disposición por un servidor conectado a dicha red.

[0039] Dicha codificación de la “Solicitud de acceso” generada para obtener una imagen c puede comprender incluir en la imagen información resumida adaptada para identificar una transacción realizada por el usuario.

[0040] Dicho envío de la imagen que contiene la "Solicitud de acceso" al usuario puede comprender incluir la imagen en un mensaje de correo electrónico, y enviar el mensaje de correo electrónico al usuario..

[0041] Dicha autenticación del usuario puede incluir permitir al usuario mostrar un documento electrónico adjunto al mensaje de correo electrónico.

[0042] De acuerdo con otro aspecto de la presente invención, se proporciona un sistema para la autenticación de usuarios en un sistema de procesamiento de datos.

[0043] El sistema incluye:

a) un servidor de autenticación, estando dicho servidor de autenticación adaptado en uso para:

- generar una “Solicitud de acceso” unívocamente asociada con un usuario a autenticar;
- procesar la “Solicitud de acceso” para generar un código de respuesta esperado, para compararlo con un código de respuesta que el usuario tiene que suministrar para su autenticación;
- codificar la “Solicitud de acceso” generada para obtener una imagen;

- enviar la imagen que contiene la “Solicitud de acceso” a un terminal de usuario de procesamiento de datos mediante una red de datos; en el que el terminal de procesamiento de datos del usuario comprende un dispositivo de representación adaptado para representar al usuario la imagen que contiene la “Solicitud de acceso”;

b) un dispositivo de usuario equipado con un dispositivo de captura de imágenes, adaptado para capturar ópticamente la imagen representada, estando el dispositivo de usuario adaptado para procesar la imagen capturada para extraer de la imagen capturada la “Solicitud de acceso” y para procesar la “Solicitud de acceso” para generar un código de respuesta para compararlo con el código de respuesta esperado para la autenticación del usuario, en el que una de entre dichas acciones de generar una “Solicitud de acceso” y generar un código de respuesta esperado, y dicha acción de procesar la imagen capturada para generar el código de respuesta usa una información secreta unívocamente asociada con el usuario.

Breve descripción de los dibujos

[**0044]** Las características y las ventajas de la presente invención se harán evidentes mediante la siguiente descripción detallada de algunas formas de realización posibles de las mismas, proporcionadas meramente a modo de ejemplos no limitativos, descripción que se lleva a cabo haciendo referencia a los dibujos adjuntos, en los cuales:

Figure 1 muestra esquemáticamente modelo lógico de sistema de autenticación adaptado para implementar un procedimiento de autenticación según una realización de la presente invención, con los principales componentes representados y las interacciones respectivas;

La **figura 2** muestra esquemáticamente un primer modo de implementación de un procedimiento de autenticación según una realización de la presente invención, también definido en lo sucesivo como "modo simétrico";
La **figura 3** muestra esquemáticamente un segundo modo de implementación de un procedimiento de autenticación según una realización de la presente invención, también definido en lo sucesivo como "modo asimétrico";
La **figura 4** muestra esquemáticamente, en términos de las operaciones principales realizadas por los diferentes jugadores y de la información intercambiada entre ellos, una posible aplicación del modo de autenticación asimétrico, según una realización de la presente invención;
La **figura 5** muestra esquemáticamente, en términos de las operaciones principales realizadas por los diferentes jugadores y de la información intercambiada entre ellos, otra posible aplicación del modo de autenticación asimétrico, según una realización de la presente invención;
La **figura 6** muestra esquemáticamente, en términos de las operaciones principales realizadas por los diferentes jugadores y de la información intercambiada entre ellos, una posible aplicación del modo de autenticación simétrico, según una realización de la presente invención;
La **figura 7** muestra esquemáticamente, en términos de las operaciones principales realizadas por los diferentes jugadores y de la información intercambiada entre ellos, otra posible aplicación adicional del modo de autenticación asimétrico, según una realización de la presente invención;
La **figura 8A** muestra un posible aspecto de un mensaje de correo electrónico recibido por el usuario, en una posible aplicación adicional del procedimiento de autenticación según una realización de la presente invención;
La **figura 8B** muestra un posible aspecto de un adjunto al mensaje de correo electrónico de la **figura 8A,** en formato PDF, que contiene información confidencial y un enlace a un sitio de internet a través del cual se ofrecen servicios en línea;
La **figura 9** esquematiza un proceso de verificación local de la autenticidad del mensaje de correo electrónico de la **figura 8A.**

Descripción detallada de algunas realizaciones de la invención

[0045] Con referencia a los dibujos, en la **figura 1** se muestra esquemáticamente un modelo lógico de un sistema de autenticación **100** según una realización de la presente invención, donde se representan los principales elementos constitutivos y las respectivas interacciones.

[0046] En la figura, la referencia **105** identifica un servidor de autenticación, en el que los usuarios, por ejemplo el usuario denotado con la referencia **110** en la figura, que tiene un ordenador personal o terminal de usuario **115** conectado a una red de datos **120** como por ejemplo Internet, una intranet de empresa, una extranet, tiene que autenticarse para poder entrar y disfrutar de los servicios puestos a disposición por el propio servidor de autenticación **105,** o, en general, por uno o más servidores (no mostrados en la figura), que dependen de la servicios ofrecidos por el servidor de autenticación **105** para la autenticación de sus propios usuarios que soliciten explotar los servicios ofrecidos por esos otros servidores. El terminal de usuario **115** puede ser un ordenador personal convencional (PC), fijo o portátil, o cualquier otro dispositivo de procesamiento de datos.

[0047] Cada vez que el usuario **110** quiere autenticarse en el servidor de autenticación **105,** este último, después de haber recibido la solicitud de autenticación desde el terminal de usuario **115** a través de la red de datos **120**, envía una información de autenticación al terminal **115** de usuario **110**, a través de la red de datos **120.**

[0048] La información de autenticación se genera en primer lugar por el servidor de autenticación **105** por medio de un algoritmo de generación **123**, y luego es procesada por un algoritmo de procesamiento adecuado **125**; el resultado del procesamiento de la información de autenticación se almacena en un soporte de memoria **130**, por ejemplo un archivo o una base de datos en un soporte no volátil, como resultado esperado como respuesta del usuario **110**; preferentemente, una validez temporal limitada respectiva está asociado con ese resultado esperado (como se muestra esquemáticamente en la figura por el reloj **135** asociado con el soporte de memoria **130**).

[0049] Subsecuentemente, el servidor de autenticación **105** codifica en forma gráfica la información de autenticación generada previamente, por medio de un algoritmo de procesamiento de imagen **140.**

[0050] Se obtiene de este modo una información de autenticación **145** codificada en forma gráfica, que se envía por el servidor de autenticación **105** al terminal **115** del usuario **110**, a través de la red de datos **120.** Such información de autenticación **145** constituye la “Solicitud de acceso” gráfica que será recibida por el usuario **110** en su propio terminal **115.**

[0051] Una vez recibida por el terminal de usuario **115**, la información de autenticación codificada en forma gráfica, es decir, la "Solicitud de acceso" gráfica, se presenta al usuario **110** como una imagen, por ejemplo en un dispositivo de visualización **147** tal como una pantalla o un monitor de la computadora **115**, y / o posiblemente impresa en un soporte de papel por medio de una impresora (no mostrada).

[0052] El usuario **110** posee un dispositivo **150**, preferentemente un dispositivo portátil como por ejemplo un teléfono móvil, un "teléfono inteligente", una PDA ("Personal Digital Assistant") o dispositivo similar, equipado con un dispositivo óptico de captura de imágenes **155**, por ejemplo un cámara digital o una cámara de vídeo, capaz de capturar la imagen visualizada por el terminal de usuario **115** (o impresa en el soporte de papel), sin la necesidad enlace de contacto / físico de datos alguno entre el dispositivo portátil **150** y el terminal de usuario **115.**

[0053] Después de haber capturado la imagen, el dispositivo portátil **150**, por medio de un software adecuado preinstalado en él y que, cuando se ejecuta, es al menos parcialmente cargado en una memoria de trabajo **160** del dispositivo portátil **150**, lleva a cabo un procesamiento digital de la imagen capturada. En particular, a través de un algoritmo de procesamiento de imagen **165**, se extrae la "Solicitud de acceso" gráfica de la imagen capturada y decodificada. La información contenida en la “Solicitud de acceso” gráfica extraída y decodificada es procesada por un algoritmo de procesamiento **170**, capaz de proporcionar al usuario **110**, a través de un vídeo y / o de la interfaz de audio **175** presente en el dispositivo portátil **150**, la información, derivada del contenido de la “Solicitud de acceso” gráfica procesada, que el usuario **110** tendrá que devolver al servidor de autenticación **105** para ser autenticado.

[0054] Usando el terminal **115**, el usuario **110** se comunica con el servidor de autenticación **105** la información de vídeo y / o de audio proporcionada al mismo por su propio dispositivo portátil **150**; dicha información que el usuario comunica al servidor de autenticación **105** constituye la "respuesta" **180** a la "Solicitud de acceso" recibida **145**.

[0055] El servidor de autenticación **105**, después de haber recibido del usuario **110** la "respuesta" **180** a través de la red de datos **120**, por medio de un algoritmo de comparación **185** compara la información recibida por el usuario con aquella previamente almacenada en el soporte de memoria **130** como resultado esperado, en particular mediante el análisis de su validez temporal su contenido. Si la verificación da resultado positivo, el servidor de autenticación **105** comunica al usuario (a través de la red de datos **120** y el terminal **115**) que él / ella ha sido "aprobado" y autenticado, de lo contrario el fallo de la verificación se comunica preferentemente al usuario. Preferentemente, después de un número predeterminado, por ejemplo tres, de intentos fallidos consecutivos de autenticación, el usuario **110** deja de ser aceptado por el sistema; el servidor de autenticación **105**, posiblemente, puede desactivar el usuario **110**, a fin de evitar nuevos intentos de autenticación; para ser re-habilitado, el usuario, por ejemplo, tiene que ponerse en contacto con un servicio de asistencia.

[0056] En lo que sigue de la presente descripción, se describirán dos posibles modos de implementación del procedimiento de autenticación presentado anteriormente: un primer modo, que se llamará "simétrico", y un segundo modo, que se llamará "asimétrico". En breve, el modo simétrico proporciona que el algoritmo de procesamiento de **125** utilizado por el servidor de autenticación **105** y el algoritmo de procesamiento de **170** utilizado por el dispositivo portátil **150** del usuario **110** son sustancialmente idénticos, mientras que el modo asimétrico proporciona que los dos algoritmos de procesamiento son diferentes.

- Modo simétrico

[0057] En la **figura 2** se muestra esquemáticamente, en términos de las operaciones principales realizadas por los diferentes jugadores y de la información intercambiada entre ellos, el modo simétrico de implementación del procedimiento de autenticación según una realización de la presente invención.

[0058] El usuario **110** que desea explotar los servicios de autenticación proporcionados por el servidor de autenticación **105** tiene que suscribirse previamente a estos servicios. En la suscripción, se crea un perfil de usuario **110** en el servidor de autenticación **105**, y el código de identificación unívoca del usuario *UserID y* una clave de

cifrado *K* se asocian con este; el código de identificación *UserID y* la clave de cifrado *K* también se instalan entonces en el dispositivo portátil **150** del usuario **110**. El código de identificación *UserID* puede ser configurado por el usuario, o preferentemente por un administrador tras una solicitud por el usuario, directamente en el servidor de autenticación **105.** La clave de cifrado *K* puede ser suministrada al usuario de diferentes maneras, y está protegida preferentemente a través de un algoritmo de cifrado, por lo que para su uso, el usuario tendrá que introducir un código de desbloqueo que sólo él / ella conoce. En particular, la clave de cifrado *K* puede ser suministrada al usuario a través de mensajes SMS (Short Message Service), enviada a un teléfono móvil del usuario e interceptada por un software instalado en el teléfono móvil, o la clave de cifrado *K* c se puede integrar en un paquete de instalación proporcionado al usuario en la suscripción del servicio. Otra posibilidad consiste en una captura óptica de la de la clave de cifrado *K*, de una manera similar a la descrita antes para la captura de la "Solicitud de acceso" **145** (en este caso, el software instalado en el dispositivo portátil **150** del usuario tiene una clave de cifrado personal pero provisional, que se usa sólo la primera vez para la instalación de la clave de cifrado *K* que se utilizará posteriormente). Una posibilidad adicional proporciona que la clave de cifrado *K* sea pre-instalada en el dispositivo portátil **150** del usuario o en la tarjeta SIM (Subscriber Identity Module) proporcionada al usuario por un operador de una red de telefonía móvil. También son posibles combinaciones de los procedimientos anteriores: por ejemplo, la primera instalación de la clave de cifrado *K* puede tener lugar a través de envío de un mensaje SMS, y si, durante el tiempo, la clave de cifrado *K* debe ser sustituida, esto se puede hacer a través de captura óptica, o la clave de cifrado *K*, instalada inicialmente a través del paquete de instalación, puede ser reemplazada posteriormente a través de la captura óptica. El usuario también puede tener más de una clave de cifrado instalada, utilizándose las diferentes claves de cifrado para diferentes servicios de autenticación (por ejemplo, dos o más de los servicios de autenticación que se describirán en lo sucesivo).

[0059] El proceso de autenticación del usuario **110** comienza con una solicitud de autenticación explícita presentada por el usuario **110**, que, declarando su propia identidad al servidor de autenticación **105**, por ejemplo, utilizando su propio código de identificación personal *UserID,* desencadena el proceso de autenticación. En una forma de realización de la presente invención, el proceso de autenticación evoluciona tal como se describe más abajo. Las diversas fases que se describirán se identifican por los respectivos números de referencia en el dibujo.

[0060] Fase **205**. Empleando un hardware o generador de software adecuado, representado esquemáticamente por el bloque **123** en **la figura 1,** el servidor de autenticación **105** genera una “Solicitud de acceso” *CLG*; esta última puede estar, por ejemplo, constituida por una secuencia aleatoria de bits, por ejemplo al menos 128 bits de longitud (sin embargo, la longitud de la secuencia que forma la “Solicitud de acceso” *CLG* no es limitativa para los fines de la presente invención). El generador **123** de la “Solicitud de acceso” *CLG* puede utilizar por ejemplo un algoritmo de generación de secuencias aleatorias de bits que cumplan con la directiva NIST FIPS Pub 140-2.

[0061] Fase **210**. El servidor de autenticación **105** procede entonces a cifrar la “Solicitud de acceso” CLG así generada con un algoritmo de cifrado, por ejemplo un algoritmo de clave simétrica, tal como un algoritmo que cumpla con la norma AES (Advanced Encryption Standard), empleando la clave de cifrado K asociada con el usuario **110** identificado por el código de identificación personal *UserID* que el usuario **105** ha suministrado al servidor de autenticación con la solicitud de autenticación. Se obtiene así una secuencia aleatoria de bits *ECLG* (Encrypted *CLG*), por ejemplo de 128 bits de largo.

