(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 553 713**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE REIVINDICACIONES DE SOLICITUD DE PATENTE EUROPEA T1

(96) Fecha de presentación y número de la solicitud europea: **28.03.2013 E 13772872 (1)**

(97) Fecha y número de publicación de la solicitud europea: **11.02.2015 EP 2834959**

(30) Prioridad:

01.04.2012 US 201261618813 P
10.05.2012 US 201261645252 P

(46) Fecha de publicación y mención en BOPI de la traducción de las reivindicaciones de la solicitud:
11.12.2015

(71) Solicitantes:

AUTHENTIFY, INC. (100.0%)
8745 West Higgins Road, Suite 240
Chicago, IL 60631, US

(72) Inventor/es:

NEUMAN, MICHAEL y
NEUMAN, DIANA

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

(54) Título: **Autentificación segura en un sistema con múltiples partes**

ES 2 553 713 T1

REIVINDICACIONES

1. Sistema de red capaz de autentificar a múltiples usuarios diferentes ante múltiples proveedores de servicios diferentes (801), que comprende:

un servidor de autentificación (100, 713) configurado para almacenar (i) un identificador de proveedor para cada uno de los múltiples proveedores de servicios diferentes en asociación con los requisitos de política de autentificación de los proveedores para el proveedor de servicios aplicable y (ii) un identificador de usuario para cada uno de los múltiples usuarios diferentes en asociación con la información de validación para el usuario de aplicación;
un primer dispositivo utilizable por un primero de los múltiples usuarios diferentes, y configurado para (901) transmitir una solicitud de entrada a un primero de los múltiples proveedores de servicios diferentes a través de la red;
un servidor de red, asociado a un primer proveedor de servicios (103) y configurado para transmitir, al servidor de autentificación a través de la red, (i) una solicitud de un número aleatorio y (ii) otras informaciones, donde el servidor de autentificación está configurado para (903) transmitir un número aleatorio al servidor de red a través de la red en respuesta a la solicitud de número aleatorio transmitida, donde el servidor de red está configurado además para transmitir el número aleatorio transmitido al primer dispositivo a través de la red en respuesta a la solicitud de entrada transmitida;
un segundo dispositivo (400) manejable por el primer usuario, y configurado (i) para recibir una entrada que le transfiere el otro número aleatorio desde el primer dispositivo, y (ii) para transmitir además el número aleatorio de entrada y una solicitud del primer usuario para ser autentificado en el servidor de autentificación a través de la red;
donde el servidor de autentificación está configurado además para (905) transmitir, después de la transmisión por parte del segundo dispositivo del número aleatorio y de la solicitud de autentificación, el identificador del primer proveedor almacenado y los requisitos de política de autentificación del primer proveedor almacenados, y transmitir otras informaciones transmitidas, al segundo dispositivo a través de la red;
donde el segundo dispositivo está configurado (907) además para transmitir, en respuesta a los requisitos de política de autentificación del primer proveedor, un identificador del primer usuario (Qid) e información de validación de entrada del usuario al servidor de autentificación a través de la red;
donde el servidor de autentificación está configurado además para asociar el identificador del primer usuario transmitido con el identificador del primer usuario almacenado, para determinar que la información de validación transmitida corresponde con los requisitos de política de autentificación del primer proveedor de servicios almacenados, y para comparar la información de validación transmitida con la información de validación almacenada en asociación con el identificador del primer usuario para autentificar el primer usuario;
donde el segundo dispositivo está configurado además para transmitir un mensaje, incluyendo el número aleatorio transferido y las otras informaciones transmitidas, firmado con una credencial del primer usuario, al servidor de autentificación a través de la red; y
donde el servidor de autentificación está además configurado para (908) transmitir un aviso de autentificación del primer usuario y además para transmitir el mensaje firmado recibido al servidor de red a través de la red.

2. Sistema de red según la reivindicación 1, donde:

la credencial del primer usuario es una credencial del primer usuario asociada sólo con el primer proveedor (103) y no con otros de los múltiples proveedores de servicios diferentes;
el número aleatorio es un identificador de sesión (Qsid); y
la otra información es otro número aleatorio.

