(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 530 715**

(51) Int. CI.:

H04L 9/32 (2006.01)
G06F 21/31 (2013.01)
H04L 9/00 (2006.01)
H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **09.03.2006 E 06737600 (4)**

(97) Fecha y número de publicación de la concesión europea: **03.12.2014 EP 1997270**

(54) Título: **Método y sistema para autenticar a un usuario**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.03.2015

(73) Titular/es:

VASCO DATA SECURITY INTERNATIONAL GMBH (100.0%)
WORLDWIDE BUSINESS CENTRE, BALZ-ZIMMERMANNSTRASSE 7
8152 GLATTBRUGG, CH

(72) Inventor/es:

FORT, NICOLAS y
GRANGE, BENOIT

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Método y sistema para autenticar a un usuario

Campo de la invención

La invención se refiere a los mejoramientos en la seguridad en la red de computadoras.

Antecedentes

Se ha vuelto común, y conforme transcurre el tiempo se hace más común, que las aplicaciones sean accedidas y las transacciones conducidas remotamente sobre redes públicas tales como la internet. La popularidad de estas aplicaciones ha atraído la atención de los piratas o hackers, y las organizaciones criminales. Para proteger las aplicaciones contra el acceso no autorizado, muchos proveedores de aplicaciones confían en que sus usuarios tengan que enviar, durante el registro, la combinación de la identificación de usuario (ID de usuario) y una contraseña (password). En la mayoría de los casos la contraseña es estática, por ejemplo, el mismo valor de contraseña sigue siendo válido en un periodo relativamente prolongado de tiempo.

Para que los hackers tengan acceso a una aplicación remota para comprometerse en transacciones fraudulentas, es suficiente con obtener una combinación válida de ID de usuario-contraseña. Por ejemplo, un método popular es enviar un correo electrónico falso que pide que el usuario (con algún pretexto más o menos creíble) envíe su ID de usuario-contraseña en respuesta. Esto es a menudo denominado cómo anzuelo o estafa electrónica. Otro método popular es crear un sitio de red impostor que parece convenientemente como un sitio de red real. Por supuesto, cuando un usuario intenta registrarse, su ID de usuario-contraseña son capturados para un mal uso posterior.

Debido a la facilidad de éxito que los hackers han logrado en la obtención de una combinación válida de ID de usuario-contraseña, es ahora ampliamente aceptado que una contraseña estática sola ofrece un nivel de seguridad demasiado bajo para ser aceptable para aplicaciones que involucran transacciones financieramente valiosas y similares. En consecuencia, existe una necesidad para un método de autenticación de usuario, alternativo que ofrezca un más alto nivel de seguridad.

Si existen técnicas alternativas. Estas incluyen:

1. Certificados (por ejemplo, software (dotación lógica informática), tarjetas inteligentes o memorias o memorias USB).
2. Memorias de autenticación fuerte de hardware (equipo físico).
3. Memorias blandas (por ejemplo, software que emulan memorias de autenticación fuertes de hardware).
4. Tarjetas inteligentes,
5. Memorias USB.

En la mayoría de los casos los usuarios tienen que estar ya sea equipados con un dispositivo de hardware personalizado (memorias USB, memorias de autenticación fuerte, tarjetas inteligentes, etc.) o deben instalar alguna pieza personalizada de software (certificados de software, memorias blandas, etc.). La desventaja principal de estas soluciones, cuando es comparada al método ordinario de ID de usuario-contraseña es que:

(a) éstos son más costosos (debido que al hardware específico que es requerido para implementarlos equipo físico es aquel), o
(b) éstos limitan la movilidad del usuario a una computadora específica (en particular la computadora en la cual ha sido instalado el hardware o el software personalizado), o
(c) éstos no son fáciles de utilizar (el usuario necesita seguir un procedimiento de instalación complicado que puede fallar), o
(d) una combinación de las desventajas anteriores.

El artículo “Enhancing the Security of Cookies” por Vorapranee Khu-Smith y Chris Mitchell (publicado en “Information Security and Cryptology - ICISC 2001”, Springer Berlgin Heidelberg, ISBN 978-3-54-043319-4, p. 132-145) desvela el almacenamiento de una clave de encriptación dentro de una cookie. También sugiere, por separado, el uso de palabras clave para usuarios que desean encriptar sus cookies. D1 no desvela la encriptación de la cookie con la contraseña, ni el uso de una applet embebida para solicitar al usuario por una contraseña. Por lo tanto, esta publicación no proporciona a un usuario web con un mecanismo de autenticación conveniente para diversos servicios en línea.

En consecuencia, lo que se necesita es una solución que proporcione mayor seguridad que la ID de usuario-contraseña pero que conserve todavía las ventajas principales de la ID de usuario-contraseña, es decir, el bajo costo, facilidad de uso y facilidad para migrar de una computadora a otra.

Normalmente los usuarios utilizan una computadora, tal como una computadora principal (pc) para acceder a las aplicaciones en un servidor remoto. No obstante, dispositivos diferentes de las pc's son también utilizados, por ejemplo, dispositivos móviles tales como un asistente de datos personales (pda, por sus siglas en inglés), teléfonos celulares habilitados en la red y similares. Para los propósitos de esta aplicación el término computadora personal o pc incluirá todos los dispositivos tales, así como otros dispositivos similares que puedan acceder a través de la internet a un dispositivo de internet remoto, tal como un servidor, intercambiar información y mensajes por medio de un software buscador (browser) que el acceso sea una vía terrestre o incluye un componente inalámbrico.

Sumario de la invención

La solución de pase digital (digipass) para la red está basado en los siguientes principios:

a. Para cada usuario, un servidor asocia al usuario con una clave de autenticación.
b. La clave de autenticación asociada con un usuario específico es también almacenada localmente en una computadora personal en la forma de a cookie.
c. La clave de autenticación de usuario almacenada en el trozo de información es protegido por una contraseña conocida únicamente por el usuario.
d. La página web de registro del servidor contiene un applet (componente de una aplicación que se ejecuta en el contexto de otro programa) de autenticación incrustado (por ejemplo, un componente de software que puede ser referido y llamado en una página web y es automáticamente descargado por el buscador si éste no está ya presente en la computadora personal de acceso). El applet es preferentemente un Applet Java pero alternativamente éste podría ser por ejemplo un componente ActiveX.
e. El applet de autenticación es capaz de pedirle a un usuario que introduzca la contraseña.
f. El applet de autenticación es capaz de acceder al trozo de información que almacena la clave de autenticación protegida por contraseña. El applet es capaz de obtener acceso a la clave de autenticación con la contraseña que el usuario ha introducido.
g. El uso de la clave de autenticación accesible (asociado en el servidor con el usuario específico, el applet de autenticación puede autenticar ya sea al usuario, o los datos de transacción de firma para garantizar la autenticidad y la integridad de la transacción.

En virtud de estos principios la solución de pase digital para la red, logra más alta seguridad que solo una contraseña estática: para la autenticación exitosa, son necesarios dos factores, por ejemplo el trozo de información (que contiene la clave de autenticación) y la contraseña de usuario (con el fin de descodificar la clave de autenticación que está almacenada en el trozo de información). La solución de pase digital para la red proporciona una solución a bajo costo ya que no existe hardware para distribuir y únicamente el software que es necesario (el applet de autenticación) es automáticamente descargado cuando se requiera. La solución de pase digital para la red también proporciona conveniencia para el usuario ya que el usuario no tiene que ir a través de cualquier proceso de instalación particular que puede fallar, y que el usuario opera la solución exactamente de la misma manera que con una contraseña estática, es decir, que el usuario solo tiene que introducir una contraseña (por ejemplo, el mecanismo de autenticación dinámico es completamente transparente para el usuario). Esto se desprende del hecho de que todo lo que es requerido por la solución es la funcionalidad estándar de buscador o es proporcionado en un applet que es automáticamente descargado por el buscador.

En algunos casos (tal como en el primer uso del applet) cuando el applet es utilizado por un usuario específico, se le pide al usuario que elija e introduzca un secreto de migración. El secreto de migración o una comprobación de clave del secreto de migración es transferido de manera segura al servidor. Si después de esto el usuario intenta acceder al servidor utilizando una computadora personal que no almacena la clave de autenticación en a cookie, se desplegarán los siguientes eventos. Después de la detección de esta condición, el applet de autenticación le pide al usuario que introduzca el secreto de la migración, así como una contraseña. Esta será denominada como una contraseña local y puede ser la misma o diferente que la contraseña utilizada en la PC original. Utilizando el secreto de migración el applet puede luego descargar de manera segura una clave de autenticación (ya sea la misma clave de autenticación que es almacenada en el trozo de información sobre la PC normalmente utilizada por el usuario, o una clave de autenticación diferente) desde el servidor y luego almacena localmente la clave de autenticación descargada en a cookie sobre la PC, actualmente empleada por el usuario. Con esta característica, la solución de base digital para la red también proporciona la movilidad, por ejemplo, el usuario puede migrar de una PC normalmente utilizada, a una PC diferente, sin tener que planearlo de antemano.

Debe ser aparente a partir de lo anterior, que el servidor y la PC de usuario mantienen una clave de autenticación en una forma o en otra. En una modalidad de la invención la confianza está basada en la seguridad estándar ofrecida por la conexión de internet entre la PC del usuario y el servidor, para mantener la confidencialidad sobre el intercambio inicial de la clave de autenticación. Por ejemplo, la PC del usuario y el servidor pueden confiar en una conexión estándar de SSL/TLS.