[0062] Fase **215.** El servidor de autenticación **105,** mediante un algoritmo adecuado, representado esquemáticamente por el bloque **125** en **la figura 1,** transforma la secuencia aleatoria de bits cifrada *ECLG* en una cadena de texto *AECLG* (por ejemplo de acuerdo con el código ASCII), de longitud predeterminada (por ejemplo de 10 caracteres). Preferentemente, se utiliza un alfabeto para garantizar que la cadena de texto *AECLG* así obtenida es representativa unívocamente de la secuencia aleatoria de bits cifrada *ECLG*, puede ser introducida por el usuario utilizando dispositivos convencionales de entrada de datos (teclado, ratón) de los que suele llevar un ordenador, y que no contiene ambigüedades sobre los caracteres (por ejemplo, la cadena de texto *AECLG* preferentemente no contiene al mismo tiempo los caracteres "o","O","0" o "i","l","L"). El alfabeto puede tener cualquier cardinalidad, y puede contener cualquier carácter alfanumérico (por ejemplo a.... z, A..... Z, 0.. 9, !"£$%&éèàçà@ù).

[0063] Particularmente, para transformar una secuencia aleatoria de bits independientes entre sí y uniformemente distribuidos en una cadena de texto correspondiente, se puede utilizar un algoritmo de decimación. La cadena de texto obtenida está constituida por una sucesión de símbolos, derivada de la secuencia aleatoria de bits, que también satisface el requisito de independencia y distribución uniforme. Más adelante, se describirá un ejemplo de un algoritmo, el cual, a partir de una secuencia aleatoria de bits, es capaz de derivar de la misma una cadena de texto que está constituida por símbolos pertenecientes a un alfabeto configurable (numérico o alfanumérico) y de longitud configurable.

[0064] Fase **220**. Preferentemente, el servidor de autenticación **105** establece un plazo temporal de validez de la cadena de texto *AECLG*, definido como el tiempo máximo en el servidor de autenticación **105** espera a que el usuario **110** devuelva su respuesta, que es la "Respuesta" de verificación (por ejemplo, el período de validez puede ser de algunos minutos, por ejemplo, 2 minutos).

[0065] Fase **225.** El servidor de autenticación **105** almacena la cadena *AECLG y,* cuando así se disponga, el plazo temporal de validez asociado con esta en un archivo local (mostrado esquemáticamente en la **figura 1** por el bloque **130**), esperándola para compararla con la "Respuesta" recibida por el usuario.

[0066] Fase **230.** El servidor de autenticación **105** codifica entonces la secuencia aleatoria binaria que forma la "Solicitud de acceso" *CLG* en caracteres, por ejemplo utilizando el formato Base64, de modo que se obtiene una cadena codificada *B64CLG*. Como alternativa, para reducir el número de caracteres a codificar gráficamente, es posible utilizar un procedimiento de codificación que consiste en la conversión de la secuencia aleatoria binaria *CLG* en una secuencia de bytes, y luego transformar el valor hexadecimal de cada byte de la secuencia en caracteres, de acuerdo con el alfabeto (0.. 9 a.. F). Por ejemplo, la secuencia de bits "10101010" se codifica como "AA"; de esta manera, una secuencia binaria de 128 bits se codifica como una secuencia de 32 caracteres.

[0067] Fase **235**. El servidor de autenticación **105** utiliza entonces la cadena *B64CLG* para la generación de un gráfico adecuado, el cual, a través de la red de datos **120**, se envía al terminal **115** del usuario **110.**

[0068] Fase **240**. Después de haber enviado al servidor de autenticación **105** la solicitud de autenticación, el usuario **110** activa en su propio dispositivo portátil **150** una aplicación adecuada, previamente instalada en el dispositivo portátil **150** (por ejemplo, en la fase de suscripción de los servicios ofrecidos por el servidor de autenticación **105**) capaz de capturar ópticamente la "Solicitud de acceso" gráfica **145** recibida por el servidor de autenticación **105**; preferentemente, la aplicación está protegida por un PIN de partida (número de identificación personal), que permite el acceso a la clave de cifrado *K* del usuario, mantenida de forma cifrada en el terminal.

[0069] Fase **245**. A través de su interfaz gráfica, el terminal de usuario **115** muestra en su pantalla al usuario **110** una imagen que contiene la "Solicitud de acceso" gráfica **145** recibida; a través del dispositivo portátil **150**, el usuario **110** captura la "Solicitud de acceso" gráfica mostrada, por ejemplo tomando una fotografía de la imagen de la pantalla **147** del terminal **115** en el que se muestra la "Solicitud de acceso" gráfica. Como alternativa a la representación en la pantalla **147** del terminal **145,** se puede prever la impresión de la imagen en un soporte de papel.

[0070] Fase **250**. Una aplicación adecuada (representado esquemáticamente por el bloque **165** en la Figura 1) residente en el dispositivo portátil **150** del usuario **110** analiza y extrae de la imagen fotografiada la cadena *B64CLG.*

***[*0071]** Fase **255**. La aplicación **165** en el dispositivo portátil **150** convierte entonces la cadena *B64CLG* (codificada con B64 u otra codificación, por ejemplo, la codificación hexadecimal previamente descrita) en la secuencia binaria *CLG*.

[0072] Fase **260.** El algoritmo de procesamiento **170** en el dispositivo portátil **150** cifra entonces la secuencia binaria *CLG* empleando la clave de cifrado *K* del usuario *110* (como alternativa a la clave de cifrado residente *K* en el dispositivo portátil *150*, también es posible utilizar como clave de cifrado el PIN utilizado para iniciar la aplicación de representación residente en el terminal de usuario **115**), con un algoritmo idéntico al utilizado por el servidor de autenticación **105**, obteniéndose una secuencia cifrada *ECLG*, por ejemplo de 128 de longitud.

[0073] Fase **265.** La secuencia cifrada *ECLG* así obtenida es transformada por el algoritmo de procesamiento **170** en el dispositivo portátil **150** en una cadena de texto *AECLG*, utilizando la misma metodología y el alfabeto utilizado por el servidor de autenticación **105** y que ya se ha descrito previamente.

[0074] Fase **270**. La cadena *AECLG* así obtenida se muestra al usuario **110** en una pantalla, o se anuncia vocalmente mediante el altavoz del dispositivo portátil **150**.

[0075] Fase **275.** El usuario **110**, empleando el terminal **115**, por ejemplo a través del teclado, entra la cadena *AECLG* comunicada a este por el dispositivo portátil **150**, y la cadena entrada *AECLG* se comunica a través de la red de datos **120** al servidor de autenticación **105** junto con el código de identificación personal *User-ID* del usuario. Como alternativa al uso del teclado, el usuario **110** puede usar el ratón de su terminal **115,** o es posible explotar una comunicación directa entre el dispositivo portátil **150** y el terminal de usuario **115**, por ejemplo explotando tecnología BlueTooth o NFC (Near Field Communication).

[0076] Fase **280**. El servidor de autenticación **105,** tras recibir del terminal de usuario **115** la cadena *AECLG*, que forma la "Respuesta" **180,** y empleando como referencia el código de identificación personal *User-ID* del usuario **110**, a través del algoritmo de **185** comprueba:

- si el usuario identificado por el código de identificación personal *User-ID* había solicitado previamente ser autenticado;
- La validez temporal de la respuesta del usuario **110**, en otras palabras, si la respuesta llegó dentro del intervalo de tiempo establecido por el servidor de autenticación **105** tras la generación de la "Solicitud de acceso"; y
- La exactitud de la cadena *AECLG* recibida del usuario **110**, por comparación con el valor almacenado previamente en asociación con ese código de identificación personal *User-ID.*

[0077] Fase **285**. Si el resultado de las comprobaciones anteriores es positiva, el servidor de autenticación **105** puede, por ejemplo:

- Eliminar el valor *AECLG* almacenado en el soporte de memoria **130**, para evitar cualquier intento posterior de reutilización de la misma “Solicitud de acceso”; y
- Enviar o redirigir al usuario **110** a una "página de bienvenida", para poner en evidencia la autenticación del usuario producida **110**.

[0078] En el caso de que una o más de las comprobaciones anteriores no tengan resultado positivo, el servidor de autenticación **105** puede, por ejemplo:
- Eliminar el valor *AECLG* almacenado en el soporte de memoria **130,** para evitar cualquier intento posterior de reutilización de la misma "Solicitud de acceso"; y
- Enviar o redirigir al usuario a una "página de error" que le invita a repetir el proceso de autenticación desde el principio.

[0079] En cada fallo de intento de autenticación, el servidor de autenticación puede incrementar un contador de fallos; al tercer fallo consecutivo, el usuario **110** puede ser desactivado por el servidor de autenticación **105**, una vez desactivado, el usuario **110** no puede volver a iniciar el proceso de autenticación (sin que le sea previamente permitido de nuevo por el servidor de autenticación).

[0080] Fase **290**. La aplicación residente en el dispositivo portátil **150** puede terminar de forma automática, una vez transcurrido un intervalo de tiempo predeterminado, por ejemplo un minuto, de haber comunicado al usuario el valor a devolver al servidor de autenticación **105**. El usuario **110** también puede terminar inmediatamente dicha aplicación de forma manual, posiblemente después de ser redirigido a la página de "bienvenida".

[0081] A continuación se describe un ejemplo de un algoritmo que, a partir de una secuencia de bits, en particular una secuencia aleatoria, es capaz de derivar de la misma una cadena de texto que está constituida por símbolos pertenecientes a un alfabeto configurable (numérico o alfanumérico) y de longitud configurable.

[0082] Sea *L* la longitud de la cadena de texto que se debe obtener, sea S = {s0,.., sM} el alfabeto de los símbolos que van a formar la cadena, y sea M = || S || la cardinalidad del alfabeto *S*.

[0083] A partir de la secuencia aleatoria de bits generada por el generador (hardware o software) **123**, se seleccionan T bloques I_0, I_1,..., I_T, cada uno constituido por *B* bits. El parámetro *B* se puede seleccionar de acuerdo con la siguiente regla:

$B = \log_2 M$ si M es una potencia de 2

$B = [\text{Log}_2 M] + 1$ de otro modo

[**0084]** De cada uno de los *T* bloques de bits I_0, I_1,..., I_T se obtiene el dígito decimal asociado I_0, I_1,...,, que se utiliza como un índice para seleccionar el símbolo del alfabeto S; para el *M*-ésimo bloque de bits genérico, el dígito decimal asociado es I_M. A partir de este índice, se obtiene el símbolo relacionado s_{Im}, aplicando la regla siguiente:

$S_{I\,m} = S\,[I_m]$ si $I_m < M$

$S_{I\,m}$ = Siguiente bloque de lo contrario

[**0085]** Este algoritmo tiene una tasa de pérdida de bits *P* igual a $P = (2^B - M)$. En caso de que el alfabeto de símbolos tenga una cardinalidad igual a una potencia de dos, que es $M \alpha 2^B$, no hay pérdida de bits, de lo contrario habrá un número *P* de bits no utilizados. Para reducir el número *P* de bits no utilizados, los bloques de bits se pueden seleccionar con el fin de obtener bloques de símbolos o bloques superpuestos.

[0086] El algoritmo realiza una decimación explorando los bits de cada bloque de bits de *T* en el que la secuencia de bits a transformar en una cadena de texto se divide primero desde la izquierda a la derecha, y posteriormente desde la derecha a la izquierda; de esta manera, la longitud en bits de cada bloque *T* se aumenta virtualmente, y se reduce la tasa de pérdidas *P.* En caso de que al final de la exploración desde la izquierda a la derecha y de la derecha a izquierda el algoritmo no converja, es decir, que no ha sido posible encontrar una secuencia de símbolos de longitud *L* deseada, pueden realizarse actividades dirigidas a encontrar los bits restantes, reiniciar para leer los bits del bloque genérico T de izquierda a derecha con una o ambas de las estrategias que se describen en lo sucesivo.

a) Cálculo del módulo

[**0087]** Los *B* bits leídos del bloque genérico *T* se "cartografían" con respecto al alfabeto seleccionado usando la regla del módulo:

$$s_{I_m} = S[\mathrm{mod}_M(I_m)]$$

b) Reducción del valor de *B*

***[*0088]** se reduce en uno, a fin de aumentar la probabilidad de obtener un valor numérico capaz de indexar un símbolo del alfabeto utilizado. El cálculo de *B* puede ser el siguiente:

$$K = \begin{cases} (\log_2 M) - 1 & \text{si M es una potencia de 2} \\ [\log_2 M] & \text{de otro modo} \end{cases}$$

[0089] Otro posible algoritmo que puede ser utilizado para la transformación de la secuencia aleatoria de bits que constituye la "Solicitud de acceso" *CLG* en una cadena textual proporciona las características y las modalidades de cálculo de las cantidades de *L, S, M y B* descritas anteriormente, para obtener una secuencia de caracteres de longitud predeterminada *L* realizando una sola exploración de los bloques de bits, desde la izquierda a la derecha.

[0090] Se definen las siguientes variables:

Q = número de bits que constituyen la secuencia aleatoria inicial de bits (*es decir* la “Solicitud de acceso” *CLG*);
W = número máximo de posibles intentos de mapeo de la secuencia aleatoria de bits en la cadena de texto, es decir *W* = *Q*/*B*;
Y = número de intentos de mapeo realizados; y
Z = número de símbolos de la cadena de texto de longitud *L* restante a mapear.

[0091] Usando el índice I_m calculado tal como se ha descrito anteriormente, el símbolo correspondiente s_{Im} se obtiene según la siguiente regla:

$$s_{I_m} = \begin{cases} S[I_m] & \textbf{si} \quad I_m < M \\ \textbf{Próximos K bits} & \textbf{si} \quad Z > (W - Y) \\ S[\mathrm{mod}_M(I_m)] & \textbf{si} \quad Z \equiv (W - Y) \end{cases}.$$

[0092] En cuanto el algoritmo de cifrado utilizado por el servidor de autenticación **105** y el dispositivo portátil **150** del usuario **110**, puede ser posiblemente sustituido por un algoritmo de autenticación de datos del tipo HMAC (Hashed Message Authentication Code), con tipo de mecanismo de huella numérica (hash) SHA-1 (Algoritmo Hash Seguro 1), que también genera como resultado una cadena que es una función de la clave de cifrado *K* del usuario **110**.