3. Sistema de red según la reivindicación 1, donde:

el segundo dispositivo (400) está además configurado para transmitir la credencial del primer usuario al servidor de autentificación (100, 713) a través de la red; y
el servidor de autentificación está además configurado para almacenar la credencial del primer usuario en asociación con el identificador del primer usuario (Qid), y para verificar el número aleatorio y la otra información del mensaje firmado transmitido mediante la aplicación de la credencial del primer usuario almacenada al mensaje firmado recibido, para autentificar todavía más al primer usuario.

4. Sistema de red según la reivindicación 3, donde:

la credencial del primer usuario almacenada es una clave pública de un par de claves privada/pública del primer usuario, una clave privada del par de claves privada/pública del primer usuario sólo la conoce el primer usuario, y el mensaje firmado transmitido se firma con la clave privada; y
el servidor de autentificación (100, 713) también transmite un certificado, que incluye la clave pública del

primer usuario y se firma con una clave privada de un par de claves privada/pública del servidor de autentificación, al primer proveedor de servicios (103) a través de la red con el aviso de autentificación y el mensaje firmado recibido.

5. Sistema de red según la reivindicación 4, donde:

el primer par de claves privada/pública del usuario es un primer par de claves privada/pública del primer usuario asociadas sólo con el primer proveedor (103) y no con otros de los múltiples proveedores de servicios.

6. Sistema de red según la reivindicación 3, donde:

el servidor de autentificación (100, 713) está configurado además para recibir un aviso de que la credencial del primer usuario está en peligro, y para invalidar la credencial del primer usuario en respuesta al aviso recibido.

7. Sistema de red según la reivindicación 6, donde:

el primer dispositivo está además configurado para transmitir otra solicitud de entrada al primer proveedor de servicios (103) a través de la red;
el servidor de red está además configurado para transmitir, al servidor de autentificación (100, 713) a través de la red, (i) otra solicitud de otro número aleatorio y (ii) otras informaciones, donde el servidor de autentificación está además configurado para transmitir otro número aleatorio al servidor de red a través de la red en respuesta a la otra solicitud de número aleatorio transmitida, donde el servidor de red está además configurado para transmitir el otro número aleatorio transmitido al primer dispositivo a través de la red en respuesta a la otra solicitud de entrada transmitida;
el segundo dispositivo (400) está además configurado para recibir una entrada que le transfiere el otro número aleatorio transmitido desde el primer dispositivo, y para transmitir además el otro número aleatorio transferido y otra solicitud del primer usuario para ser autentificado en el servidor de autentificación a través de la red;
el servidor de autentificación está configurado además para transmitir de nuevo, después de la transmisión por parte del segundo dispositivo del otro número aleatorio y de la otra solicitud de autentificación, el identificador del primer proveedor almacenado y los requisitos de política de autentificación del proveedor almacenados asociados, y para transmitir además las otras informaciones transmitidas, al segundo dispositivo a través de la red;
el segundo dispositivo está además configurado para transmitir de nuevo, en respuesta a los requisitos de política de autentificación del primer proveedor transmitidos de nuevo, el identificador del primer usuario (Qid) y la información de validación de entrada del usuario al servidor de autentificación a través de la red; y
el servidor de autentificación está además configurado para asociar el identificador del primer usuario transmitido de nuevo al identificador del primer usuario almacenado, para determinar que la información de validación nuevamente transmitida corresponde a los requisitos de política de autentificación del primer proveedor de servicios almacenados, para comparar la información de validación nuevamente transmitida con la información de validación almacenada en asociación con el identificador del primer usuario para autentificar al primer usuario, y, después de que el servidor de autentificación haya invalidado la credencial del primer usuario almacenada, para determinar que la credencial de primer usuario almacenada es inválida.

8. Sistema de red según la reivindicación 7, donde:

el servidor de autentificación (100, 713), si además está configurado para transmitir, al primer proveedor de servicios (103) a través de la red después de determinar que la credencial del primer usuario almacenada es inválida, un aviso de autentificación del primer usuario basado en la información de validación y de la invalidez de la credencial del primer usuario.