En una modalidad alternativa, el usuario y el servidor comparten un secreto a un tiempo antes de un contacto inicial entre la PC y el servidor. Este puede ser el caso si el usuario había sido un usuario con una ID de usuario establecida y una contraseña estática y la intención fue migrar al usuario a la solución de pase digital para la red

para fines de autenticación. Si el usuario y el servidor comparten tal secreto histórico (por ejemplo, la contraseña de usuario) entonces el secreto puede ser utilizado para asegurar el intercambio inicial entre el usuario y el servidor de la clave de autenticación.

En una modalidad, el secreto histórico (la contraseña estática existente) puede ser utilizada de acuerdo a algún protocolo de intercambio de claves de autenticación, basado en la contraseña existente (por ejemplo, protocolo SRP-contraseña remota segura) para proteger el intercambio de la clave de autenticación secreta.

En otra modalidad más, el usuario y el servidor utilizan un canal de comunicación diferente de la internet (tal como el correo electrónico, una máquina ATM, un correo basado en papel, etc.) para intercambiar la clave de autenticación directamente, u otro secreto que será utilizado de la misma manera que el secreto histórico descrito anteriormente.

La clave de autenticación, en una modalidad, es una clave de codificación simétrica que es utilizada en el servidor y en el PC de un usuario. Con las claves de autenticación simétricas, la autenticación del usuario puede ser lograda utilizando protocolos de autenticación existentes basados en secretos compartidos tales como el Protocolo de Autenticación de Apretón de Manos de Reto (CHAP, por sus siglas en inglés).

En una modalidad alternativa, el applet de autenticación utiliza una clave de autenticación compartida para emular una ficha de autenticación fuerte de hardware. En ese caso el applet genera palabras clave dinámicas que son calculadas como sigue:

a. El applet toma el valor de una entrada variable que es implícita o explícitamente conocida para el servidor. La entrada variable podría ser la hora actual, un reto dinámicamente generado por el servidor, el valor de un contador que está localmente almacenado (en el mismo trozo de información con la clave de autenticación) y automáticamente incrementado después de cada uso, o una combinación de cualquiera de los anteriores.

b. El applet codifica la entrada variable (como tal o con algún formateo particular) con la clave de autenticación mediante el uso de algún algoritmo de codificación simétrico.

c. El criptograma resultante (como tal, o después de cierto formateo y/o truncamiento adicional) es una contraseña dinámica y es luego enviado al servidor.

d. El servidor conoce el valor de la entrada variable y el valor de la autenticación asociada con el usuario dado. Con estos datos, el servidor realiza los mismos cálculos para obtener su propio valor para la contraseña dinámica.

e. El servidor compara el valor de la contraseña dinámica que es generado con el valor que es recibido del usuario. Si ambos valores son los mismos o de otro modo se comparan, entonces el usuario es considerado como autenticado.

Alternativamente, los datos de transacción de firma con un secreto compartido por la generación de un Código de Autenticación de Mensaje (MAC, por sus siglas en inglés) es una práctica común. Un ejemplo es descrito en el estándar ANSI X9.9. Una alternativa incluye los datos de transacción en la entrada variable para el algoritmo de autenticación que fue descrito anteriormente.

Como una alternativa, la clave de autenticación puede ser una parte privada de un par de clave pública-privada. En este caso, el servidor mantiene, para cada usuario, la parte de la clave pública correspondiente a una clave privada asociada con el usuario. Los usuarios de autenticación y los datos de firma mediante el uso de un par de clave privada-pública es una práctica común que no necesita ser explicada aquí.

En una modalidad de la invención, la precisión de la contraseña del usuario, introducida en respuesta a una petición por el applet, no es validada localmente antes de que sea descodificada la clave de autenticación. Más bien, el applet descodifica la clave de autenticación codificada con la contraseña como fue proporcionada por el usuario, pero si el valor de la contraseña proporcionada no es correcto, el valor de la clave de autenticación descrita será también incorrecto. En consecuencia, la autenticación fallará. Las consecuencias de que esa falla y las fallas repetidas depende de la configuración del servidor, por ejemplo, si y después de cuántos intentos la cuenta del usuario será bloqueada en un número de intentos de autenticación fallidos, consecutivos.

En otra modalidad más, la contraseña puede ser verificada localmente por el applet antes de ser utilizado para descodificar la clave de autenticación.

En una modalidad, el trozo de información no solamente almacena la clave de autenticación codificada sino también una comprobación de clave de la contraseña. Cuando el usuario introduce la contraseña, el applet calcula la comprobación de clave de la contraseña y la compara con la comprobación de clave almacenada en el trozo de información. Si los valores concuerdan, la contraseña introducida por el usuario es correcta y el applet continúa con la descodificación de la clave de autenticación.

La desventaja principal de la validación local de la contraseña ocurre en el caso en que un atacante haya tenido acceso al trozo de información. Ese atacante puede en principio montar una búsqueda exhaustiva fuera de línea. Por otra parte, en el caso de la validación remota, (por el servidor), la única manera de validar la contraseña es mediante el intento de una autenticación. De este modo, el servidor puede detectar fácilmente una búsqueda exhaustiva.

En una modalidad, el trozo de información es almacenado sobre la PC del usuario puede ser unido a la PC del usuario. Esto puede ser realizado no solamente por la validación de la contraseña del usuario, sino también la identidad de la PC del usuario. Esto puede ser implementado por la modificación de la contraseña utilizada para codificar la clave de autenticación almacenada en el trozo de información por la combinación de la contraseña con el valor de uno o más elementos de datos que representan la identidad de la PC del usuario. Estos elementos de datos pueden ser seleccionados como números seriales del procesador de PC del usuario, la tarjeta madre, la unidad de disco duro, la tarjeta de ethernet, etc. Por ejemplo, la clave de autenticación es codificada bajo una combinación (concatenación) de la contraseña del usuario y el número serial (o una parte del mismo) del procesador de la PC del usuario.

En una modalidad, la clave de autenticación que es descargada a una nueva PC de usuario, cuando el usuario migra de una PC a otra, tiene el mismo valor que la clave de autenticación sobre la PC vieja del usuario. Esto significa que efectivamente la nueva PC de usuario ha recibido una copia del trozo de información sobre la PC vieja del usuario.

En principio, el usuario puede trabajar desde PCs viejas y nuevas. En la práctica, esto podría crear un problema de sincronización si la variable introducida está basada en contador, ya que los contadores sobre ambas PCs de usuario pueden bien evolucionar independientemente. Este problema puede ser evitado si la variable introducida para el algoritmo de autenticación no está basado en contador, sino más bien basado en reto.

La desventaja de esta modalidad, es que una copia válida de la clave de autenticación permanece presente sobre cada PC con la que el usuario ha trabajado. Esto podría representar un riesgo de seguridad.

En otra modalidad más de la invención, el servidor genera un nuevo valor para la clave de autenticación que es descargado a una nueva PC de usuario cuando un usuario migra de una PC de usuario a otra. La operación del servidor también invalida el valor viejo de la clave de autenticación que está almacenado en el trozo de información de la PC vieja de usuario. Esto evita la situación que surge de las copias válidas de la clave de autenticación secreta codificada que permanece en las PCs viejas de usuario. Surge una desventaja si el usuario migra a otra PC de usuario y luego después de esto desea trabajar sobre la PC original nuevamente. En ese caso, el usuario tiene que migrar a una PC de usuario más vieja nuevamente. No obstante, no es aparente para un applet, que a cookie sobre el PC de usuario haya sido invalidado. En esta situación, si el applet sobre una PC vieja de usuario no está enterado de que la clave de autenticación disponible a éste, ha sido invalidada, la situación podría conducir a intentos no válidos secuenciales, los cuales a su vez podrían conducir a que el servidor bloquee la cuenta del usuario.

De este modo, en un aspecto, la invención proporciona un método para autenticar a un usuario con respecto a un servidor de la red en el contexto de una sesión de búsqueda de la red, operando el usuario una computadora personal conectada a la internet y comunicándose con el servidor de la red por medio de un buscador de la red capaz de manejar y almacenar trozos de información, cuyo método proporciona mayor seguridad que el uso de las palabras clave fácilmente memorizadas sin requerir que el usuario mantenga un efecto físico, que comprende:

el almacenamiento de a cookie en el dispositivo de computo personal, el trozo de información que incluye una primera clave, la primera clave almacenada en el trozo de información en una forma codificada, codificada bajo una contraseña dependiente de la información conocida únicamente para el usuario, la primera clave también conocida para el servidor de la red y asociada con el servidor de la red con el usuario,

el buscador que recibe del servidor de la red una página web que contiene un applet incrustado, en respuesta a una petición de acceso dirigida a la página web, el applet incrustado en la página web requiere que el usuario introduzca la contraseña,

el applet descodifica la clave codificada almacenada en el trozo de información, utilizando la contraseña, para generar la primera clave, y

el empleo de la primera clave para autenticar al usuario al servidor y/o firmar los datos transmitidos al servidor.

En otro aspecto más, la invención proporciona un método implementado por el servidor que proporciona la autenticación de un usuario a un servidor de la red en el contexto de una sesión de búsqueda de la red que opera con una computadora personal conectada a la internet y que se comunica con el servidor de la red por medio de un buscador de la red capaz de administrar y almacenar trozos de información, cuyo método proporciona mayor seguridad que el uso de las palabras clave fácilmente memorizadas sin requerir que el usuario mantenga un objeto físico, que comprende:

el mantenimiento de un archivo que asocia cada uno de una pluralidad de usuarios, con una primera clave diferente, en respuesta a un acceso por un usuario particular que utiliza una computadora personal, transmitiendo, la computadora personal un applet incrustado en una página web requerida por el acceso de la computadora personal del usuario,

el applet cuando es ejecutado en la computadora personal,

requiere que el usuario introduzca una contraseña,
el acceso de a cookie, si está presente, en la computadora personal del usuario y la descodificación de una primera clave codificada, almacenada en el trozo de información con la contraseña para recuperar la primera clave relacionada al usuario, y
el uso de la primera clave para autenticar al usuario al servidor y/o firmar los datos transmitidos al usuario.