[0093] Como es conocido por los expertos en la materia, HMAC es un algoritmo no reversible para la autenticación de mensajes basado en una función hash. Por medio de HMAC es posible garantizar tanto la integridad como la autenticidad de un mensaje. El algoritmo HMAC utiliza una combinación del mensaje original y de una clave secreta para la generación del código. Una peculiaridad de la algoritmo HMAC es que no está ligado a una función hash en particular, y esto con el fin de permitir la sustitución de la función hash utilizada en caso de que se descubra que es débil. En la siguiente tabla, se presentan algunos ejemplos de cálculo que explotan HMAC de tipo SHA1.

Fila	Datos	Clave	Resultado del cálculo de HMAC con HASH tipo SHA1
1	1	1	**5b0c157d4e7672444c41033561554839ed1fd2d6**
2	1	marco	**a9774f9c88cc84c691ca7aaf5cf42d4f58e20ad3**
3	123456789	mirco	**404b5c7716cfe6adda7c9be1a4e0611349b99fb3**
4	123456	mirco	**caca41a07de234932f29f92e0876672f39ebdce4**
5	123456	marco	**73c90c08d7e5996a331fe89e3bd3d011068a9d28**
6	789012	marco	**5e52768fde27503da90915a2f9d8beab1a888da0**
7	789012	mirco	**510e7397ee2711be94f0ecc69a6675ab11d813d6**
8	Mirco	789012	**9e81045405f127544ad4fb38da573f96f56c6426**

[0094] Se puede apreciar que, en el ejemplo considerado, el resultado es siempre una cadena de longitud igual a 40 caracteres, independientemente del tamaño de los datos y de la clave (filas de 1 a 8); también es posible tener en cuenta que la función siempre devuelve un valor diferente para los mismos datos a transferir, puesto que la clave cambia (filas 4-7).

[0095] En una implementación práctica de la presente invención, preferentemente no se le pide al usuario entrar en el teclado de su propio terminal **115** todos los 40 caracteres generados por la función de huella numérica, sino más bien un número menor de caracteres de tal manera que es posible evaluar la exactitud del hash generado. Se ha demostrado (véase el documento RFC4635) que la función MAC tipo SHA1 ya contiene características de singularidad de la información en los primeros 96 bits, o más bien los primeros 12 bytes, y por lo tanto en los primeros 12 caracteres codificados en ASCII estándar Unicode. Dicho mecanismo se utiliza por ejemplo en "IPSEC Encapsulating Security Payload" y se describe en el documento RFC 2404. IPSEC (IP SECurity) es un estándar aplicado para lograr conexiones seguras en redes con protocolo de comunicación IP (Internet Protocol) y el protocolo "Encapsulating Security Payload" (conocido con las siglas ESP) pertenece al conjunto de protocolos IPSEC y tiene como objetivo proporcionar la confidencialidad y el control de la integridad y la autenticidad de la comunicación IPsec utilizando el mecanismo de hash descrito.

[0096] En una implementación práctica de la presente invención, en vista del hecho de que la "Solicitud de acceso" *CLG* es una secuencia aleatoria de bits, al cual, debido al carácter aleatorio, es prácticamente imposible generar más de una vez la misma secuencia, que una secuencia aleatoria genérica de bits es preferentemente válida solamente durante un tiempo limitado, y del hecho de que se utiliza un algoritmo de MAC seguro como el SHA1, es posible reducir aún más, por ejemplo de 12 a 8, el número de caracteres que el usuario tiene que entrar (estos caracteres se destacan en la tabla anterior subrayados) sin alterar sustancialmente el nivel de seguridad de la metodología general.

[0097] Se puede apreciar que la traducción que se realiza para generar la cadena *AECLG* se hace en la "Solicitud de acceso" *ECLG* cifrada, es decir, en el valor resultante de la operación de cifrado de la "Solicitud de acceso" *CLG* binaria.

[0098] En el modo de aplicación simétrica del procedimiento de acuerdo con la forma de realización de la presente invención aquí descrita, la “Solicitud de acceso” gráfica **145** generada y enviada por el servidor de autenticación **105**, mostrada por el terminal de usuario **115** y capturada por el dispositivo portátil **150**, se puede definir como "en claro", ya que la codificación realizada para la obtención de la cadena *B64CLG* se realiza en la secuencia binaria original *CLG*.

[0099] Para la codificación / decodificación de la “Solicitud de acceso” gráfica se pueden utilizar varias tecnologías de representación en dos dimensiones (2D), por ejemplo, los códigos de barras, en particular, aunque no de forma limitativa, las tecnologías DataMatrix, PDF417, colas QR, Código Aztec, MaxiCode, ya disponibles en el mercado a bajo coste.

- Modo asimétrico

[0100] En la figura **3** se muestra esquemáticamente, en términos de las operaciones principales realizadas por los diferentes jugadores y de la información intercambiada entre ellos, el modo asimétrico de implementación del procedimiento de autenticación. El modo asimétrico difiere del modo simétrico sólo en algunas fases del proceso de autenticación (son aplicables las mismas consideraciones hechas en la descripción del modo simétrico en relación con las longitudes de las secuencias de bits, de las cadenas, su generación, el alfabeto utilizable para las cadenas de texto, etc).

[0101] Al igual que en el modo simétrico, el proceso de autenticación de los usuarios **110** comienza con una solicitud de autenticación explícita enviada por el usuario **110** quien declarando su propia identidad al servidor de autenticación **105**, por ejemplo, mediante el uso de su propio código de identificación personal *UserID,* desencadena el proceso de autenticación. Tal proceso se desarrolla tal como se describe más abajo.

[0102] Fase **305**. Al igual que en el modo simétrico, utilizando un generador adecuado, hardware o software, el servidor de autenticación **105** genera la “Solicitud de acceso” *CLG*.

[0103] Fase **310**. Al igual que en el modo simétrico, el servidor de autenticación **105** cifra entonces la secuencia de bits que compone la “Solicitud de acceso” *CLG* así generada con un algoritmo de cifrado, por ejemplo un algoritmo de clave simétrica, como el AES, empleando la clave de cifrado *K* asociada con el usuario **110** identificado por el código de identificación personal usuario *ID* que el usuario ha suministrado al servidor de autenticación con la solicitud de autenticación. Se obtiene así una secuencia cifrada *ECLG*.

[0104] Fase **315**. El servidor de autenticación **105** transforma la secuencia binaria *CLG* que forma la “Solicitud de acceso” en una cadena de texto *ACLG* de longitud predeterminada (por ejemplo 10 caracteres), preferentemente

usando un alfabeto con características similares a las descritas en relación con el modo simétrico (por lo tanto, a diferencia del modo simétrico, es la secuencia aleatoria CLG "en claro", no la secuencia de cifrado *ECLG*, que se transforma en la cadena de texto *ACLG*).

[0105] Fase **320**. Preferentemente, el servidor de autenticación **105** establece un plazo temporal de validez de la cadena de texto *ACLG*, definido como el tiempo máximo en el que el servidor de autenticación espera que el usuario **110** le devuelva su respuesta, que es la "Respuesta" de verificación (también en este caso, el período de validez puede ser, por ejemplo, de algunos minutos, por ejemplo, 2 minutos).

[0106] Fase **325**. La “Solicitud de acceso” *ACLG* textual y el plazo temporal de validez asociado se almacenan en un archivo (**130** en la Figura 1) del servidor de autenticación **105**, en espera de ser verificado.

[0107] Fase **330**. La secuencia binaria cifrada *ECLG* se codifica en caracteres, por ejemplo en el formato Base64 u otra codificación, tal como se describe en conexión con el modo simétrico, obteniéndose una cadena *B64ECLG.*

[0108] Fase **335**. De manera similar al modo simétrico (pero utilizando la cadena de texto derivada de la secuencia cifrada *ECLG*, en lugar de la secuencia "en claro" *CLG*), la cadena *B64ECLG* es utilizada por el servidor de autenticación **105** para la generación de una “Solicitud de acceso” gráfica adecuada **145**, que se envía a través de la red de datos **120** al terminal **115** del usuario **110**.

[0109] Fase **340**. Al igual que en el modo simétrico, el usuario **110** inicia en su propio dispositivo portátil **150** una aplicación adecuada.

[0110] Fase **345.** Al igual que en el modo simétrico, a través de su interfaz gráfica, el terminal de usuario **115** muestra en su pantalla al usuario **110** una imagen que contiene la “Solicitud de acceso” gráfica recibida **145;** mediante el dispositivo portátil **150** el usuario **110** captura la imagen que contiene la “Solicitud de acceso” gráfica, por ejemplo él / ella toma una fotografía de la imagen visualizada que contiene la “Solicitud de acceso” gráfica. Como alternativa a la visualización en la pantalla del terminal **115**, se puede proporcionar una copia impresa de la imagen sobre un soporte de papel.

[0111] Fase **350.** La aplicación **165** residente en el dispositivo portátil **150** analiza y extrae de la imagen fotografiada la cadena *B64ECLG.*

[0112] Fase **355.** La aplicación **165** en el dispositivo portátil **150** convierte la cadena *B64ECLG* en la secuencia cifrada binaria *ECLG.*

[0113] Fase **360.** El algoritmo de procesamiento **170** en el dispositivo portátil **150** descifra la secuencia binaria cifrada *ECLG* empleando la clave de cifrado *K* del usuario (como alternativa a la clave *K* residente en el terminal también es posible utilizar como clave de cifrado el PIN utilizado para iniciar la aplicación en el terminal **115),** con un algoritmo idéntico al utilizado por el servidor de autenticación **105,** para obtener una secuencia binaria *CLG.*

[0114] Fase **365.** El dispositivo portátil **150** transforma la secuencia binaria *CLG* en una cadena de texto ACLG, utilizando la misma metodología y alfabeto utilizado por el servidor de autenticación **105.**

[0115] Fase **370**. De manera similar al modo simétrico, la cadena *AECLG* así obtenida se muestra o anuncia de manera vocal mediante el dispositivo portátil **150** al usuario **110.**

[0116] Fase **375.** De manera similar al modo simétrico, el usuario **110** comunica **105** al servidor de autenticación su código de identificación personal *User-ID* y el valor de la cadena de texto *ACLG.*

[0117] Fase **380.** De manera similar al modo simétrico, el servidor de autenticación **105,** tras recibir del terminal de usuario **115** la cadena *ACLG* y empleando como referencia el código de identificación personal *User-ID* del usuario **110** evalúa:

- si el usuario identificado por el código de identificación personal *User-ID* había solicitado previamente ser autenticado;
- La validez temporal de la respuesta del usuario **110**, en otras palabras, si la respuesta llegó dentro del intervalo de tiempo establecido;
- La exactitud de la cadena *ACLG* recibida del usuario **110,** por comparación con el valor almacenado previamente en asociación con ese código de identificación personal *User-ID.*

[0118] Fase **385.** De manera similar al modo simétrico, si el resultado de las comprobaciones anteriores es positiva, el servidor de autenticación **105** puede, por ejemplo:

- Eliminar el valor *ACLG* almacenado en el soporte **130,** para evitar cualquier intento posterior de reutilización de la misma "Solicitud de acceso";

- Enviar o redirigir al usuario **110** a una "página de bienvenida", para poner en evidencia que se produjo la autenticación del usuario **110.**

[0119] En caso de que una o más de las comprobaciones falle, el servidor de autenticación **105** puede, por ejemplo:

- Eliminar el valor *ACLG* almacenado en el soporte **130,** para evitar cualquier intento posterior de reutilización de la misma "Solicitud de acceso";
- Enviar o redirigir al usuario a una "página de error" que le invita repetir el proceso de autenticación desde el principio.

[0120] En cada fallo de intento de autenticación, el servidor de autenticación puede incrementar un contador de fallos; al tercer fracaso consecutivo, el usuario **110** puede ser desactivado por el servidor de autenticación **105**; una vez desactivado, el usuario **110** no puede volver a iniciar el proceso de autenticación sin haber sido previamente reactivado.

[0121] Fase **390.** La aplicación residente en el dispositivo portátil **150** puede terminarse automáticamente, transcurrido un tiempo predeterminado, por ejemplo de un minuto, desde que ha comunicado al usuario el valor a devolver al servidor de autenticación **105.** El usuario **110** puede rescindir inmediatamente la aplicación manualmente, posiblemente después de ser redirigido a la página de "bienvenida".

[0122] Se destaca que el algoritmo de cifrado utilizado por el servidor de autenticación **105** puede ser arbitrario, siempre que sea congruente con aquel disponible en el dispositivo portátil **150** del usuario.

[0123] Es posible apreciar que, a diferencia del modo simétrico, en el modo asimétrico la traducción realizada con el propósito de generar el elemento de verificación ACLG se realiza directamente en el valor de la “Solicitud de acceso” binaria *CLG* obtenida mediante el descifrado de la secuencia cifrada *ECLG.* La “Solicitud de acceso” gráfica **145** generada o interpretada se puede definir como enviada "no en claro" o cifrada, ya que la codificación realizada para la obtención de la cadena *B64ECLG* se realiza en la secuencia binaria cifrada *ECLG.*

[0124] Como en el caso del modo simétrico, para la codificación / decodificación de gráficos pueden utilizarse diferentes tecnologías de representación de código de barras que ya están comercialmente disponibles a bajo coste.

[0125] El procedimiento de autenticación de acuerdo con las realizaciones de la presente invención tiene varias ventajas.

[0126] Una ventaja del procedimiento de autenticación según la presente invención es que, para la adquisición de la información de autenticación enviada por el servidor de autenticación, no es necesario contacto físico con el terminal de usuario **115** (no hay cables, conexiones de radio o interfaces de intercambio de datos) para la adquisición de la información de autenticación enviada por el servidor de autenticación: la adquisición es de tipo óptico, y no hay riesgo de compromiso desde el punto de vista de seguridad.

[0127] Otra ventaja es que en la red de datos **120** nunca transita la información suficiente para poder reconstruir, a partir de los datos que se pudiesen interceptar, el contenido de información adaptada para permitir una "ingeniería inversa" o un "ataque de diccionario", con el propósito de calcular o hallar la clave de cifrado K del usuario.

[0128] Otra ventaja adicional es que no se requiere la compra de dispositivos ad hoc, sino más bien el simple uso de un dispositivo, por ejemplo, portátil, equipado con un dispositivo de captura de imágenes, por ejemplo una cámara, tal como un teléfono móvil, una PDA, etc, estando estos dispositivos ya difundidas en el mercado y al alcance de casi todos los usuarios.

[0129] Una ventaja adicional es que aunque se pueden utilizar dispositivos tales como teléfonos móviles y teléfonos inteligentes, no se requiere la cobertura de una red de telefonía móvil: es suficiente explotar las funcionalidades de captura de imágenes ofrecidas por estos dispositivos.

[0130] La codificación de la "Solicitud de acceso" puede ser cifrada para proteger la información contra la manipulación durante el transporte en la red, o no cifrada, pero protegida mediante la codificación con un algoritmo no reversible HMAC.