9. Sistema de red según la reivindicación 7, donde:

el servidor de autentificación (100, 713) está configurado además para transmitir una solicitud de una credencial de sustitución al segundo dispositivo (400) a través de la red, después de determinar que la credencial del primer usuario almacenada es inválida;
el segundo dispositivo está además configurado para transmitir, en respuesta a la solicitud de la credencial de sustitución transmitida, una credencial de sustitución al servidor de autentificación a través de la red; y
el servidor de autentificación está además configurado para almacenar la credencial de sustitución transmitida en asociación con el identificador del primer usuario (Qid), generar un certificado para la credencial de sustitución transmitida, y transmitir, al segundo dispositivo a través de la red, el certificado

generado para ser utilizado al volver a registrar al primer usuario en el primer proveedor de servicios (103).

10. Sistema de red según la reivindicación 9, donde:

el segundo dispositivo (400) está configurado además para transmitir, al servidor de autentificación (100, 713) a través de la red, otro mensaje, con el otro número aleatorio y las otras informaciones, firmado con la credencial de sustitución del primer usuario; y
el servidor de autentificación está configurado además para (i) verificar el otro número aleatorio y la otra información mediante la aplicación de la credencial de sustitución del primer usuario almacenada a otro mensaje firmado recibido para autentificar al primer usuario, y (ii) transmitir, al servidor de red a través de la red, un aviso de autentificación del primer usuario y el otro mensaje firmado.

11. Sistema de red según la reivindicación 3, donde el segundo dispositivo (400) está además configurado para transmitir, al servidor de autentificación (100, 713) a través de la red, otra credencial del primer usuario, y el servidor de autentificación está además configurado para almacenar la otra credencial del primer usuario recibida en asociación con otro identificador para el primer usuario, y que comprende además:

otro servidor de red, asociado a un segundo de los múltiples proveedores de servicios diferentes y configurado para transmitir, al servidor de autentificación a través de la red, (i) una solicitud de otro número aleatorio y (ii) de otras informaciones;
donde el servidor de autentificación está configurado además para transmitir otro número aleatorio al otro servidor de red a través de la red en respuesta a la otra solicitud de número aleatorio transmitida;
donde el primer dispositivo está además configurado para transmitir otra solicitud de entrada al segundo proveedor de servicios a través de la red;
donde el otro servidor de red está además configurado para transmitir el otro número aleatorio transmitido al primer dispositivo a través de la red en respuesta a la otra solicitud de entrada de registro;
donde el segundo dispositivo está además configurado para recibir una entrada que le transfiere el otro número aleatorio transmitido desde el primer dispositivo, y para transmitir además el otro número aleatorio de entrada y otra solicitud del primer usuario para ser autentificado en el servidor de autentificación a través de la red;
donde el servidor de autentificación está además configurado para transmitir, después de la transmisión por parte del segundo dispositivo del otro número aleatorio y de la otra solicitud de autentificación, el identificador del segundo proveedor almacenado y los requisitos de política de autentificación del segundo proveedor asociados almacenados, y para transmitir además las otras informaciones transmitidas al segundo dispositivo a través de la red;
donde el segundo dispositivo está configurado además para transmitir, en respuesta a los requisitos de política de autentificación del segundo proveedor transmitidos, otro identificador del primer usuario y otras informaciones de validación de entrada del usuario al servidor de autentificación a través de la red;
donde el servidor de autentificación está además configurado para asociar el otro identificador del primer usuario transmitido al otro identificador del primer usuario almacenado, para determinar que la otra información de validación transmitida corresponde a los requisitos de política de autentificación del segundo proveedor de servicios almacenados, y para comparar la otra información de validación transmitida con la información de validación almacenada en asociación con el otro identificador del primer usuario para autentificar al primer usuario;
donde el segundo dispositivo está además configurado para transmitir otro mensaje, con el otro número aleatorio transferido y la otra información transmitida, firmado con otra credencial del primer usuario, al servidor de autentificación a través de la red; y
donde el servidor de autentificación está además configurado para transmitir otro aviso de autentificación del primer usuario y para transmitir además el otro mensaje firmado recibido al otro servidor de red a través de la red.