La invención proporciona además un método como se describe, en donde el usuario puede acceder al servidor de la red con una computadora personal particular que ya mantiene a cookie en almacenamiento, incluyendo una primera clave codificada bajo la contraseña, en el cual el usuario puede acceder al servidor de la red con otra computadora personal que no mantiene todavía el trozo de información en almacenamiento, y en el cual el usuario puede acceder al servidor de la red con una computadora personal particular que ya mantiene a cookie en almacenamiento que incluye una primera clave codificada bajo la contraseña, pero mediante la cual ese trozo de información está de algún modo perdido o dañado,
el archivo mantenido por el servidor también incluye un secreto de migración o una comprobación de clave de un secreto de migración,
el servidor que autentica al usuario después de la recepción de la información que comparte favorablemente al secreto de migración o a la comprobación de clave del secreto de migración almacenado en el servidor, o por medio de un protocolo de autenticación que demuestra que el usuario conoce el valor correcto del secreto de migración,
el servidor, después de esto transmite una indicación que significa que el usuario será autenticado después de la presentación de la contraseña.

Breve descripción de los dibujos

El método y el aparato serán descritos con mayor detalle para hacer posible así que aquellos expertos en la técnica realicen y utilicen el mismo cuando se tome en conexión con las figuras anexas en donde:

La figura 1 es un esquema que ilustra la relación entre los elementos principales del pase digital para la red que incluye el dispositivo de cómputo personal del usuario (PC) y su conexión al servidor a través de la Internet;
La figura 2 es un diagrama de bloques que muestra una petición de acceso del servidor por la PC;
La figura 3 ilustra las funciones principales del applet de autenticación en las operaciones de registro y activación;
La figura 4 ilustra las funciones del servidor realizadas en respuesta a la información transmitida por el applet en las fases de registro y activación;
La figura 5 ilustra las funciones principales realizadas por el servidor y la PC en la terminación de la fase de activación;
La figura 6 ilustra la fase operacional que muestra las funciones principales en la interacción entre la PC y el servidor;
La figura 7 ilustra la operación de migración que muestra las funciones principales en interacción entre la nueva PC del usuario y el servidor.

Descripción detallada de las realizaciones preferidas

El pase digital para la red incluye cinco fases:

a. pre-registro (opcional). El usuario y el servidor establecen algún secreto histórico compartido.
b. fase de registro: El usuario se registra con el servidor empleando una PC.
c. fase de activación: La PC del usuario es activada por la obtención de un secreto de autenticación compartida.
d. fase operacional: Uso del secreto de autenticación compartido, la PC del usuario puede generar palabras clave dinámicas y/o firmas dinámicas para autenticar al usuario y las transacciones originadas por el usuario, y
e. fase de migración: El usuario migra a un PC diferente.

Fase de Pre-Registro

En esta fase el usuario servidor establece en cierto modo algún secreto histórico compartido que será utilizado en la siguiente fase cuando sea activado el Pase Digital para la Red en la PC (cliente).

Esta fase es opcional en el pase digital para la red. Este es normalmente incluido si es requerido un mayor nivel de seguridad. El secreto histórico compartido podría ser:

a. Una contraseña de internet existente que el servidor y el usuario ya comparten, o
b. Una contraseña que es específicamente generada para el propósito de ser utilizada en una fase de registro y activación,
c. El secreto histórico puede ser intercambiado entre el usuario del servidor en un número de formas. Por ejemplo, el intercambio puede tener lugar:

1. En una sucursal bancaria cuando el usuario firma un contrato para servicios de banca por internet.
2. A través de un ATM después de que el usuario ha introducido su tarjeta de ATM e introducido el código PIN, o
3. Como parte de otra información incluida en una declaración bancaria confidencial impresa, enviada al usuario vía el correo convencional, o
4. En la forma de un remitente de PIN empleado al usuario vía el correo registrado.

Fase de Registro

Durante esta fase el usuario registra el servicio de Pase Digital para la Red y el Pase Digital para la Red es activado en la PC del usuario (cliente). La figura 1 ilustra los componentes importantes de este proceso. En particular, el usuario opera un dispositivo 10 de computadora personal. Este es normalmente una computadora persona aunque como se mencionó pueden ser también utilizados otros dispositivos. El dispositivo 10 de computadora personal está conectado (ya sea a través de una conexión alámbrica o inalámbrica) vía la internet 20 a un servidor 30. Sobreviene entonces una sesión 40 de red en donde es efectuado el registro de la PC 10 del usuario.

La Figura 2 ilustra en un diagrama de bloques que muestra componentes importantes de la computadora personal 10, el servidor 30 e identifica la información importante que es intercambiada durante la parte de la sesión 40 de la red durante la cual es implementado el registro.

La Figura 1 ilustra la interacción típica entre un usuario, operando un dispositivo de cómputo personal, tal como la PC 10 y un servidor 30 de internet, en la cual la PC y el servidor toman parte en una sesión 40 de la red apoyada por la internet 20. La Figura 1 es representativa de las operaciones en las fases de registro, activación y operación del Pase Digital para la Red. Una de las ventajas del Pase Digital para la Red es la habilidad del usuario para migrar de uso de una PC 10 (mostrada en la Figura 1) a una PC diferente u otro dispositivo de usuario. La manera en la cual la migración sea implementada será descrita más adelante en la presente en conexión con la Figura 7.

Fase de Registro

Antes del uso del Pase Digital para la Red, ciertos datos deben ser intercambiados por el usuario y el servidor. Esto es logrado durante la fase de registro. A este tiempo, el usuario registra el servicio de Pase Digital para la Red.

La Figura 2 es un diagrama de bloques que muestra la interacción entre la PC 10 del usuario y el servidor 30. Antes del registro y/o activación la PC 10 del usuario no podría incluir el applet 12 mostrado en la Figura 2. De hecho, durante la fase de registro y activación el applet 12 es suministrado al usuario PC 10 desde el servidor 30. Además, el trozo de información 14 será creado por el applet 12, también en una fase posterior del proceso. Al inicio de la fase de registro, la PC 10 del usuario incluye un buscador 11 el cual, respondiendo a una petición por el usuario, puede transmitir una petición de acceso 41 al servidor 30. Dependiendo del URL particular contenido en la petición de acceso 41, el servidor responde con una página web que contiene el applet 12 como se ilustra en la Figura 2. El applet 12 incluye el contenido específico para las funciones de registro. El applet 12 puede también incluir el contenido relacionado a la activación, aunque eso no es esencial, el contenido del applet para la activación puede ser suministrado en un tiempo posterior, específicamente cuando es requerida la funcionalidad de activación. El applet 12 puede también incluir el contenido específico para las funciones de autoindicación que van a ser ejecutadas en una fase operacional. Dependiendo de cómo esté estructurada la implementación, puede existir únicamente un applet simple que proporciona registro, activación y operación. Alternativamente, pueden existir diferentes applets para el registro por una parte, y otro applet para la fase de activación y operacional. Además, dependiendo del detalle de implementación incluso el applet operacional puede ser dividido en diferentes segmentos. Aquellos expertos en la técnica entenderán cómo segmentar el applet, de modo que la operación total es relativamente sin unión.

El buscador carga el applet 12 y luego lo ejecuta. La Figura 2 también representa las etapas iniciales de la fase de registro, no obstante al inicio de la fase de registro el trozo de información 14 no estará presente. En particular, el usuario dirige al buscador 11 al sitio de la red del servidor 30. En respuesta a la petición de acceso 41, el servidor 30 transmite el applet apropiado, por ejemplo el applet de registro y activación. Cuando el applet 12 es recibido y cargado por el buscador 11, éste es ejecutado.

Las funciones principales realizadas por el applet de activación son mostradas en la Figura 3. La función inicial 301, para establecer una Clave de Sesión de Activación, es opcional. Con el fin de establecer la clave de sesión de activación debe existir algún secreto histórico el cual, antes de la ejecución de la función 301, es compartido entre el usuario y el servidor 30. Si ese es el caso, entonces el usuario puede iniciar la función 301. La función 301 pide que

el usuario introduzca el secreto histórico. Después de la recepción del secreto, el applet 12 utiliza el secreto con un protocolo para establecer una clave de sesión común (la clave de sesión de activación) con base en el secreto histórico compartido. Usualmente, por ejemplo, en la mayoría de los protocolos, algunos datos (por ejemplo denominadas “sales” o “nonces”) serán generados e intercambiados, lo cual es utilizado para derivar la clave de sesión común del secreto histórico compartido; esos datos serán denominados como los datos de derivación de la clave de sesión de activación. La función 301 concluye con el applet 12 que guarda los datos de derivación de la clave de sesión de activación.

Después de esto, la función 302, el applet 12 pide que el usuario elija e introduzca una identidad de usuario (UID). Después de esto, la función 303 pide que el usuario seleccione una pregunta de una lista de preguntas predefinidas (“¿cuál es el nombre de soltera de su madre?”, “¿cuál es su película favorita?”, “¿cuál es el nombre de su mascota?”, etc.) e introduzca la respuesta secreta a esa pregunta. La pregunta será utilizada en la fase de migración y será denominada como un secreto de migración o respuesta secreta.