[0131] La codificación gráfica de la "Solicitud de acceso", en general, no puede ser alterada sin la invalidación completa del contenido transportado, lo que representa un elemento de seguridad intrínseco.

[0132] Por otra parte, como ya se ha mencionado, para la codificación gráfica pueden utilizarse diversas tecnologías de representación ya disponibles en el mercado a bajo coste.

[0133] Las clave de cifrado y y los algoritmos de criptografía y / o MAC se pueden elegir libremente. Estas claves pueden ser gestionadas tanto por un operador de telefonía móvil en cooperación con el proveedor del servicio, como

directamente por éste. En otras palabras, un proveedor genérico de los servicios on-line puede, para la autenticación de sus suscriptores, tanto contar con un servicio específico de autenticación puesto a disposición por un proveedor de servicios de autenticación, como usar una solución completamente autónoma en la que el servidor de autenticación está directamente gestionado por el proveedor de servicios en línea.

[0134] Como se ha descrito anteriormente, las claves de cifrado y/o algoritmos MAC pueden ser, por ejemplo distribuidos, en la suscripción del servicio de autenticación de modo óptico, mediante fotografía, siempre con el dispositivo portátil **150**, un gráfico adecuado que no contiene una "Solicitud de acceso", sino la clave de cifrado del usuario, o por aire (Over-The-Air OTA), a través de mensajes SMS aplicativos, y pueden residir en una tarjeta inteligente asociable en el dispositivo portátil **150**, por ejemplo, en la tarjeta SIM (Módulo de identificación del suscriptor) del teléfono móvil.

[0135] La “Solicitud de acceso” gráfica **145** enviada al usuario puede contener, además de la información necesaria para la autenticación, también otros tipos de información, como por ejemplo, el resumen de una transacción, una contraseña o un código de verificación o mensajes publicitarios.

[0136] El software de procesamiento de imágenes para la extracción de la "Solicitud de acceso" de la imagen capturada puede ser diseñada para diferentes tipos de teléfonos móviles y los ordenadores de bolsillo equipados con la cámara (por ejemplo basados en Symbian, WindowsMobile, plataformas de dispositivos de Java).

[0137] En lo que sigue de la descripción se presentarán algunos ejemplos de aplicación del procedimiento de autenticación según la presente invención.

[0138] En **la figura 4** se muestra esquemáticamente, en términos de las operaciones principales realizadas por los diferentes jugadores y de la información intercambiada entre ellos, una posible aplicación del procedimiento de autenticación según una realización de la presente invención, para el acceso a una aplicación Web.

[0139] Particularmente, la aplicación práctica que se analizará a continuación utiliza el modo asimétrico descrito anteriormente con referencia a la **Figura 3.** Las diversas fases del proceso de autenticación son aquellas descritas en relación con el modo asimétrico, al que se hace referencia, y por lo tanto no se describirán de nuevo. Sin embargo, nada impide adoptar el modo simétrico.

[0140] El usuario *Bob* tiene un PIN, que nunca transita en la red de datos **120,** y que puede tener tanto la función de clave simétrica para el cifrado y descifrado de la "Solicitud de acceso" recibida por el servidor de autenticación **105**, y de hacer accesible la clave de cifrado del usuario *K* durante la activación de la aplicación en el dispositivo portátil **150,** por ejemplo el teléfono móvil del usuario Bob.

[0141] El usuario *Bob* puede insertar su PIN en el dispositivo portátil **150** mientras está en un lugar seguro, antes de activar el proceso de autenticación.

[0142] El PIN se puede proporcionar al usuario Bob en la suscripción del servicio de autenticación, tanto en papel o en soporte electrónico, o por un tercero, por ejemplo, la operadora de telefonía móvil de los cuales el usuario Bob es un suscriptor.

[0143] Al completar con éxito el proceso de autenticación, el usuario Bob puede acceder al servicio Web que desee.

[0144] El procedimiento de autenticación se puede utilizar para acceder a más servicios, como por ejemplo los servicios de banca por Internet, el acceso a una intranet, servicios de negociación, cada uno de los cuales utiliza un PIN específico, sin la necesidad de cambios en el lado del servidor de autenticación o en el software en el teléfono móvil del usuario Bob.

[0145] En **la figura 5** se muestra esquemáticamente, en términos de las operaciones principales realizadas por los diferentes jugadores y de la información intercambiada entre ellos, una posible aplicación del procedimiento de autenticación según una realización de la presente invención para un servicio "on-line" de servicios que permite al usuario impartir disposiciones que implican el desembolso de sumas de dinero, como por ejemplo, un giro bancario, o una compra de servicios o bienes. En particular, en esta aplicación práctica del procedimiento según la invención se explota para proporcionar una contramedida frente a los ataques de tipo "Man In The Middle" durante una operación de disposición.

[0146] La aplicación práctica considerada en la **figura 5** utiliza el modo asimétrico antes descrito. Las diversas fases del proceso de autenticación son los descritos en relación con el modo asimétrico, al que se hace referencia, y no se describirán de nuevo. Sin embargo, nada impide adoptar el modo simétrico.

[0147] En la fase **305,** el servidor de autenticación **105,** por ejemplo del banco del usuario Bob, genera un resumen *SUM de* la transacción (que por ejemplo implica un escrito de banco), y este resumen *SUM* contiene la “Solicitud de acceso” *CLG* (secuencia aleatoria de bits) a utilizar para la autenticación / verificación de la autenticidad de la

disposición impartida. El resumen de la transacción *SUM* se cifra mediante el servidor de autenticación **105** empleando la clave de cifrado *K de Bob,* el resumen cifrado *ESUM* se codifica transformándolo en una cadena de texto *B64ESUM y* la cadena *B64ESUM* se transforma en forma gráfica (código de barras bidimensional) y se envía al terminal (por ejemplo un Ordenador Personal) de *Bob.* En la fase **365,** la aplicación en el teléfono móvil **150** de Bob extrae la "Solicitud de acceso" *CLG* del resumen, y en la fase **370,** mediante el teléfono móvil, el resumen *SUM de la transacción* y la "Solicitud de acceso" *CLG* se presentan a *Bob.*

[0148] Un atacante capaz de interponerse entre el usuario Bob y el servidor de autenticación **105** del banco del usuario Bob podría ser capaz de alterar la información que el usuario Bob envía al servidor de autenticación **105**, sin embargo, gracias al hecho de que la información contenida en la "Solicitud de acceso" se envía al usuario Bob junto con el resumen de la transacción, es posible garantizar un nivel de seguridad aumentado.

[0149] El atacante, incluso si es capaz de alterar la información enviada por el usuario, no está sin embargo en condiciones de alterar la información de la transacción sintética contenida en la "Solicitud de acceso" gráfica enviada por el servidor de autenticación al usuario, porque esta está cifrada.

[0150] El usuario puede darse cuenta inmediatamente de si la información recibida por el servidor de autenticación **105** se diferencia de la que ha introducido (por ejemplo, en el caso de un proyecto de banco, a un beneficiario diferente, y / o una cantidad diferente de dinero), y por lo tanto puede negar la confirmación de la transacción mediante el envío de un código de verificación erróneo o acordado, por ejemplo los dígitos "0000000".

[0151] Con el fin de confirmar la transacción, el usuario tiene que volver a enviar al servidor de autenticación **105** la "respuesta" generada a partir de la "Solicitud de acceso" recibida, y de esta manera, la confirmación de la transacción está protegida por un código de verificación unívoco. Esta estrategia permite evitar la reutilización de los mismos por un atacante que puede supervisar un cierto número de operaciones que el usuario concluyó con éxito enviando el código de verificación correcto.

[0152] También es posible que, antes de poder proceder a enviar al servidor de autenticación una disposición, el usuario tenga que autenticarse en el servidor de su / su banco, utilizando una de las metodologías descritas en lo que antecede.

[0153] En **la figura 6** se muestra esquemáticamente, en términos de las operaciones principales realizadas por los diversos jugadores y de la información intercambiada entre ellos, una posible aplicación del procedimiento de autenticación según una realización de la presente invención en el contexto de la distribución de contenidos multimedia, en particular la televisión digital a través del aire o por cable, por ejemplo, en la red telefónica (IPTV).

[0154] Esta aplicación del procedimiento de autenticación de acuerdo con la invención se dirige a proporcionar una solución capaz de aumentar el nivel de seguridad en relación con el acceso y / o las operaciones realizadas utilizando nuevos servicios (correo electrónico, de taquilla, encuestas, sondeo electrónico, vídeo bajo demanda, etc) que ofrecen las plataformas TDT e IPTV. Estas plataformas están constituidas por una interfaz de usuario, normalmente representada por un aparato de televisión, un aparato instalado en el hogar del usuario llamado "Set Top Box" (STB) o descodificador mediante el cual es posible recibir la señal digital (a través del aire en el caso de la TDT, a través de una línea de datos en el caso de la televisión por cable o por conexión de banda ancha para IPTV) a la que una línea telefónica llamada "canal de retorno" está conectada la cual, a través de módem tradicionales (V.90) o RDSI o a través de banda ancha (ADSL), permite la interacción del usuario con un centro de servicios.

[0155] En esta aplicación, se explota el modo simétrico descrito anteriormente, al que se hace referencia para la descripción detallada de las diferentes fases, y en el que se asume que se utiliza HMAC como algoritmo de verificación en lugar del cifrado. Sin embargo, nada impide utilizar el modo asimétrico.

[0156] Las características y el nivel de seguridad de la solución propuesta son análogos a los de la aplicación relacionada con el acceso a una aplicación web, ya que en el STB del usuario el estándar MHP (Multimedia Home Platform), permite la ejecución de aplicaciones interactivas con contenido gráfico según lo permitido por el código HTML y JAVA para la World Wide Web.

[0157] En **la figura 7** se muestra esquemáticamente, en términos de las operaciones principales realizadas por los diversos jugadores y de la información intercambiada entre ellos, una posible aplicación del procedimiento de autenticación según una realización de la presente invención a cajeros automáticos (Automatic Teller Machines - ATMs). En particular, el ejemplo de **la Figura** 7 se refiere al modo asimétrico descrito anteriormente.

[0158] Los cajeros automáticos se instalan normalmente tanto cerca de instituciones financieras (oficinas bancarias, por ejemplo), como en centros comerciales, y permiten sacare dinero en efectivo o realizar otras operaciones de bajo nivel, tal como la inspección el balance o el extracto bancario de la cuenta. Los cajeros automáticos representan, para las instituciones financieras, una herramienta que afecta sustancialmente a la "experiencia del cliente" de sus clientes. Sin embargo, las tarjetas bancarias para usar en cajeros automáticos a menudo se pierden o

se sustraen fraudulentamente, y esto constituye un problema bajo el punto de vista de la seguridad del sistema, que contribuye a aumentar de forma significativa los riesgos de fraude.

[0159] Son varios los problemas relacionados con el uso de tarjetas bancarias en terminales ATM.

[0160] El PIN que se solicita al usuario después de haber introducido la tarjeta de crédito en el terminal de ATM o POS (Punto de Venta), aunque corto, tiene que ser recordado y guardado en secreto por el usuario, que sin embargo a menudo, para facilitarse las cosas, lo escribe en un papel, o lo esconde dentro de un número de teléfono en una libreta de direcciones, y en algunos casos el usuario comunica el PIN a terceros (esto es por ejemplo el caso de las personas mayores que comunican el PIN a los parientes, asistentes o similares, a quiénes consideran de confianza).

[0161] El PIN debe ser introducido manualmente por el usuario en el punto de venta o terminal de ATM, y por lo tanto puede ser visto por ojos indiscretos o por medio de microcámaras.

[0162] Los almacenes de la tarjeta bancaria del PIN internamente, y el PIN, incluso si está cifrados, podría ser objeto de ataques de "fuerza bruta", por ejemplo a través de un programa que obliga a la apertura de una Archivo comprimido (ZIP) con todas las combinaciones posibles para la contraseña, hasta que se encuentra un que coincide.

[0163] La pérdida de la tarjeta de crédito es un acontecimiento que supone un problema para el usuario y, para la entidad que lo emitió, una serie de actividades onerosas con el propósito de bloquear su uso.

[0164] Los tipos de fraudes inherentes a este servicio son la clonación de la tarjeta mediante la técnica "skimmer" (duplicación de los datos contenidos en la tarjeta y captura simultánea del código secreto introducido por el usuario), y la captura de la tarjeta directamente en el terminal (por ejemplo a través de la técnica de "cocodrilo", o mediante el secuestro del propietario de la tarjeta o por hurto).

[0165] El procedimiento de autenticación según una realización de la presente invención se puede utilizar en este contexto, en particular también en los terminales de punto de venta con terminal gráfico a color o monocromo.

[0166] Dado que en este modo de aplicación el usuario tiene que introducir convencionalmente una secuencia de números en el teclado del cajero automático, el diccionario que se utiliza para traducir la secuencia aleatoria de bits que constituye la "Solicitud de acceso" original a una cadena puede utilizar exclusivamente un alfabeto numérico, en lugar de alfanumérico.

[0167] De acuerdo con esta posible aplicación del procedimiento de acuerdo con la invención, el usuario no conoce un "código válido" a introducir en el teclado del cajero automático o terminal de punto de venta, y no es necesario recordarlo, porque se le proporcionará dicho código n el momento adecuado mediante su dispositivo portátil, por ejemplo su teléfono móvil.

[0168] El PIN se utiliza para activar la aplicación en el dispositivo portátil del usuario el (que podría ser el mismo PIN que hoy en día tiene que ser introducido en el teclado del cajero automático o terminal de punto de venta) puede ser introducido antes de la operación, y en un lugar seguro (por ejemplo, en el coche o desde el cajero automático o terminal de punto de venta).

[0169] La cadena de números que el usuario introduce en el teclado del terminal de ATM o POS es válido para una sola operación o el acceso a sólo el servicio, y no se puede volver a utilizar, y por lo tanto su captura es inútil.

[0170] Las tarjetas de cajero automático ya no almacenan el PIN del usuario, y por lo tanto su duplicación, pérdida o captura no es crítica para el usuario.

[0171] El robo o la pérdida de un dispositivo portátil del usuario no pone en peligro la seguridad del sistema, ya que para la activación y el uso de la aplicación residente debe ser introducido un código (por ejemplo, el PIN).

[0172] Otra posible aplicación del procedimiento de autenticación según una realización de la presente invención está relacionada con los servicios de mensajería electrónica (e-mail).

[0173] Particularmente, la aplicación aquí considerada está destinada a proporcionar una solución capaz de aumentar el nivel de seguridad de servicios de correo electrónico con el fin de limitar el fenómeno de "phishing".