12. Sistema de red según la reivindicación 1, donde:

el segundo dispositivo está configurado además para transmitir, al servidor de autentificación (100, 713) a través de la red, los requisitos de política de autentificación del primer usuario; y
el servidor de autentificación está configurado además para almacenar los requisitos de política de autentificación del primer usuario transmitidos, para comparar los requisitos de política de autentificación del primer proveedor almacenados con los requisitos de política de autentificación del primer usuario almacenados, para determinar cualquier requisito de política de autentificación adicional determinado basándose en la comparación, para transmitir cualquier requisito de política de autentificación adicional determinado al segundo dispositivo a través de la red, y también para determinar que la información de validación transmitida por el segundo dispositivo corresponde a cualquier requisito de política de autentificación adicional determinado.

13. Sistema de red según la reivindicación 1, donde:

el segundo dispositivo (400) está configurado además para generar datos secretos del primer usuario, para dividir los datos secretos en partes múltiples, para cifrar la primera credencial de usuario con los datos secretos, para almacenar la credencial cifrada y para transmitir una primera de las múltiples partes de datos secretos al servidor de autentificación (100, 713) a través de la red;
el servidor de autentificación está configurado además para almacenar la primera parte de datos secretos transmitida, y para transmitir la primera parte de datos secretos almacenada al segundo dispositivo a través de la red después de autentificar al primer usuario;
el segundo dispositivo está configurado además para combinar la primera parte de datos secretos transmitida por el servidor de autentificación con las otras partes de datos secretos para obtener todos los datos secretos, y para descifrar la credencial cifrada almacenada con los datos secretos obtenidos; y
el mensaje firmado se firma con la credencial descifrada.

14. Sistema de red según la reivindicación 1, donde:

el servidor de red está además configurado para transmitir, al servidor de autentificación (100, 713) a través de la red, el identificador del primer proveedor de servicios, un identificador de transacción, requisitos de autentificación de transacción, y un mensaje con respecto a la transacción, donde el mensaje se cifra con una clave pública de un par de claves privada/pública del primer usuario, donde una clave privada del par de claves privada/pública del primer usuario la conoce sólo el primer usuario, y se firma también con una clave privada de un par de claves privada/pública del primer proveedor de servicios (103), donde una clave pública del par de claves privada/pública del primer proveedor de servicios la conoce el primer usuario;
el servidor de autentificación (100, 713) está configurado además para transmitir, al segundo dispositivo (400) a través de la red, el identificador de transacción transmitido, los requisitos de autentificación de transacción y el mensaje encriptado firmado;
el segundo dispositivo está configurado además para transmitir, al servidor de autentificación a través de la red después de la transmisión del identificador de transacción, los requisitos de autentificación de transacción y el mensaje encriptado firmado, al menos una de entre una aprobación de transacción y una información de autentificación; y
el servidor de autentificación está además configurado para (a) determinar, basado en al menos una de entre la aprobación de transacción y la información de autentificación recibidas, que al menos una de (i) la transacción identificada es aprobada por el primer usuario y (ii) que el primer usuario es auténtico, y (b) transmitir una notificación de la determinación a por lo menos uno de entre el servidor de red y el primer dispositivo a través de la red.

15. Sistema de red según la reivindicación 1, donde:

el dispositivo del primer usuario y el dispositivo del segundo usuario (400) son el mismo dispositivo;
el número aleatorio sirve como identificador de sesión (Qsid); y la otra información es otro número aleatorio.

16. Sistema de red según la reivindicación 1, donde:

el primer dispositivo está además configurado para mostrar visualmente el otro número aleatorio transmitido desde el servidor de red;
el otro número aleatorio transmitido tiene la forma de un código óptico (200); y
el segundo dispositivo (400) incluye una cámara y la entrada recibida correspondiente al otro número aleatorio transmitido se recibe a través de la cámara como una imagen digital del código óptico presentado.