Después de esto, la función 304 pide que el usuario elija, introduzca y confirme una contraseña local de Pase Digital para la Red. Esta contraseña de Pase Digital para la Red se volverá la contraseña utilizada por la PC 10 para fines de descodificación (ver funciones 603, 606 y 607 de la Figura 6). En particular, la contraseña será utilizada para proteger una clave de autenticación que será almacenada en a cookie en la PC. Aunque en algunas modalidades la contraseña puede ser transmitida al servidor, ésta no será almacenada en el servidor y por lo tanto la contraseña puede ser referida como información que está disponible únicamente a la PC 10.

Después de esto, la función 305 deriva la clave de enmascaramiento del código de activación. Esto es realizado en una secuencia de pasos. Primeramente, el applet genera una Sal Aleatoria (Random Salt). Después de esto, el applet 12 lee el valor de algún elemento o elementos de datos que representan la identidad de la PC del usuario. Éste puede ser un número en serie del procesador de la PC, la unidad de disco duro, la tarjeta madre, etc. El applet combina luego el Random Salt, el o los valores de identificación de la PC, y la contraseña local con el fin de obtener la clave de enmascaramiento del código de activación utilizando un algoritmo criptográfico. El algoritmo debe ser seleccionado para tener las siguientes características:

1. Es muy difícil encontrar una combinación de Random Salt, valores de identificación de la PC y contraseña local que den como resultado un valor dado para una Clave de Enmascaramiento de Código de Activación, y
2. Para una Random Salt dada y los valores de identificación de la PC dados, es difícil encontrar una contraseña local que dé como resultado un valor dado para la Clave de Enmascaramiento de Código de Activación.

Un ejemplo de un algoritmo criptográfico apropiado es la comprobación de clave por SHA-1 de la concatenación de Random Salt, los valores de identificación de la PC y la contraseña local.

Después de esto, la función 306 guarda a cookie de registro en la PC 10 del usuario. El trozo de información contiene dos o tres elementos. El primer elemento es el dato de derivación de la Clave de Sesión de Activación, si el paso opcional 301 fue realizado, por ejemplo si el usuario y el servidor, antes de la activación, habían compartido un secreto histórico. El trozo de información también contiene el Random Salt así como la UID.

Finalmente, la función 307, el applet 12 transmite un Mensaje de Registro, que contiene cuatro elementos, hacia el servidor. El mensaje contiene:

a. UID.
b. La dirección de correo electrónico del usuario.
c. La comprobación de clave de la respuesta secreta (secreto de migración).
d. La Clave de Enmascaramiento de Activación.

Si la función opcional 301 fue realizada, y correspondientemente fue establecida una clave de sesión de activación, el mensaje de registro es codificado con una Clave de Sesión de Activación. Eso termina la operación del applet 12 en la fase de registro.

La Figura 4 ilustra la respuesta del servidor 30 a la información proporcionada por el applet 12 en la porción de conclusión de la fase de registro, así como las etapas iniciales de la fase de activación.

Como se muestra en la Figura 4, en la función inicial 401, el servidor 30 recibe el mensaje de registro. En la función 402 ese mensaje es descodificado, si éste había sido codificado.

En la función 403 el servidor registra el usuario que utiliza la UID, la dirección de correo electrónico, y la comprobación de clave de la respuesta secreta (secreto de migración).

En la función 404 el servidor genera un Glóbulo (Blob) de Pase Digital. La instancia del Glóbulo de Pase Digital para este usuario particular contiene la clave de autenticación secreta del Pase Digital (originada en el servidor), y los parámetros del algoritmo de Pase Digital, por ejemplo, los parámetros que indican el tipo de variable introducida

para el OTP de Pase Digital (que va a ser descrito) y el algoritmo de Firma, el tipo de formateo para aplicar a la variable introducida, el tipo de formateo para aplicar al criptograma. La distancia del Glóbulo del Paso Digital es asignada a la UID para este usuario particular, la función 405, por ejemplo, es indizada de modo que sus contenidos estarán asociados con este usuario.

El servidor 30 realiza luego las funciones 406 a la 408.

En particular, en la función 406, el servidor 30 codifica el Glóbulo de Pase Digital (DigiPass Blob) con la Clave de Enmascaramiento de Código de Activación; el resultado es denominado como el Código de Activación. El servidor 30 codifica luego el Código de Activación con la Clave de Sesión de Activación, si está disponible. Recuérdese que la Clave de Sesión de Activación es opcional y requiere la compartición preparatoria de un secreto histórico entre el usuario y el servidor 30. Finalmente, en la función 408, el servidor envía un correo electrónico al usuario, en la dirección de correo electrónico registrada por el usuario, el correo electrónico que contiene una URL de activación. La URL de activación, cuando es accedida por el usuario, le proporcionará al usuario con un applet de activación como se describe más adelante en la presente.

La Figura 5 ilustra la terminación del proceso de activación subsecuente a la ejecución para la función 408 en el servidor 30.

Como se muestra en la Figura 5, el siguiente paso que es realizado es la función 501 ejecutada por la PC 10 del usuario. La función 501 ocurre cuando el usuario selecciona la URL de activación. Cuando el servidor 30 recibe el acceso desde el usuario de la PC 10, el servidor 30 envía la página web que contiene el código de activación de Pase Digital específico, identificado con el usuario, junto con el applet de activación.

El applet de activación y el código de activación de Pase Digital es recibido en la PC 10 del usuario. En la función 503, el applet lee el trozo de información de registro almacenado en la PC 10 (almacenada en la función 306).

En la función 504, el applet pide que el usuario introduzca el secreto histórico si ha existido un secreto histórico compartido, preparatorio a la fase de registro. Si existió tal secreto la Clave de Sesión de Activación es reconstruida por la PC 10 (a partir del secreto histórico compartido introducido por el usuario, y los datos de derivación de la clave de sesión de activación almacenados en el trozo de información de registro). El acceso a la Clave de Sesión de Activación permite que el applet descodifique el Código de Activación. Por otra parte, si no existía el secreto histórico, el Código de Activación podría no haber sido codificado y por lo tanto no sería necesaria la operación de descodificación.

Después de esto, en la función 505 la PC 10 del usuario guarda el trozo de información del Glóbulo de Pase Digital en la PC 10. El trozo de información de Glóbulo contiene la UID, el Random Salt, el Código de Activación de Pase Digital y un valor contador particular.

Para confirmar la activación exitosa el applet de autenticación del Pase Digital genera una contraseña dinámica, la función 506. El servidor 30 recibe la contraseña dinámica, función 507. Esto completa la fase de activación. La generación de la contraseña dinámica en la función 506 y su validación en la función 507 confirma, en el servidor, que la activación ha sido exitosa. Los detalles de la función 506 son los mismos que las funciones 603-609 que van a ser descritos en conexión con la Figura 6.

La Figura 6 ilustra la interacción entre la PC 10 y el servidor 30 en la fase operacional.

Como se muestra en la función 601, la fase operacional es iniciada cuando el usuario, subsecuente al registro, dirige a la PC 10 para acceder al sitio apropiado de la red del servidor 30. En respuesta al acceso por el usuario, el servidor 30 en la función 602 transmite una página de registro al usuario, que contiene el applet de autenticación. Las funciones 603 etc., son dirigidas por el applet de autenticación en la PC 10.

En particular, en la función 603 se le pide al usuario que introduzca la contraseña local que el usuario había elegido e introducida en la función 304 de la Figura 3. En la función 604, el applet lee el o los valores de la ID de la PC (que habían sido utilizados en el algoritmo de codificación de la función 305). En la función 605, el applet lee el trozo de información de Glóbulo para obtener el Random Salt. En la función 606, el applet reconstruye la Clave de Enmascaramiento de Código de Activación, con base en los datos recuperados en las funciones 603 a 605. Con la clave de enmascaramiento del código de activación, reconstruido, en la función 607, el código de activación es descodificado.

Con base en el código de activación descodificado, la función 608 genera una Contraseña de Una Sola vez (OTP, por sus siglas en inglés). La función 609 envía la OTP al servidor. La función 610 (ejecutada por el servidor 30) proporciona la validación de la OTP recibida en el servidor 30. El servidor 30 valida la OTP mediante el uso de sus propios valores de datos y genera una versión de servidor de la OTP, que es luego comparada a la OTP recibida. La validación de la OTP autentica el usuario al servidor 30.

Como una alternativa al envío de la OTP al servidor 30 para fines de autenticación, el usuario podría utilizar la OTP para codificar o firmar datos relacionados a las transacciones o los mensajes. Esto podría en efecto “firmar” los datos para la transacción o mensajes por el usuario, de modo que los datos y/o los mensajes podrían ser aceptados por el servidor 30 como auténticos.

Fase de Migración

El usuario, habiéndose registrado y utilizado el servicio de Pase Digital para la Red desde una PC, puede desear utilizar el servicio de Pase Digital para la Red desde una PC diferente, una PC que no ha sido registrada. Además, es algunas veces importante que el usuario sea capaz de realizar esta función sin ninguna planeación, por ejemplo inesperadamente de la base momentánea. El servicio de Pase Digital para la Red proporciona esta funcionalidad en una fase de migración.

La Figura 7 ilustra la función realizada durante la fase de migración. Inicialmente, el usuario accede al sitio de la red del servidor 30 (función 701) desde la PC 100, una computadora que no ha sido registrada y por lo tanto no almacena los datos que están almacenados en la PC 10. El servidor 30 responde a la petición de acceso desde el usuario mediante el envío de una página web de registro con un applet de autenticación, por ejemplo el servidor 30 no responde diferente a la petición de acceso desde la PC 100 que podría responder a una petición proveniente de una PC registrada tal como la PC 10.

En la función 703, el applet, que ha sido instalado en el buscador 11 determina que no existe trozo de información de Glóbulo almacenado, como debería haber sido la PC activada y registrada. En consecuencia, el applet propone una función de migración al usuario, función 703. Para fines de esta descripción asumiremos que el usuario está de acuerdo en la función de migración, función 704.