[0174] El "phishing" es un fraude informático difundido que involucra la recepción por parte del usuario de un mensaje de correo electrónico, que parece provenir de su banco o de una compañía de comercio en línea, que invita al usuario a conectarse, a través de una conexión ("hipervínculo") HTML (Hyper Text Markup Language), a una página web gestionada por el "phisher" y al parecer totalmente "similar" a la original de la firma real. Posteriormente, dentro de la página web imitada se pide al usuario que ingrese información sensible (contraseñas, número de tarjeta de crédito, etc) para poder acceder a las funcionalidades requeridas en el mensaje de correo electrónico (por

ejemplo, el cambio de la información personal, la provisión del consentimiento para el tratamiento de la información, la supresión de una operación financiera asignada erróneamente al usuario, etc.) La información proporcionada por el usuario es capturada (robada) por el "phisher" que la utilizará para llevar a cabo, en el nombre del usuario, compras indebidas o transacciones fraudulentas.

[0175] Normalmente, los mensajes de correo electrónico, también los enviados por los bancos e instituciones financieras, no están protegidos, ya que el correo electrónico se considera a menudo simplemente como una comunicación, y también los usuarios están acostumbrados a considerarlos así. A menudo, la protección sólo está relacionada con el acceso a los sitios Web de las empresas, para las que el usuario tiene que introducir su credencial cuya validez se verifica sólo en el momento de acceso. El usuario no tiene una posibilidad directa de verificar la validez del remitente y el contenido del mensaje de correo electrónico, y ni siquiera tiene la posibilidad de verificar la validez de la página web visitada.

[0176] Por tanto, existe el problema de proteger el contenido de los mensajes de correo electrónico con un sistema simple y eficaz. El mensaje de correo electrónico puede ser protegido utilizando la estrategia descrita a modo de ejemplo en lo sucesivo.

[0177] De acuerdo con una realización de la presente invención, los enlaces de hipertexto utilizables por el usuario no están directamente incluidos en el texto de un mensaje de correo electrónico.

[0178] Toda la información confidencial y sensible se coloca dentro de un documento adjunto al mensaje de correo electrónico, con un formato tal que sea modificable sólo por aquellos que lo creatron (por ejemplo, el documento adjunto puede ser un archivo en formato PDF - Portable Document Format -, protegidos contra los cambios) y cuya lectura está protegido por una contraseña. En el archivo adjunto al mensaje de correo electrónico es posible insertar, además de la información confidencial, enlaces que permiten al usuario acceder a un sitio Web, tal como el portal de un banco.

[0179] El mensaje de correo electrónico contiene la información de autenticación en forma gráfica (es decir, la “Solicitud de acceso” gráfica) generada por el servidor de autenticación en el momento de la creación del mensaje de correo electrónico.

[0180] Para aumentar el nivel de seguridad, la "Solicitud de acceso" de autenticación gráfica puede contener información adicional relacionada con el adjunto, como por ejemplo un código de verificación, partes aleatorias del mensaje, la fecha y hora de emisión, la respuesta a una "pregunta secreta" que el usuario ha definido en la suscripción del servicio.

[0181] La **Figura 8A** muestra el aspecto posible de un mensaje de correo electrónico recibido por el usuario. La **Figura 8B** muestra en su lugar el aspecto posible de un adjunto al mensaje de correo electrónico, por ejemplo en formato PDF, que contiene la información confidencial y un enlace al sitio del banco.

[0182] La **Figura 9** esquematiza un proceso de verificación local de la autenticidad del mensaje de correo electrónico.

[0183] El usuario recibe del remitente **905** el mensaje de correo electrónico **910,** y lo muestra en su terminal (por ejemplo, PC) **115,** entonces el usuario activa la aplicación en su dispositivo portátil **150** (por ejemplo el teléfono móvil), preferentemente empleando a PIN; entonces el usuario toma una fotografía, con la cámara **155** del teléfono móvil **150,** de la imagen visualizada en la pantalla del PC **115** y lee la cadena mostrada por el teléfono móvil **150** (derivada por procesamiento de la “Solicitud de acceso” gráfica, como se ha descrito anteriormente), o escucha su declamación vocal en el altavoz del teléfono móvil.

[0184] El usuario solicita entonces abrir el adjunto **915** al mensaje de correo electrónico **910,** y se presenta la solicitud de inserción de una contraseña **920** al usuario; el usuario inserta la contraseña leída previamente en o escuchada desde el teléfono móvil **150,** de modo que una aplicación residente en el PC **115** puede mostrar el contenido del adjunto **915.** De esta manera, introduciendo la contraseña correcta, el usuario se autentica, y, como resultado de la autenticación ocurrida, puede acceder al contenido informativo de los datos adjuntos.

[0185] Dentro del adjunto **915** es posible la inserción de uno o más enlaces 925 que permiten al usuario llegar al sitio Web correcto de forma segura.

[0186] Con el propósito de incrementar el nivel de seguridad general de la metodología, el sitio Web visitado por el usuario a través del enlace presente en el documento adjunto **915** podría utilizar a su vez un mecanismo de autenticación basado en una “Solicitud de acceso” gráfica y una "Respuesta" del usuario, tal como se describe más arriba. En este caso, dentro del adjunto **915** habrá una “Solicitud de acceso” gráfica adicional **930,** desde la cual el usuario puede obtener las credenciales de acceso al servicio (contraseña / PIN / ID o IDUsuario y contraseña / PIN).

[0187] De esta manera, toda la información sensible está contenida en el archivo adjunto al mensaje de correo electrónico, y que está protegido por un OTP cifrado (One Time Password), representado en forma gráfica y contenido en el mensaje de correo electrónico. El mensaje y el archivo adjunto se pueden duplicar, pero sólo para el usuario al que se dirige, haciendo por lo tanto inútil su reutilización debido a que el archivo adjunto no puede ser leído por otros usuarios.

[0188] El proceso permite que el usuario se de cuenta de inmediato si hay algo sospechoso, como por ejemplo la falta de la "Solicitud de acceso" gráfica o la imposibilidad de leerlo o de que un adjunto que no requiera la contraseña o en el que la contraseña no funciona.

[0189] La “Solicitud de acceso” gráfica no puede ser imitada, ya que para su generación, o para derivar de ella la contraseña que el usuario tiene que introducir para abrir el adjunto, es necesario conocer la clave de cifrado, compartida solamente entre el dispositivo portátil del usuario y la entidad que envía el mensaje de correo electrónico.

[0190] Esta metodología también permite leer mensajes de correo electrónico en los terminales públicos y los servicios de correo electrónico, ya que el dispositivo portátil del usuario es el único dispositivo capaz de decodificar los gráficos y derivar los códigos para la lectura del adjunto.

[0191] Otra posible aplicación de la presente invención en los servicios de correo electrónico consiste en la posibilidad de que se envíe un mensaje de correo electrónico al usuario que contenga una “Solicitud de acceso” gráfica, de la que el usuario pueda derivar, de la manera descrita, una "respuesta " a utilizar como un código de acceso a un sitio Web desde el cual obtener del remitente del mensaje una confirmación de la autenticidad del mensaje de correo electrónico recibido. La dirección (URL) del sitio Web al que conectarse puede estar contenida en la misma “Solicitud de acceso” gráfica y ser mostrada al usuario por su dispositivo portátil.

[0192] El uso del formato PDF para el adjunto permite hacer que su contenido sea no modificable.

[0193] Por otra parte, no se requiere conectividad de radio para la verificación del mensaje de correo electrónico.

[0194] La presente invención ha sido descrita aquí mediante la presentación de algunas formas de realización posibles; sin embargo, los expertos en la materia podrán hacer varios cambios a las realizaciones descritas, o idear formas de realización alternativas, sin apartarse del ámbito de protección de la invención definida en las reivindicaciones adjuntas.

[0195] Por ejemplo, podría no preverse la codificación en formato Base64, por ejemplo, en el caso en el que los gráficos utilizados para codificar la "Solicitud de acceso" soporten la transferencia de la información en forma binaria, es decir que la codificación de hexadecimal a ASCII se haga directamente por el algoritmo de procesamiento de imagen **140** cuando se genera el código de barras bidimensional.

REIVINDICACIONES

1. Procedimiento de autenticación de usuarios a utilizar en un sistema de procesamiento de datos, comprendiendo el procedimiento: en un servidor de autenticación (**105**):

- recibir una solicitud de autenticación presentada por un usuario, incluyendo la solicitud un código de identificación personal del usuario;
-generar una “Solicitud de acceso” (**205;305**) unívocamente asociada con el código de identificación personal del usuario;
- procesar la “Solicitud de acceso” (**210-225:310-325**) para generar un código de respuesta esperado, para compararlo con un código de respuesta que el usuario tiene que proporcionar para su autenticación;
- codificar la “Solicitud de acceso” generada (**230.235:330.335**) para obtener una imagen representable mediante un dispositivo de representación (**115,147**) adaptado para mostrar la imagen al usuario;
- enviar (**235:335**) la imagen que contiene la “Solicitud de acceso” al usuario;
- al nivel del dispositivo de representación del usuario (**147**) presentar al usuario la imagen que contiene la “Solicitud de acceso” mediante el dispositivo de representación;
- mediante un dispositivo de usuario (**150**) Dotado de un dispositivo de captura de imágenes (**155**), capturar ópticamente (**245:345**) la imagen representada;
- mediante el dispositivo de usuario, procesar la imagen capturada (**250,255:350,355**) para extraer de la imagen capturada la “Solicitud de acceso”, y subsecuentemente procesar la “Solicitud de acceso” obtenida (**260,265;360,365**) para generar el código de respuesta; en el servidor de autenticación (**105**):
- recibir el código de respuesta del usuario y compararlo (**280:380**) con el código de respuesta esperado; y
- en caso de comparación positiva, autenticar el usuario, en el que una de entre dichas acciones de generar una “Solicitud de acceso” y un código de respuesta esperado, y dicha acción de procesar la imagen capturada para generar dicho código de respuesta explota una información secreta unívocamente asociada con el usuario, siendo dicha información secreta una clave de cifrado compartida por el servidor de procesamiento de datos y por el dispositivo de usuario.

2. El procedimiento según la reivindicación 1, en el que dicha generación de un código de respuesta esperado incluye asociar con el código de respuesta esperado un límite temporal de validez, y recibir el código de respuesta del usuario y compararlo con el código de respuesta esperado incluye estimar si el código de respuesta del usuario se recibe dentro de dicho límite temporal de validez.

3. El procedimiento según la reivindicación 1 o la 2, en el que dicha generación de la “Solicitud de acceso” comprende generar una secuencia de bits sustancialmente aleatoria.

4. El procedimiento según la reivindicación 3, en el que dicha generación de la “Solicitud de acceso” comprende codificar la secuencia de bits sustancialmente aleatoria en una primera cadena de caracteres alfanuméricos la representan unívocamente.

5. El procedimiento según la reivindicación 4, en el que dicha codificación de la “Solicitud de acceso” comprende codificar la primera cadena de caracteres alfanuméricos, y codificar la primera cadena de caracteres alfanuméricos codificada para obtener la imagen representable mediante el dispositivo de representación.

6. El procedimiento según la reivindicación 5, en el que dicha generación del código de respuesta esperado incluye cifrar la secuencia de bits sustancialmente aleatoria con dicha información secreta o calcular una huella numérica de la secuencia de bits sustancialmente aleatoria con dicha información secreta.

7. El procedimiento según la reivindicación 6, en el que dicha generación del código de respuesta esperado incluye codificar la secuencia de bits sustancialmente aleatoria cifrada, o la huella numérica de la secuencia de bits sustancialmente aleatoria, para obtener una segunda cadena de caracteres alfanuméricos y almacenar la cadena obtenida.

8. El procedimiento según la reivindicación 7, en el que dicho procesamiento de la imagen capturada para extraer de la imagen capturada la “Solicitud de acceso” y generar el código de respuesta incluye:

- descodificar la primera cadena de caracteres alfanuméricos para obtener la secuencia de bits sustancialmente aleatoria;
- cifrar la secuencia de bits sustancialmente aleatoria con dicha información secreta para obtener una secuencia adicional de bits sustancialmente aleatoria cifrada, o calcular una huella numérica de la secuencia de bits sustancialmente aleatoria con dicha información secreta;
- codificar la secuencia adicional de bits sustancialmente aleatoria cifrada, o la huella numérica de la secuencia de bits sustancialmente aleatoria, para obtener la segunda cadena de caracteres alfanuméricos, constituyendo dicha segunda cadena de caracteres alfanuméricos el código de respuesta.

9. El procedimiento según la reivindicación 3, en el que dicha generación de la “Solicitud de acceso” comprende cifrar la secuencia de bits sustancialmente aleatoria con dicha información secreta.

10. El procedimiento según la reivindicación 9, en el que dicha generación de la “Solicitud de acceso” comprende codificar la secuencia de bits sustancialmente aleatoria cifrada en una primera cadena de caracteres alfanuméricos, y codificar la primera cadena de caracteres alfanuméricos para obtener la imagen representable mediante el dispositivo de representación.

11. El procedimiento según la reivindicación 10, en el que dicha generación del código de respuesta esperado incluye codificar la secuencia de bits sustancialmente aleatoria into una segunda cadena de caracteres alfanuméricos y almacenar la segunda cadena obtenida.

12. El procedimiento según la reivindicación 11, en el que dicho procesamiento de la imagen capturada para extraer de la imagen capturada la “Solicitud de acceso” y generar el código de respuesta incluye:

- descodificar la primera cadena de caracteres alfanuméricos para obtener la secuencia de bits sustancialmente aleatoria cifrada;
- descifrar la secuencia de bits sustancialmente aleatoria cifrada con dicha información secreta para obtener la secuencia de bits sustancialmente aleatoria;
- codificar la secuencia de bits sustancialmente aleatoria para obtener la segunda cadena de caracteres alfanuméricos, constituyendo dicha segunda cadena de caracteres alfanuméricos el código de respuesta.

13. El procedimiento según cualquiera de las reivindicaciones anteriores, en el que dicha codificación de la “Solicitud de acceso” generada para obtener una imagen comprende generar un código de barras bidimensional.

14. Un sistema para la autenticación de usuarios a utilizar en un sistema de procesamiento de datos, comprendiendo el sistema de autenticación: un terminal de procesamiento de datos del usuario, un servidor de autenticación (**105**), teniendo dicho servidor de autenticación medios adaptados para:

recibir una solicitud de autenticación presentada por un usuario, incluyendo la solicitud un código de identificación personal del usuario;
- generar una “Solicitud de acceso” (**205;305**) unívocamente asociada con el código de identificación personal del usuario;
- procesar la “Solicitud de acceso (**210-225;310-325**) para generar un código de respuesta esperado, para compararlo con un código de respuesta que el usuario tiene que proporcionar para su autenticación;
- codificar la “Solicitud de acceso” generada (**230,235;330,335**) para obtener una imagen;
- enviar (**235;335**) la imagen que contiene la “Solicitud de acceso” al terminal de procesamiento de datos (**115**) del usuario mediante una red de datos (**120**); y en el que el terminal de procesamiento de datos comprende un dispositivo de representación (**147**) adaptado para representar al usuario la imagen que contiene la “Solicitud de acceso”; comprendiendo además el sistema un dispositivo de usuario (**150**) dotado de un dispositivo de captura de imágenes (**155**), que tiene medios adaptados para capturar ópticamente la imagen visualizada, estando el dispositivo de usuario adaptado durante su utilización para procesar (**250,255;350,355**) la imagen capturada para extraer de la imagen capturada la “Solicitud de acceso” y para procesar (**260,265; 360,365**) la “Solicitud de acceso” para generar un código de respuesta; y en el que el servidor de autenticación tiene medios adaptados para: recibir el código de respuesta del usuario y compararlo con el código de respuesta esperado; y en caso de comparación positiva, autenticar el usuario, en el que uno de entre dichos medios adaptados para generar una “Solicitud de acceso” y generar un código de respuesta esperado, y dichos medios adaptados para procesar la imagen capturada para generar el código de respuesta están adaptados para explotar una información secreta unívocamente asociada con el usuario, siendo dicha información secreta una clave de cifrado compartida por el servidor de procesamiento de datos y por el dispositivo de usuario.

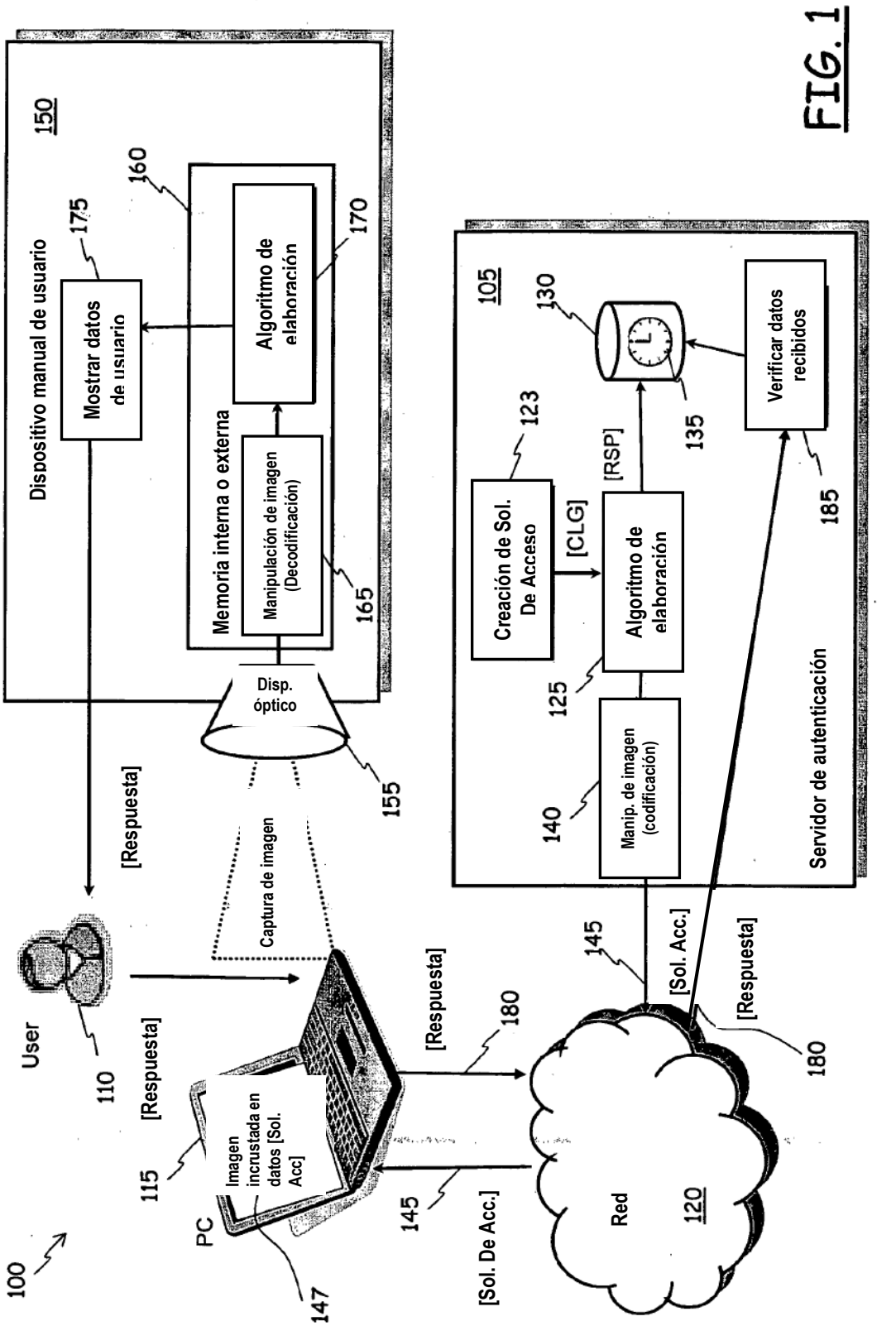

100
User
110
[Respuesta]
Captura de imagen
Dispositivo manual de usuario
150
Mostrar datos de usuario
175
160
Memoria interna o externa
Manipulación de imagen (Decodificación)
165
Algoritmo de elaboración
170
Disp. óptico
155
[Respuesta]
115
Imagen incrustada en datos [Sol. Acc]
PC
147
[Sol. De Acc.]
145
[Respuesta]
180
Red
120
[Sol. Acc.]
145
[Respuesta]
180
Servidor de autenticación
105
Manip. de imagen (codificación)
140
Algoritmo de elaboración
125
[CLG]
Creación de Sol. De Acceso
123
[RSP]
130
135
Verificar datos recibidos
185

FIG. 1

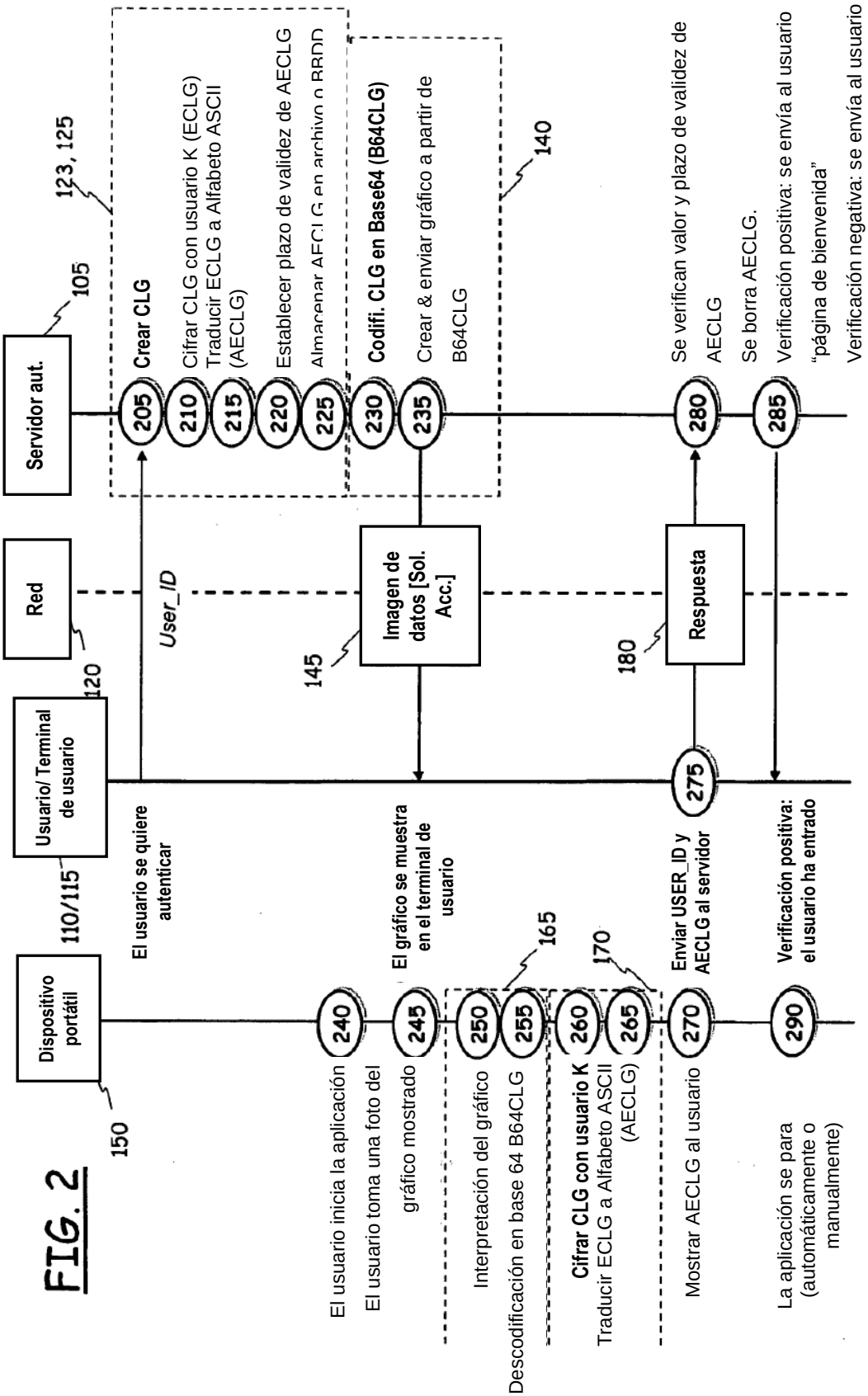

Servidor aut.
105
123, 125
Crear CLG
Cifrar CLG con usuario K (ECLG)
Traducir ECLG a Alfabeto ASCII (AECLG)
Establecer plazo de validez de AECLG
Almacenar AECLG en archivo o BBDD
Codifi. CLG en Base64 (B64CLG)
Crear & enviar gráfico a partir de B64CLG
140
205
210
215
220
225
230
235
Red
User_ID
Imagen de datos [Sol. Acc.]
145
Respuesta
180
Se verifican valor y plazo de validez de AECLG
Se borra AECLG.
Verificación positiva: se envía al usuario "página de bienvenida"
Verificación negativa: se envía al usuario "página de error"
280
285
Usuario/ Terminal de usuario
120
110/115
El usuario se quiere autenticar
El gráfico se muestra en el terminal de usuario
275
Enviar USER_ID y AECLG al servidor
Verificación positiva: el usuario ha entrado
Dispositivo portátil
150
165
170
240
245
250
255
260
265
270
290
El usuario inicia la aplicación
El usuario toma una foto del gráfico mostrado
Interpretación del gráfico
Descodificación en base 64 B64CLG
Cifrar CLG con usuario K
Traducir ECLG a Alfabeto ASCII (AECLG)
Mostrar AECLG al usuario
La aplicación se para (automáticamente o manualmente)

FIG. 2

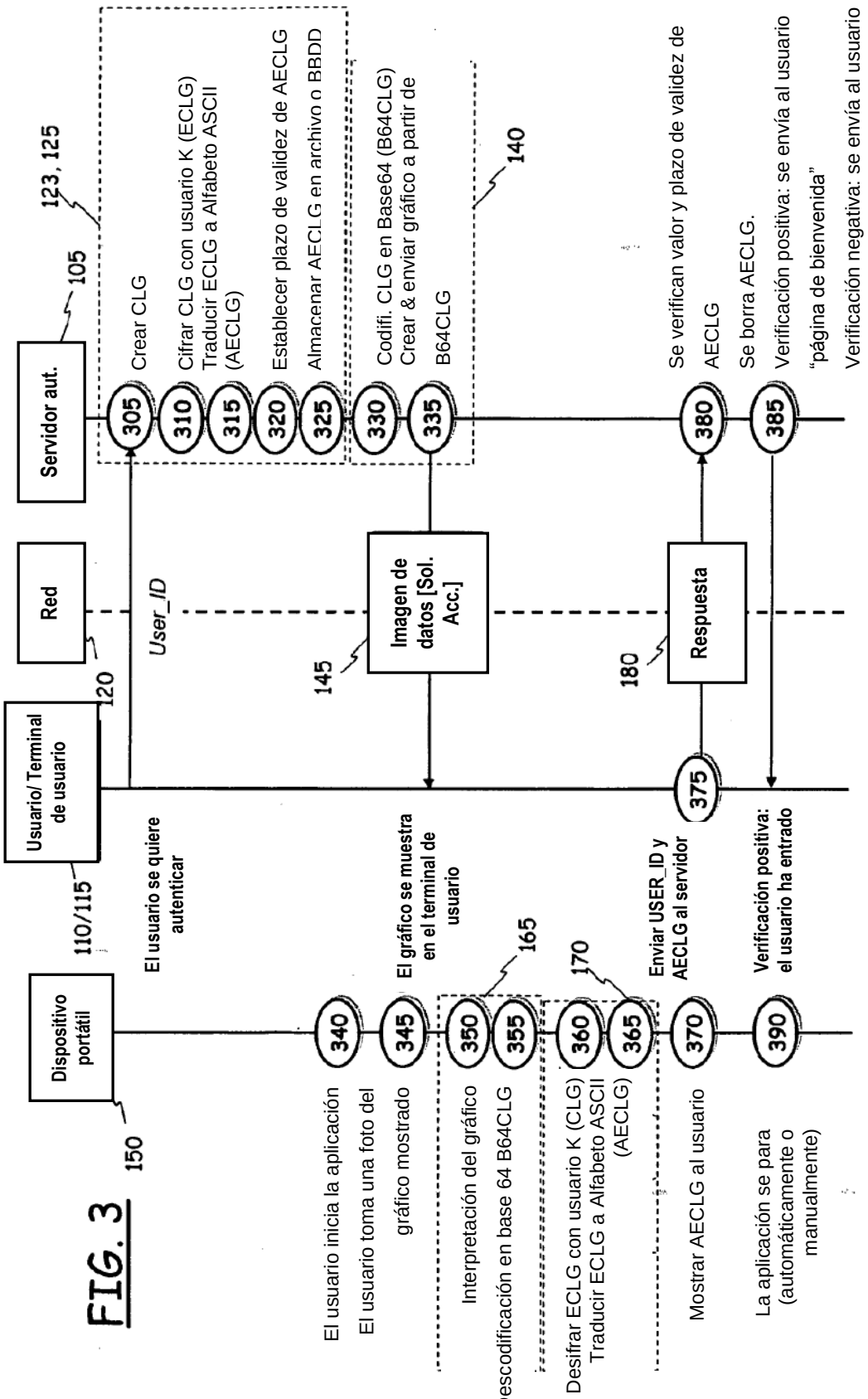

Servidor aut.
105
123, 125
Red
Usuario/ Terminal de usuario
120
Dispositivo portátil
150
110/115
User_ID
El usuario se quiere autenticar
Crear CLG
Cifrar CLG con usuario K (ECLG)
Traducir ECLG a Alfabeto ASCII
(AECLG)
Establecer plazo de validez de AECLG
Almacenar AECLG en archivo o BBDD
Codifi. CLG en Base64 (B64CLG)
Crear & enviar gráfico a partir de
B64CLG
140
Imagen de datos [Sol. Acc.]
145
El gráfico se muestra en el terminal de usuario
El usuario inicia la aplicación
El usuario toma una foto del
gráfico mostrado
Interpretación del gráfico
Descodificación en base 64 B64CLG
165
Desifrar ECLG con usuario K (CLG)
Traducir ECLG a Alfabeto ASCII
(AECLG)
170
Enviar USER_ID y AECLG al servidor
Mostrar AECLG al usuario
Respuesta
180
Se verifican valor y plazo de validez de
AECLG
Se borra AECLG.
Verificación positiva: se envía al usuario
“página de bienvenida”
Verificación negativa: se envía al usuario
“página de error”
Verificación positiva: el usuario ha entrado
La aplicación se para (automáticamente o manualmente)
305
310
315
320
325
330
335
340
345
350
355
360
365
370
375
380
385
390