Después de esto, el applet repite las funciones de registro y activación, como se describe en conexión con las Figuras 3, 4 y 5 con varias modificaciones. La dirección de correo electrónico del usuario y la UID no son cambiadas. No obstante, con el fin de autenticar al usuario, se requerirá que el usuario introduzca la respuesta secreta que había sido previamente introducida en la función 303. Además, se le pedirá al usuario que introduzca una nueva contraseña local en lugar de la contraseña local introducida en la función 304.

El applet y el servidor emplean la respuesta secreta como un secreto histórico y realizan los procesos de registro y activación como ya se explicó.

Un problema de implementación en la fase de migración es si la clave de autenticación secreta generada por el servidor debe ser o no la misma que la clave de autenticación secreta que había sido generada por el servidor y utilizada con la PC 10 originalmente registrada, o debería ser una clave de autenticación secreta, nueva. Efectivamente, la clave de autenticación secreta, generada en la fase de migración puede ser ya sea la misma o diferente ya que existen ventajas y desventajas de cualquier modalidad. Una ventaja es que el uso de la misma clave de autenticación permite que el usuario trabaje alternadamente de la PC vieja y la nueva, como desee. Una desventaja es que si un valor de contador forma un elemento de una clave, pueden existir problemas de sincronización ya que las PCs viejas y nuevas podrían almacenar más probablemente diferentes valores de contador. Por supuesto, esta ventaja puede ser eliminada si la variable introducida para el algoritmo de autenticación no está basada en contador. Otra desventaja más de este procedimiento es que una copia válida de la clave de autenticación secreta permanece presente sobre cada PC en la que el usuario se ha registrado y activado. Esto puede por sí mismo representar un riesgo de seguridad.

Alternativamente, el servidor 30 podría generar una nueva clave de autenticación secreta para cada nueva PC a la cual migre el usuario. Esto significa necesariamente que la clave de autenticación secreta previa se vuelve no válida. La ventaja de esta implementación es que la presencia de claves de autenticación secretas viejas sobre las PCs previamente utilizadas, ya no es un riesgo, ya que esas claves no son válidas. Una desventaja de este procedimiento es que si el usuario, habiendo migrado a la PC 100, desea ahora regresar a la PC 10, el usuario tendría que realizar otra operación de migración ya que la clave de autenticación secreta contenida en la PC 10 habría sido invalidada por la migración a la PC 100.

Debería ser aparente que esta especificación describe uno o más ejemplos de las implementaciones de la invención. Aquellos expertos en la materia reconocerán que muchos y variados cambios pueden ser realizados que caen dentro del espíritu y alcance de la invención. En consecuencia, el alcance de las reivindicaciones no debe estar limitado por los ejemplos específicos descritos en la presente.

REIVINDICACIONES

1. Un método para autenticar un usuario con respecto a un servidor de la red (30) en el contexto de una sesión de búsqueda en la red (40), el usuario opera una computadora personal (10) conectada a la internet (20) y se comunica con el servidor de la red (30) por medio de un buscador de la red (11) capaz de administrar y almacenar cookies, que comprende:

el almacenamiento (505) de una cookie (14) en la computadora personal (10), la (14) cookie incluye una primera clave, la primera clave almacenada en la cookie (14) en una forma codificada, que es codificada bajo una contraseña dependiente de la información conocida únicamente por el usuario, la primera clave también conocida por el servidor de la red (30) y asociada en el servidor de la red (30) con el usuario,
el buscador (11) recibe (602) del servidor de la red una página web que contiene un applet (12) incrustado, en respuesta a una petición de acceso (601) dirigida a la página web, el applet (12) incrustado en la página web requiere (603) que el usuario introduzca la contraseña,
el applet (12) que descodifica (607) la clave codificada almacenada en la cookie (14), utilizando la contraseña, para generar (608) la primera clave, y
el empleo (609) de la primera clave para autenticar (610) el usuario al servidor (30) y/o firmar los datos transmitidos al servidor (30).

2. El método de conformidad con la reivindicación 1, en el que la primera clave codificada que es almacenada en la cookie (14) es codificada con una combinación de una contraseña conocida para el usuario y la información que representa al menos una característica del dispositivo de cómputo personal (10).

3. Un método implementado por el servidor para proporcionar la autenticación de un usuario a un servidor de la red (30), en el contexto de una sesión de búsqueda en la red (40) que opera con una computadora personal (10) conectada a la internet (20), y que se comunica con el servidor de la red (30) por medio de un buscador de red (11) capaz de administrar y almacenar cookies, que comprende:

mantener un archivo que asocia cada uno de una pluralidad de usuarios con una primera clave diferente,
en respuesta a un acceso (601) por un usuario particular que utiliza una computadora personal (10), la transmisión (602), hacia la computadora personal (10), de un applet (12) incrustado en una página web requerida por el acceso de la computadora personal (10) del usuario, dicho applet (12), cuando es ejecutado en la computadora personal;

pide (603) que el usuario introduzca una contraseña,
el acceso (605) de una cookie (14), si está presente, en la computadora personal del usuario y
la descodificación (607) de una primera clave codificada, almacenada en la cookie (14) con la contraseña para recuperar la primera clave relacionada al usuario, y
el uso (610) de la primera clave para autenticar al usuario hacia el servidor (30) y/o los datos de firma transmitidos al servidor (30).

4. El método de conformidad con la reivindicación 3, en el que el usuario puede acceder al servidor de la red (30) con una computadora personal (10) particular que ya mantiene una cookie (14) en almacenamiento que incluye una primera clave codificada bajo dicha contraseña, y en el cual el usuario puede acceder al servidor de la red (30) con otra computadora personal (10) que todavía no mantiene la cookie (14) en almacenamiento, o en el cual el usuario puede acceder al servidor de la red (30) con una computadora personal (10) particular que ya mantiene una cookie (14) en almacenamiento, que incluye una primera clave codificada bajo la contraseña, pero estando la cookie (14) de algún modo perdida o dañada,
el archivo mantenido por el servidor también incluye un secreto de migración, o una comprobación de clave de un secreto de migración,
el servidor (30) autentica al usuario después de la recepción de la información que compara favorablemente al secreto de migración o la comprobación de clave del secreto de migración almacenado en el servidor, o por medio de un protocolo de autenticación que demuestra que el usuario conoce el valor correcto del secreto de migración,
el servidor (30) después de esto transmite una indicación que significa que el usuario será autenticado después de la presentación de la contraseña.

5. El método de conformidad con la reivindicación 4, en el que la información incluye la primera clave codificada bajo la contraseña.

6. El método de conformidad con la reivindicación 4, en el que la información contiene una segunda clave, diferente de la primera clave, codificada bajo la contraseña, en donde la segunda clave puede ser utilizada en vez de la primera clave por el applet (12) para autenticar el usuario al servidor (30).

7. El método de conformidad con la reivindicación 4, en el que el applet (12) transmitido a la computadora personal (10) es transmitido en uno o más segmentos.

8. El método de conformidad con la reivindicación 7, en el que un segmento particular del applet (12) es únicamente transmitido a petición.

9. Un sistema para autenticar a un usuario con respecto a un servidor de la red (30) en el contexto de una sesión de búsqueda en la red (40), utilizando el usuario una computadora personal (10) conectada a la internet (20) y que se comunica con el servidor de la red (30) por medio de un buscador de la red (11) capaz de administrar y almacenar cookies, que incluye:

una memoria para almacenar una cookie (14) en la computadora personal (10), la cookie (14) incluye una primera clave, la primera clave almacenada en la cookie (14) está en una forma codificada, que es codificada bajo una contraseña dependiente de la información conocida únicamente por el usuario, la primera clave también es conocida para el servidor de la red (30) y asociada en el servidor de la red (30) al usuario,
un buscador (11) que recibe del servidor de la red (30) una página web (42) que contiene un applet (12) incrustado en respuesta a una petición de acceso (41) dirigida a la página de red (42), el applet (12) incrustado en la página web (42) requiere que el usuario introduzca la contraseña,
el applet (12) que descodifica la clave codificada almacenada en la cookie (14), utilizando la contraseña, para generar la primera clave, y
el applet (12) que emplea además la primera clave para autenticar el usuario al servidor y/o los datos de firma transmitidos al servidor.

10. El sistema de conformidad con la reivindicación 9, en el que la primera clave codificada que es almacenada en la cookie (14) es codificada con una combinación de una contraseña conocida por el usuario y la información que representa al menos una de las características del dispositivo (10) de computadora personal.

11. Un sistema para proporcionar autenticación de un usuario a un servidor de la red en el contexto de una sesión de búsqueda en la red (40) con una computadora personal (10) conectada a la internet (20), y que se comunica con el servidor de la red (30) por medio de un buscador de la red (11) capaz de administrar y almacenar cookies, que incluye:

medios para almacenar en el servidor (30) un archivo que asocia cada uno de una pluralidad de usuarios, con una primera clave diferente,
medios, en respuesta a un acceso por un usuario particular que utiliza una computadora personal (10), para la transmisión, hacia la computadora personal (10), de un applet (12) incrustado en una página de red (41) requerida por el acceso de la computadora personal (10) del usuario,
dicho applet (12) que incluye medios de código para:

pedir que el usuario introduzca una contraseña,
el acceso de una cookie (14), si está presente, en la computadora personal (10) del usuario y
la descodificación de una primera clave codificada, almacenada en la cookie (14) con la contraseña para recuperar la primera clave relacionada al usuario, y
el uso de la primera clave para autenticar al usuario hacia el servidor (30) y/o los datos de firma transmitidos al servidor (30).

12. El sistema de conformidad con la reivindicación 11, en el que el usuario puede acceder al servidor de la red (30) con una computadora personal (10) particular que ya mantiene una cookie (14) en almacenamiento que incluye una primera clave codificada bajo dicha contraseña, y en el cual el usuario puede acceder al servidor de la red (30) con otra computadora personal (10) que todavía no mantiene la cookie (14) en almacenamiento, o en el cual el usuario puede acceder al servidor de la red (30) con una computadora personal (10) particular que ya mantiene una cookie (14) en almacenamiento, que incluye una primera clave codificada bajo la contraseña, pero estando la cookie (14) de algún modo perdida o dañada,
dicho archivo almacenado en el servidor (30) también incluye un secreto de migración, o una comprobación de clave de un secreto de migración,
dicho servidor (30) incluye además los medios para autenticar al usuario después de la recepción de la información que compara favorablemente al secreto de migración o la comprobación de clave del secreto de migración almacenado en el servidor (30) o por medio de un protocolo de autenticación que demuestra que el usuario conoce el valor correcto del secreto de migración,
el servidor (30) transmite una indicación que significa que el usuario será autenticado después de la presentación de la contraseña.

13. El sistema de conformidad con la reivindicación 12, en el que la información incluye la primera clave codificada bajo la contraseña.

14. El sistema de conformidad con la reivindicación 12, en el que la información contiene una segunda clave, diferente de la primera clave, codificada bajo la contraseña, en donde la segunda clave puede ser utilizada en vez de la primera clave por el applet (12) para autenticar el usuario al servidor (30).

15. El sistema de conformidad con la reivindicación 12, en el que el medio para la transmisión del applet (12) transmite el applet en uno o más segmentos.

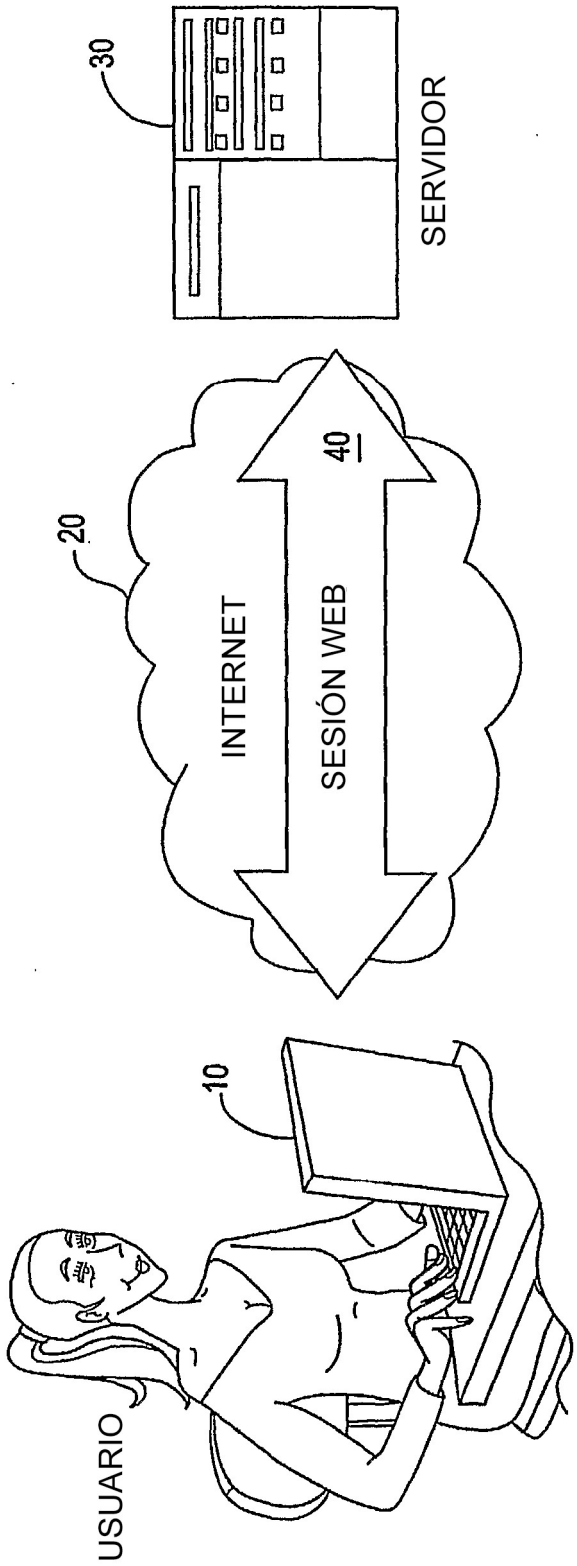
30
SERVIDOR
20
INTERNET
SESIÓN WEB
40
10
USUARIO
DISPOSITIVO
INFORMÁTICO
PERSONAL

FIG. 1

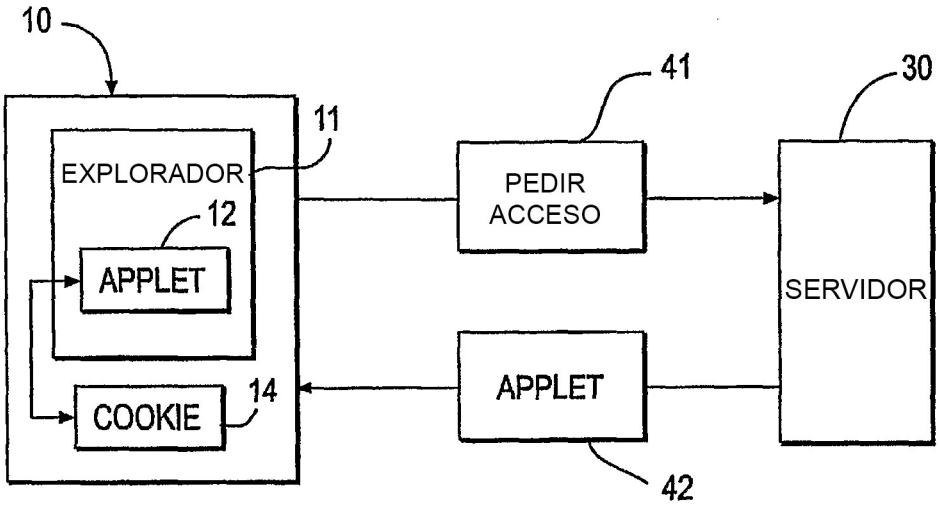
10
11
EXPLORADOR
12
APPLET
COOKIE
14
41
PEDIR
ACCESO
30
SERVIDOR
APPLET
42

FIG. 2

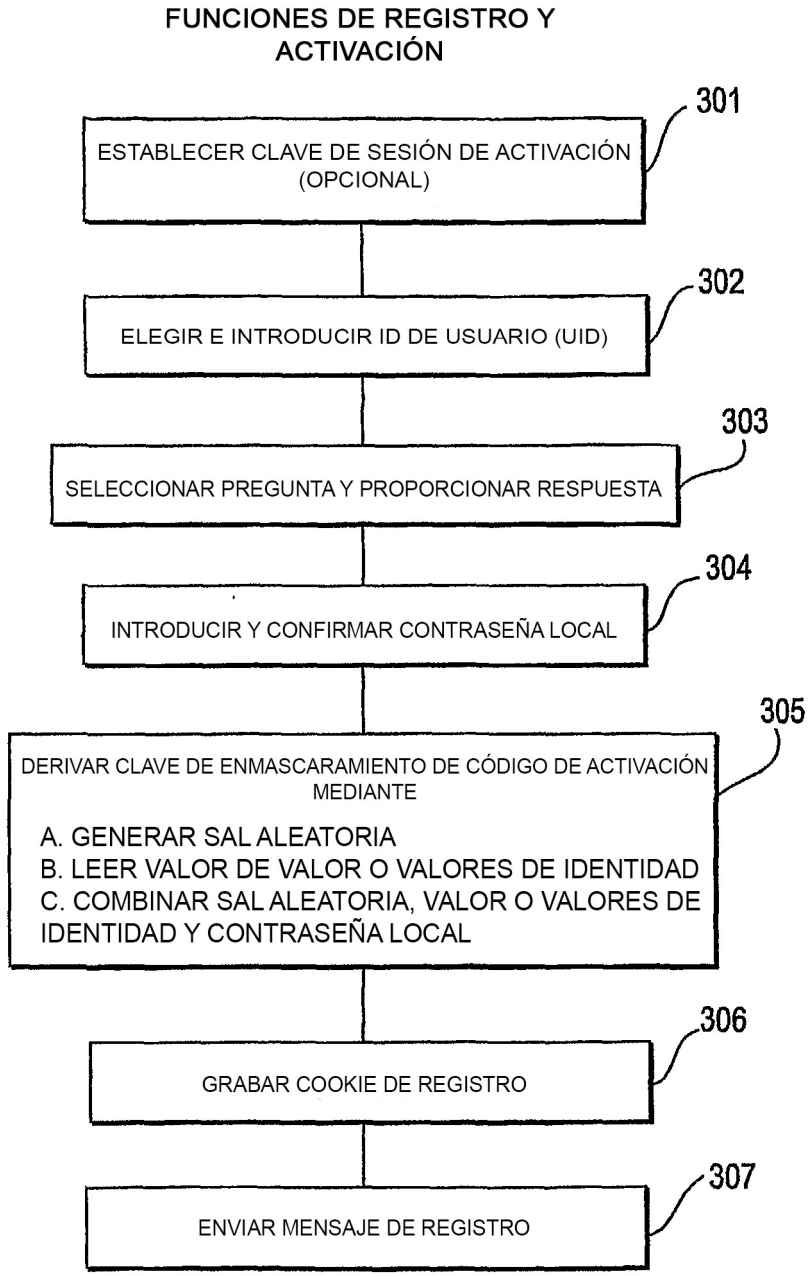
FUNCIONES DE REGISTRO Y ACTIVACIÓN
301
ESTABLECER CLAVE DE SESIÓN DE ACTIVACIÓN (OPCIONAL)
302
ELEGIR E INTRODUCIR ID DE USUARIO (UID)
303
SELECCIONAR PREGUNTA Y PROPORCIONAR RESPUESTA
304
INTRODUCIR Y CONFIRMAR CONTRASEÑA LOCAL
305
DERIVAR CLAVE DE ENMASCARAMIENTO DE CÓDIGO DE ACTIVACIÓN MEDIANTE
A. GENERAR SAL ALEATORIA
B. LEER VALOR DE VALOR O VALORES DE IDENTIDAD
C. COMBINAR SAL ALEATORIA, VALOR O VALORES DE IDENTIDAD Y CONTRASEÑA LOCAL
306
GRABAR COOKIE DE REGISTRO
307
ENVIAR MENSAJE DE REGISTRO