FIG. 3

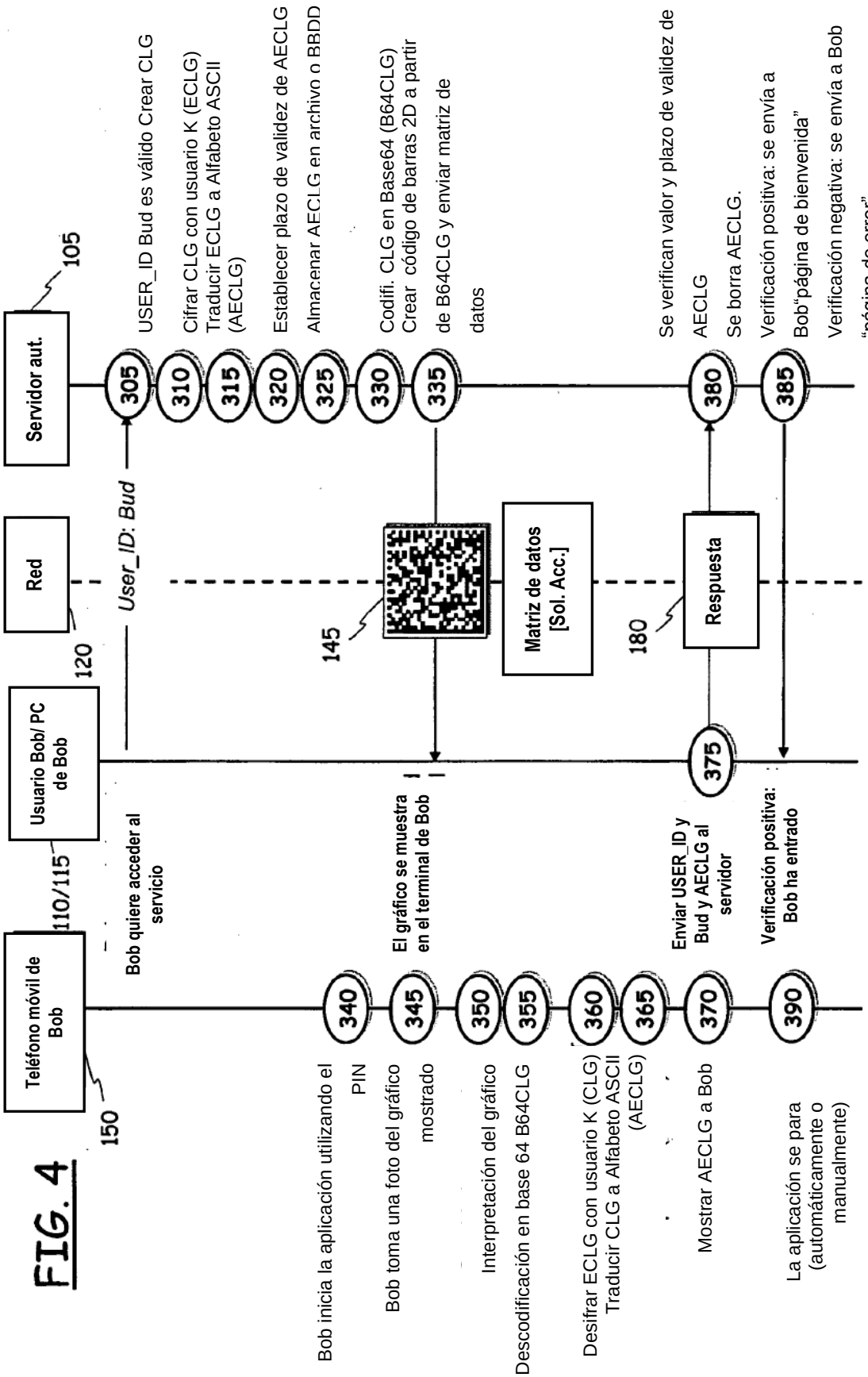

Teléfono móvil de Bob
150
110/115
Usuario Bob/ PC de Bob
120
Red
Servidor aut.
105
User_ID: Bud
Bob quiere acceder al servicio
USER_ID Bud es válido Crear CLG
305
Cifrar CLG con usuario K (ECLG)
Traducir ECLG a Alfabeto ASCII (AECLG)
310
Establecer plazo de validez de AECLG
315
Almacenar AECLG en archivo o BBDD
320
Codifi. CLG en Base64 (B64CLG)
Crear código de barras 2D a partir de B64CLG y enviar matriz de datos
325
330
335
145
El gráfico se muestra en el terminal de Bob
Matriz de datos [Sol. Acc.]
Bob inicia la aplicación utilizando el PIN
340
Bob toma una foto del gráfico mostrado
345
Interpretación del gráfico
350
Descodificación en base 64 B64CLG
355
Desifrar ECLG con usuario K (CLG)
Traducir CLG a Alfabeto ASCII (AECLG)
360
365
Enviar USER_ID y Bud y AECLG al servidor
375
180
Respuesta
Se verifican valor y plazo de validez de AECLG
380
Mostrar AECLG a Bob
370
Se borra AECLG.
Verificación positiva: se envía a Bob"página de bienvenida"
385
Verificación positiva: Bob ha entrado
La aplicación se para (automáticamente o manualmente)
390
Verificación negativa: se envía a Bob "página de error"

FIG. 4

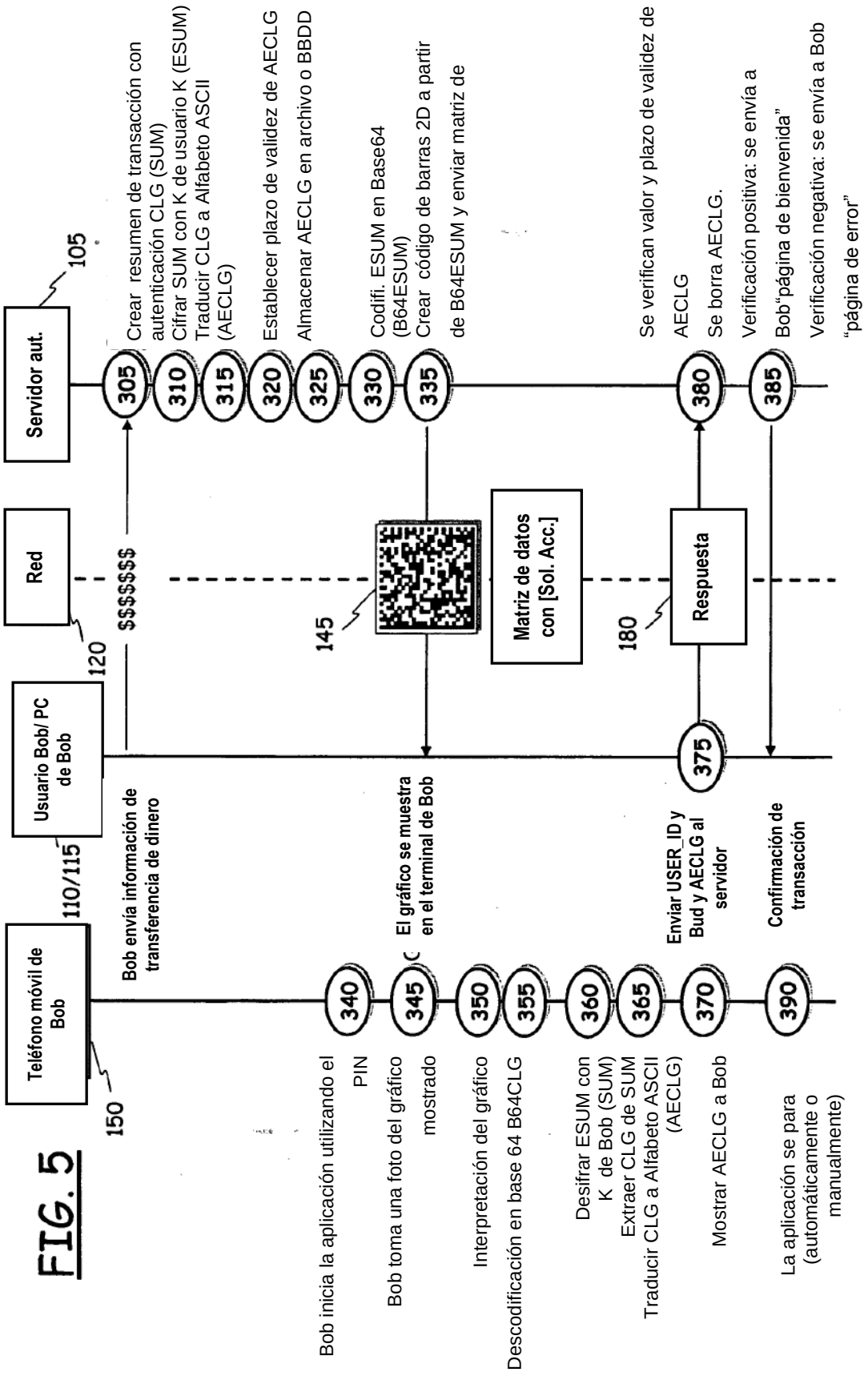

Teléfono móvil de Bob
150
Usuario Bob/ PC de Bob
110/115
Red
120
Servidor aut.
105
$$$$$$
Bob envía información de transferencia de dinero
Crear resumen de transacción con autenticación CLG (SUM)
Cifrar SUM con K de usuario K (ESUM)
Traducir CLG a Alfabeto ASCII (AECLG)
Establecer plazo de validez de AECLG
Almacenar AECLG en archivo o BBDD
Codifi. ESUM en Base64 (B64ESUM)
Crear código de barras 2D a partir de B64ESUM y enviar matriz de
145
Matriz de datos con [Sol. Acc.]
El gráfico se muestra en el terminal de Bob
Bob inicia la aplicación utilizando el PIN
Bob toma una foto del gráfico mostrado
Interpretación del gráfico
Descodificación en base 64 B64CLG
Desifrar ESUM con K de Bob (SUM)
Extraer CLG de SUM
Traducir CLG a Alfabeto ASCII (AECLG)
Mostrar AECLG a Bob
La aplicación se para (automáticamente o manualmente)
180
Respuesta
Enviar USER_ID y Bud y AECLG al servidor
Se verifican valor y plazo de validez de AECLG
Se borra AECLG.
Verificación positiva: se envía a Bob"página de bienvenida"
Verificación negativa: se envía a Bob "página de error"
Confirmación de transacción
305
310
315
320
325
330
335
340
345
350
355
360
365
370
375
380
385
390