FIG. 3

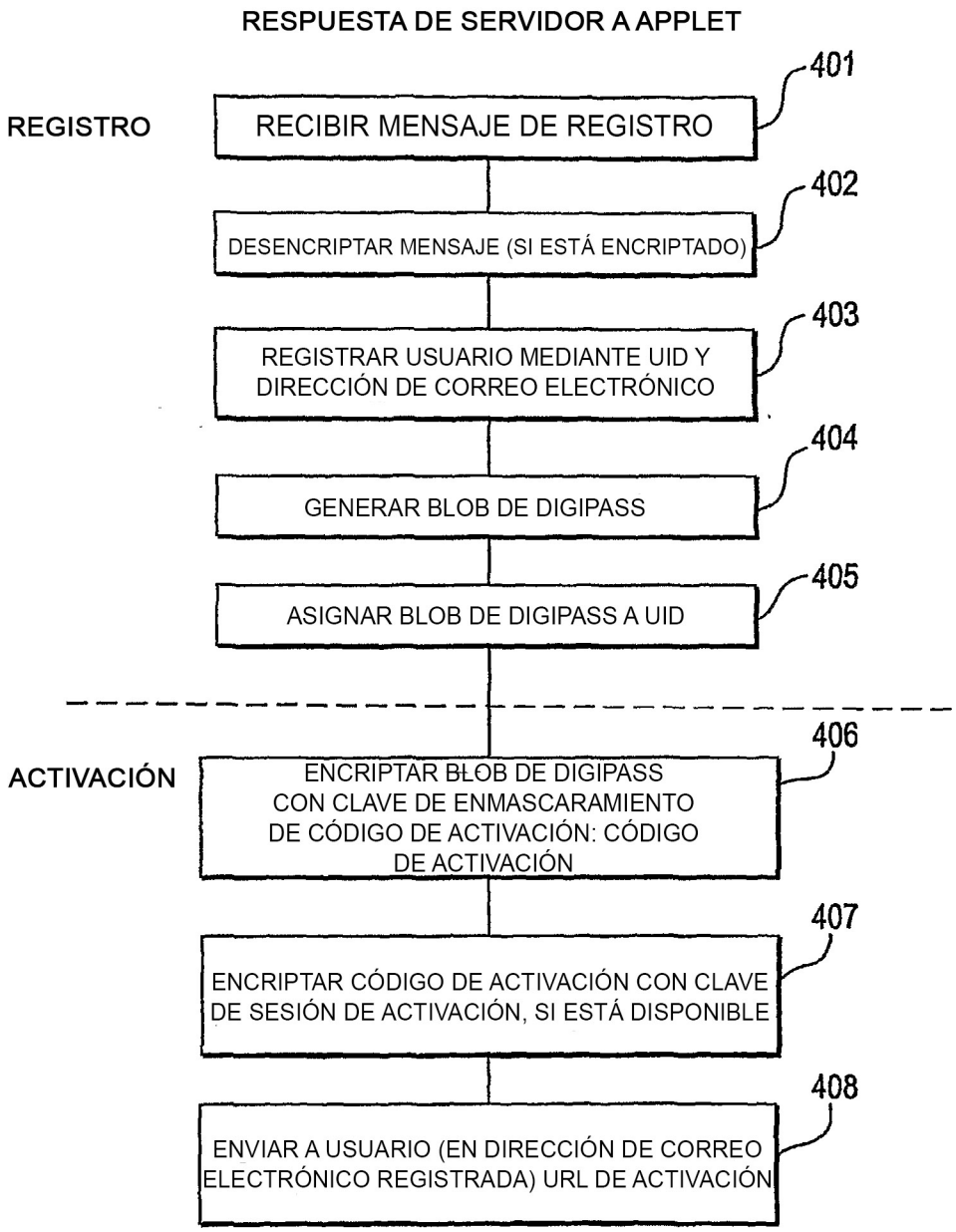
RESPUESTA DE SERVIDOR A APPLET
REGISTRO
RECIBIR MENSAJE DE REGISTRO
401
DESENCRIPTAR MENSAJE (SI ESTÁ ENCRIPTADO)
402
REGISTRAR USUARIO MEDIANTE UID Y DIRECCIÓN DE CORREO ELECTRÓNICO
403
GENERAR BLOB DE DIGIPASS
404
ASIGNAR BLOB DE DIGIPASS A UID
405
ACTIVACIÓN
ENCRIPTAR BLOB DE DIGIPASS CON CLAVE DE ENMASCARAMIENTO DE CÓDIGO DE ACTIVACIÓN: CÓDIGO DE ACTIVACIÓN
406
ENCRIPTAR CÓDIGO DE ACTIVACIÓN CON CLAVE DE SESIÓN DE ACTIVACIÓN, SI ESTÁ DISPONIBLE
407
ENVIAR A USUARIO (EN DIRECCIÓN DE CORREO ELECTRÓNICO REGISTRADA) URL DE ACTIVACIÓN
408

FIG. 4

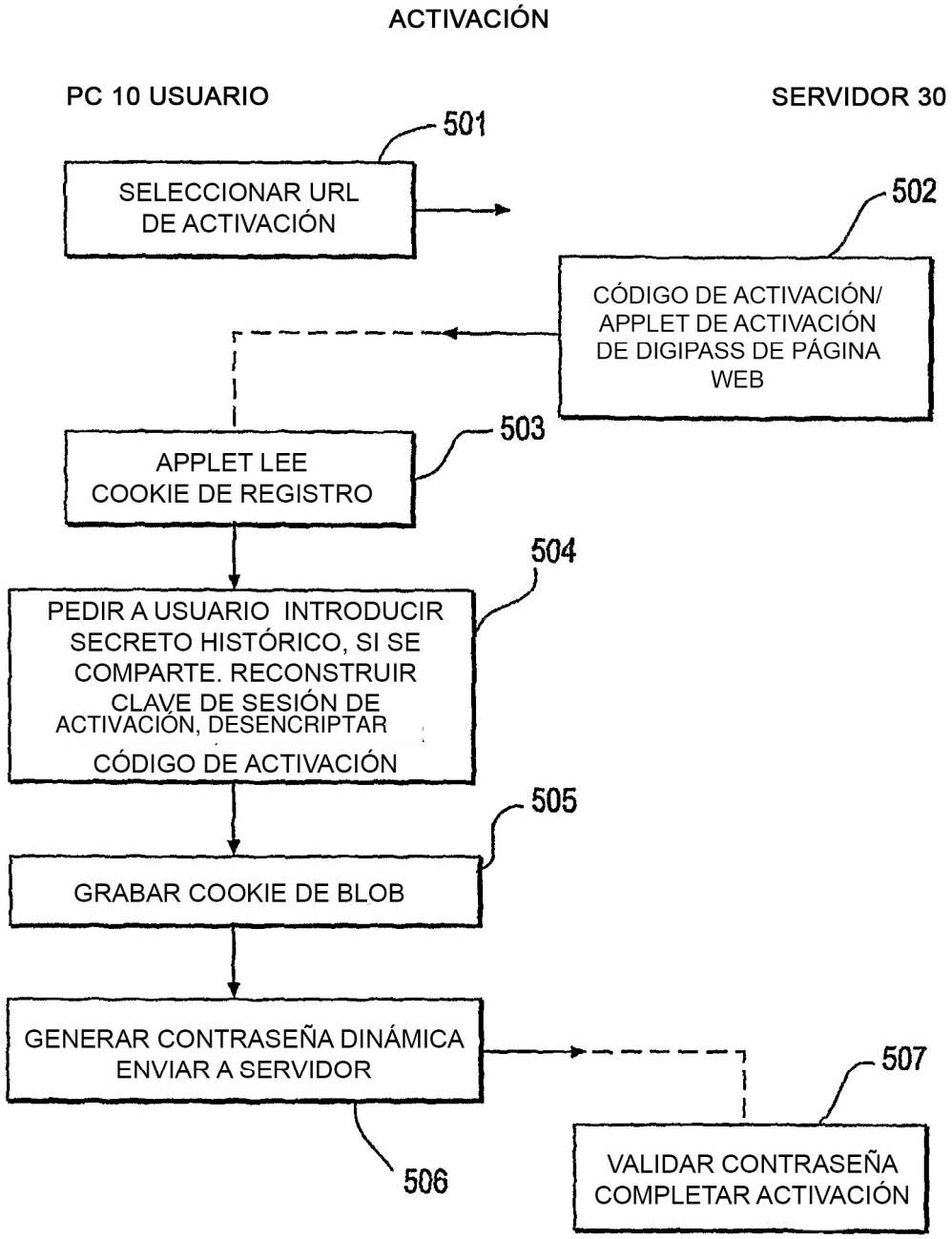
ACTIVACIÓN
PC 10 USUARIO
SERVIDOR 30
501
SELECCIONAR URL DE ACTIVACIÓN
502
CÓDIGO DE ACTIVACIÓN/ APPLET DE ACTIVACIÓN DE DIGIPASS DE PÁGINA WEB
503
APPLET LEE COOKIE DE REGISTRO
504
PEDIR A USUARIO INTRODUCIR SECRETO HISTÓRICO, SI SE COMPARTE. RECONSTRUIR CLAVE DE SESIÓN DE ACTIVACIÓN, DESENCRIPTAR CÓDIGO DE ACTIVACIÓN
505
GRABAR COOKIE DE BLOB
GENERAR CONTRASEÑA DINÁMICA ENVIAR A SERVIDOR
506
507
VALIDAR CONTRASEÑA COMPLETAR ACTIVACIÓN