FIG. 5

FIG. 6

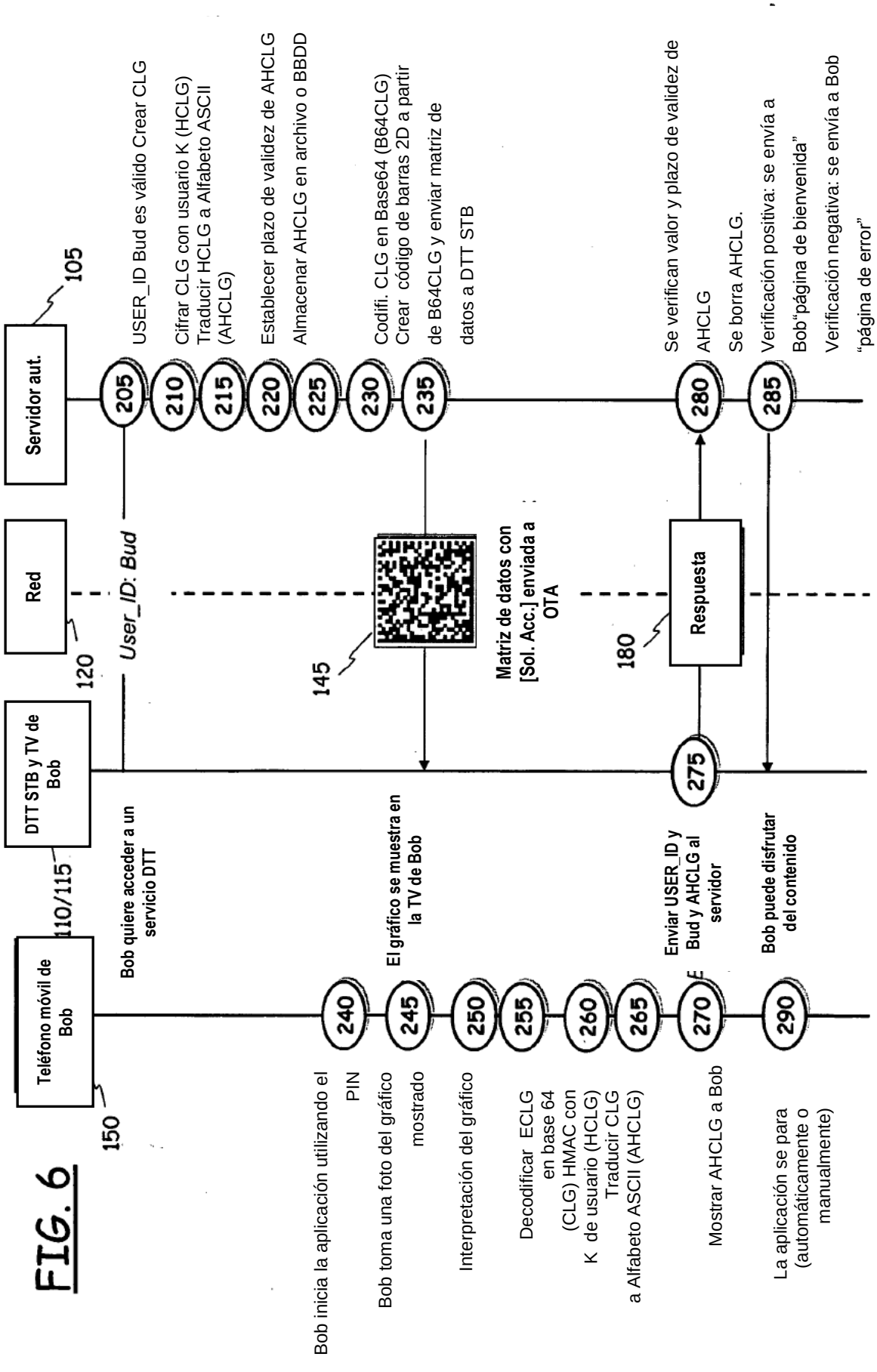
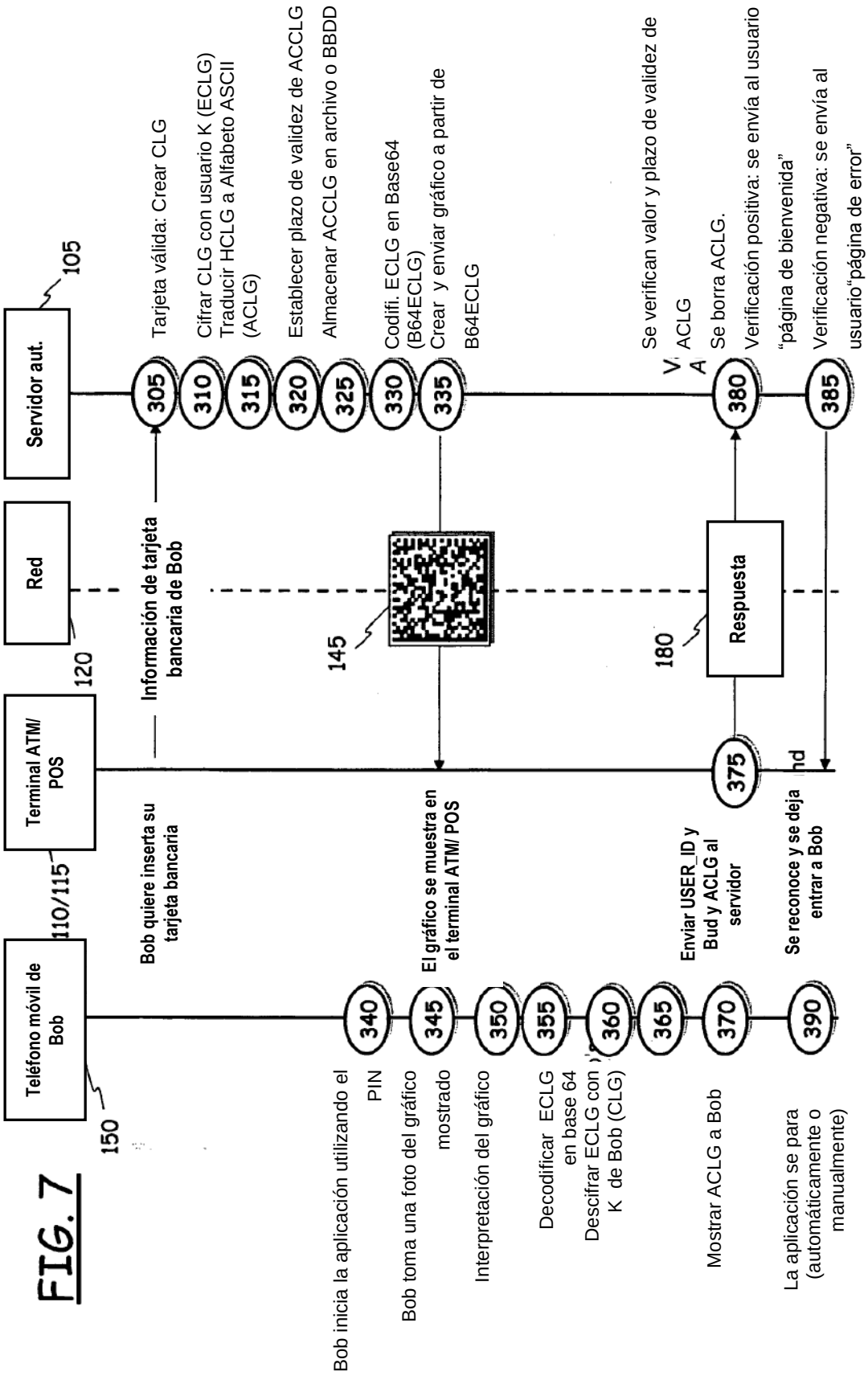

Teléfono móvil de Bob
150
DTT STB y TV de Bob
110/115
Red
120
Servidor aut.
105
Bob quiere acceder a un servicio DTT
User_ID: Bud
USER_ID Bud es válido Crear CLG
205
Cifrar CLG con usuario K (HCLG)
Traducir HCLG a Alfabeto ASCII (AHCLG)
210
215
Establecer plazo de validez de AHCLG
Almacenar AHCLG en archivo o BBDD
220
225
Codifi. CLG en Base64 (B64CLG)
Crear código de barras 2D a partir de B64CLG y enviar matriz de datos a DTT STB
230
235
145
Matriz de datos con [Sol. Acc.] enviada a OTA
Bob inicia la aplicación utilizando el PIN
240
Bob toma una foto del gráfico mostrado
245
El gráfico se muestra en la TV de Bob
Interpretación del gráfico
250
Decodificar ECLG en base 64
255
(CLG) HMAC con K de usuario (HCLG)
260
Traducir CLG a Alfabeto ASCII (AHCLG)
265
Enviar USER_ID y Bud y AHCLG al servidor
275
180
Respuesta
Se verifican valor y plazo de validez de AHCLG
280
Mostrar AHCLG a Bob
270
Se borra AHCLG.
Verificación positiva: se envía a Bob"página de bienvenida"
285
La aplicación se para (automáticamente o manualmente)
290
Bob puede disfrutar del contenido
Verificación negativa: se envía a Bob "página de error"

FIG. 7


Teléfono móvil de Bob
150
110/115
Terminal ATM/ POS
120
Red
Servidor aut.
105
Bob quiere inserta su tarjeta bancaria
Información de tarjeta bancaria de Bob
Tarjeta válida: Crear CLG
Cifrar CLG con usuario K (ECLG)
Traducir HCLG a Alfabeto ASCII (ACLG)
Establecer plazo de validez de ACCLG
Almacenar ACCLG en archivo o BBDD
Codifi. ECLG en Base64 (B64ECLG)
Crear y enviar gráfico a partir de B64ECLG
145
El gráfico se muestra en el terminal ATM/ POS
Bob inicia la aplicación utilizando el PIN
Bob toma una foto del gráfico mostrado
Interpretación del gráfico
Decodificar ECLG en base 64
Descifrar ECLG con K de Bob (CLG)
Mostrar ACLG a Bob
La aplicación se para (automáticamente o manualmente)
Enviar USER_ID y Bud y ACLG al servidor
180
Respuesta
Se verifican valor y plazo de validez de ACLG
Se borra ACLG.
Verificación positiva: se envía al usuario "página de bienvenida"
Verificación negativa: se envía al usuario "página de error"
Se reconoce y se deja entrar a Bob
305
310
315
320
325
330
335
340
345
350
355
360
365
370
375
380
385
390

Solicitud de actualización de información personal

A: [redacted]

Allegati: Mail_in_allegato.pdf (42 KB)

Apreciado cliente,
Por favor mire la información contenida en el adjunto.
Para su seguridad, el documento adjunto está protegido por una contraseña.
La contraseña a utilizar está incrustada en el gráfico siguiente, que puede ser leído utilizando su equipo móvil e introduciendo el PIN de activación solicitado.

Equipo del banco

FIG. 8A

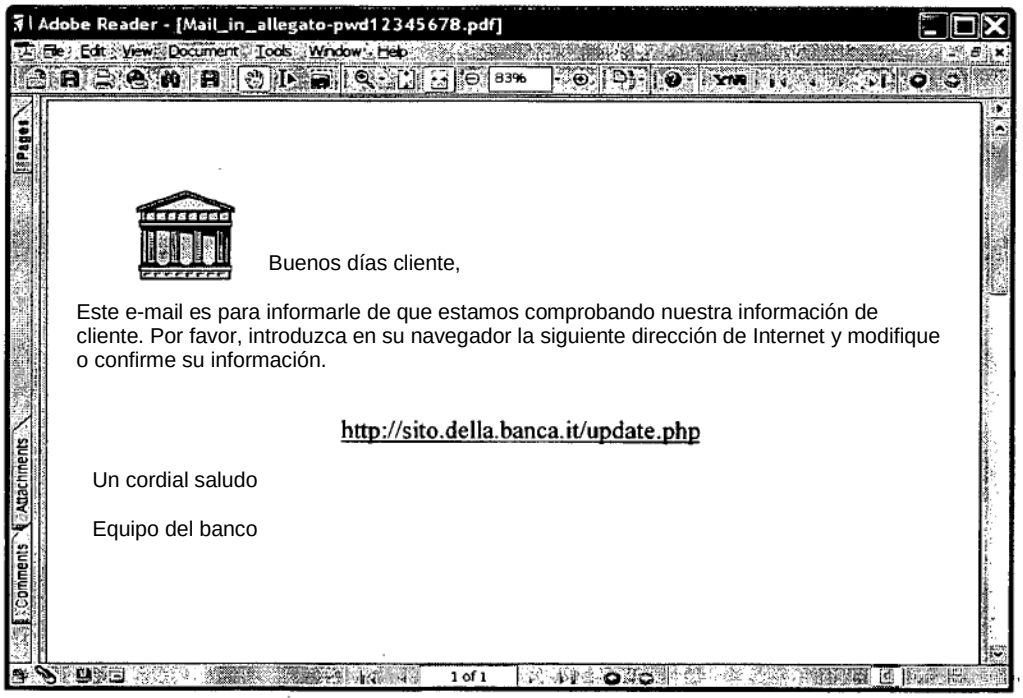
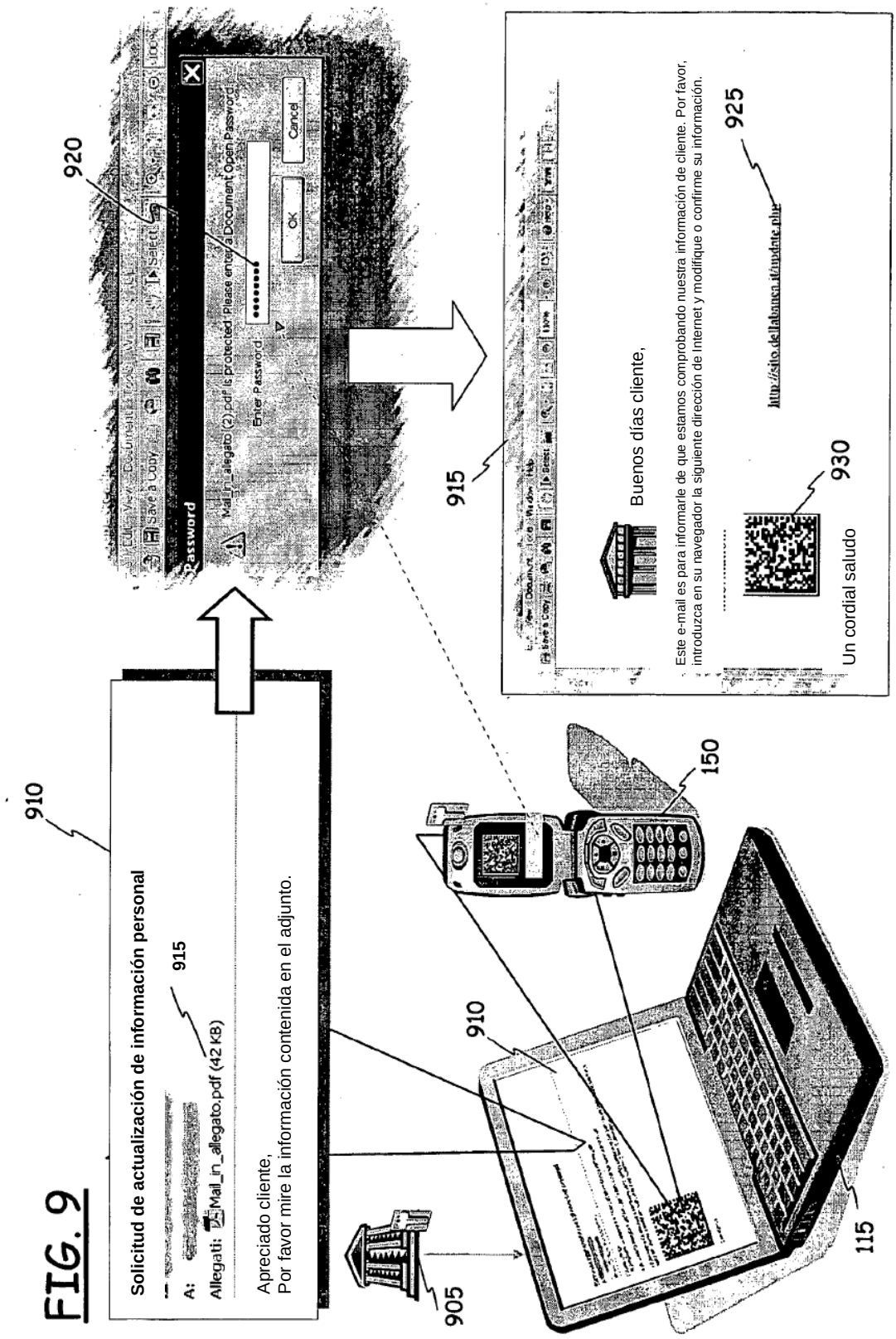


FIG. 8B

FIG. 9


910
Solicitud de actualización de información personal
A:
915
Allegati: Mail_in_allegato.pdf (42 KB)
Apreciado cliente,
Por favor mire la información contenida en el adjunto.
920
Password
Mail_in_allegato (2).pdf is protected. Please enter a Document Open Password.
Enter Password:
OK
Cancel
915
Buenos días cliente,
Este e-mail es para informarle de que estamos comprobando nuestra información de cliente. Por favor, introduzca en su navegador la siguiente dirección de Internet y modifique o confirme su información.
925
http://sito.de.labanca.it/update.php
930
Un cordial saludo
150
910
905
115