FIG. 5

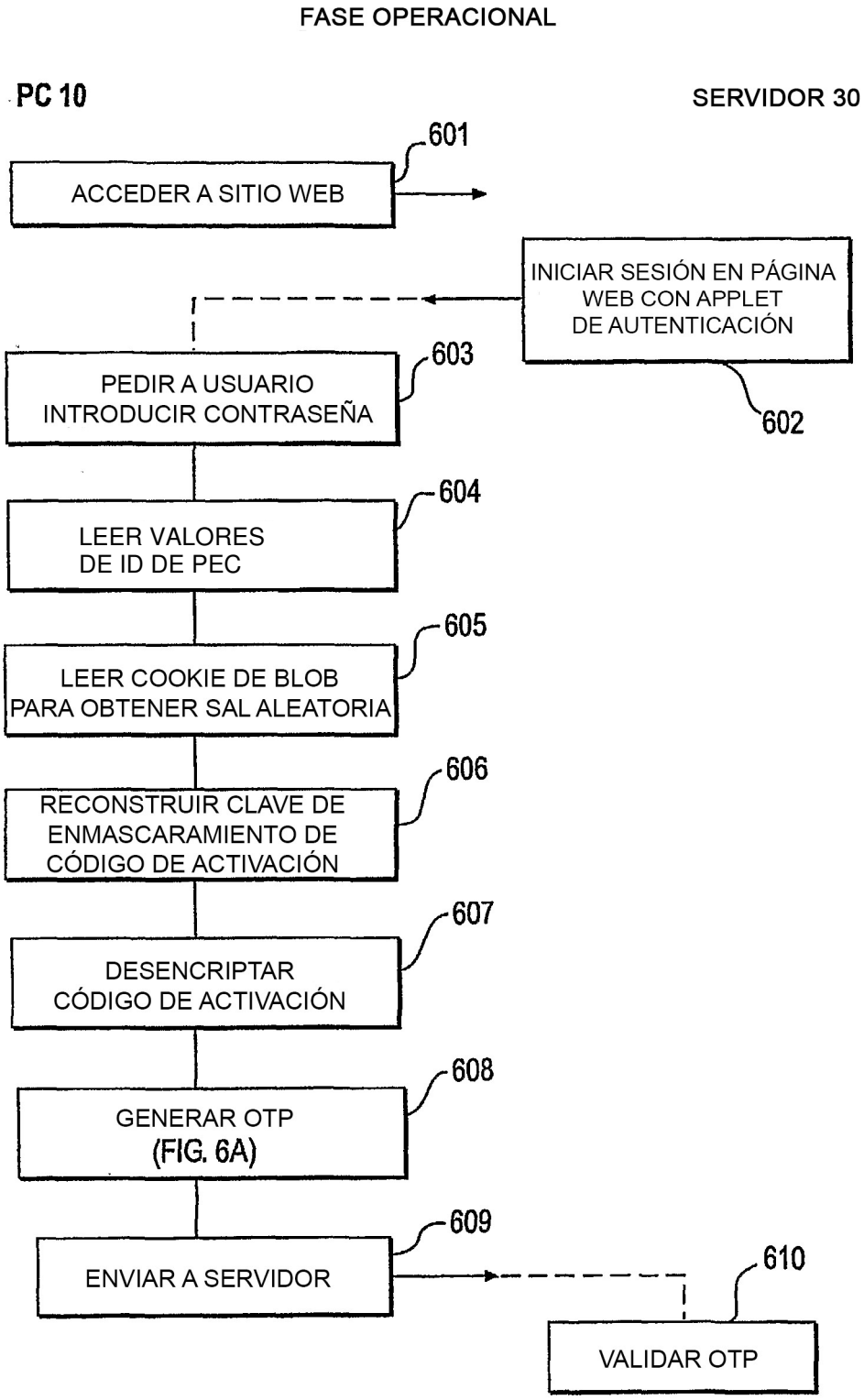
FASE OPERACIONAL
PC 10
SERVIDOR 30
601
ACCEDER A SITIO WEB
INICIAR SESIÓN EN PÁGINA WEB CON APPLET DE AUTENTICACIÓN
602
603
PEDIR A USUARIO INTRODUCIR CONTRASEÑA
604
LEER VALORES DE ID DE PEC
605
LEER COOKIE DE BLOB PARA OBTENER SAL ALEATORIA
606
RECONSTRUIR CLAVE DE ENMASCARAMIENTO DE CÓDIGO DE ACTIVACIÓN
607
DESENCRIPTAR CÓDIGO DE ACTIVACIÓN
608
GENERAR OTP (FIG. 6A)
609
ENVIAR A SERVIDOR
610
VALIDAR OTP

FIG. 6

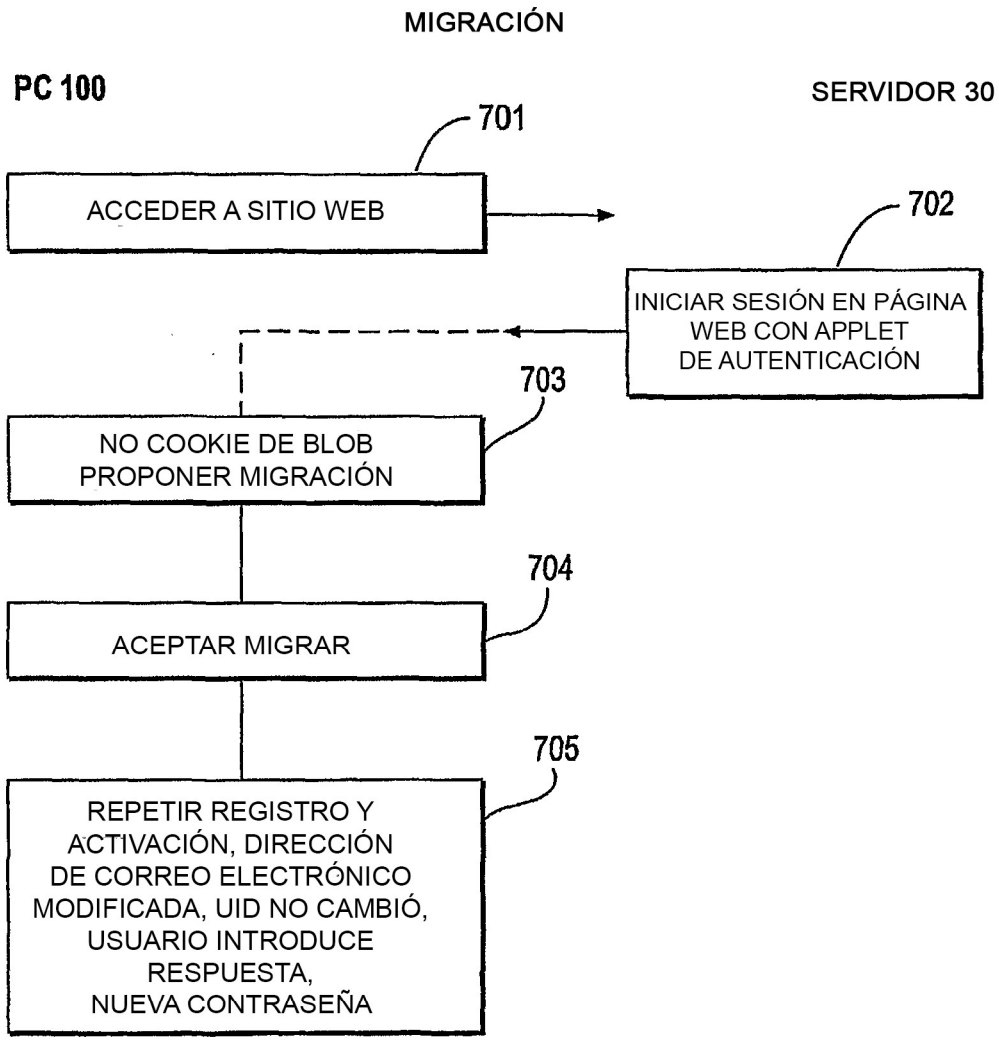
MIGRACIÓN
PC 100
SERVIDOR 30
701
ACCEDER A SITIO WEB
702
INICIAR SESIÓN EN PÁGINA WEB CON APPLET DE AUTENTICACIÓN
703
NO COOKIE DE BLOB PROPONER MIGRACIÓN
704
ACEPTAR MIGRAR
705
REPETIR REGISTRO Y ACTIVACIÓN, DIRECCIÓN DE CORREO ELECTRÓNICO MODIFICADA, UID NO CAMBIÓ, USUARIO INTRODUCE RESPUESTA, NUEVA CONTRASEÑA

FIG. 7