17. Sistema de red según la reivindicación 1, donde:

el servidor de autentificación (100, 713) está configurado además para almacenar el identificador del proveedor para cada uno de los múltiples proveedores de servicios diferentes en asociación con los requisitos de datos de registro del proveedor para el proveedor de servicio aplicable;
el segundo dispositivo (400) está configurado además para (i) recibir un conjunto de identidades de usuario (806) introducidas por el usuario, datos de registro introducidos por el usuario y una selección del usuario de datos particulares de los datos de registro introducidos que se asociarán a cada identidad respectiva en el conjunto recibido de identidades, y para (ii) almacenar cada identidad respectiva en asociación con los datos de registro particulares seleccionados que se asociarán a dicha identidad;
el primer dispositivo está configurado además para transmitir, a través de la red, una solicitud de registro al servidor de red;
el servidor de red está configurado además para transmitir, al servidor de autentificación a través de la red, una solicitud de otro número aleatorio;
el servidor de autentificación está además configurado para transmitir otro número aleatorio al servidor de

red a través de la red en respuesta a la otra solicitud de número aleatorio transmitida;
el servidor de red está configurado además para transmitir además el otro número aleatorio transmitido al primer dispositivo a través de la red en respuesta a la solicitud de registro transmitida;
el segundo dispositivo está configurado además para recibir una entrada que le transfiere el otro número aleatorio transmitido desde el primer dispositivo, y para transmitir además el otro número aleatorio introducido y una solicitud del primer usuario para registrarse con el primer proveedor de servicio (103) en el servidor de autentificación a través de la red;
el servidor de autentificación está además configurado para transmitir, después de la transmisión por parte del segundo dispositivo del otro número aleatorio y de la solicitud de registro, del identificador del primer proveedor almacenado y de los requisitos de datos de registro del primer proveedor asociados almacenados al segundo dispositivo a través de la red;
el segundo dispositivo está configurado además para recibir una entrada del usuario que selecciona una de las identidades de usuario almacenadas, para recuperar automáticamente los datos de registro particulares almacenados en asociación con la identidad de usuario seleccionada en respuesta a la identidad seleccionada introducida, y para transmitir los datos de registro recuperados al servidor de autentificación a través de la red;
el servidor de autentificación está configurado además para determinar que los datos de registro transmitidos corresponden a los requisitos de datos de registro del primer proveedor de servicios almacenados, y para transmitir además los datos de registro transmitidos al servidor de red a través de la red para registrar al primer usuario con el primer proveedor de servicios.

18. Sistema de red según la reivindicación 1, donde:

el servidor de red está además configurado para transmitir una solicitud de registro y una clave pública de un par de claves privada/pública del primer proveedor de servicios (103) al servidor de autentificación (100, 713) a través de la red, la clave privada del par de claves privada/pública del primer proveedor de servicios la conoce sólo el servidor de red; y
el servidor de autentificación está además configurado para (i) almacenar la clave pública del primer proveedor transmitida, y (ii) transmitir un certificado, con la clave pública del primer proveedor, firmado con una clave privada de un par de claves privada/pública del servidor de autentificación al servidor de red a través de la red, la clave pública del par de claves privada/pública del servidor de autentificación la conoce el servidor de red.

19. Sistema de red según la reivindicación 18, donde:

el segundo dispositivo (400) está además configurado para transmitir una solicitud de registro y una clave pública de un par de claves privada/pública del primer usuario al servidor de autentificación (100, 713) a través de la red, la clave privada del par de claves privada/pública del primer usuario la conoce sólo el segundo dispositivo; y
el servidor de autentificación está además configurado para (i) almacenar la clave pública del primer usuario almacenada, y (ii) transmitir un certificado, con la clave pública del primer usuario, firmado con la clave privada del servidor de autentificación para el segundo dispositivo a través de la red, la clave pública del par de claves privada/pública del servidor de autentificación la conoce el segundo dispositivo.

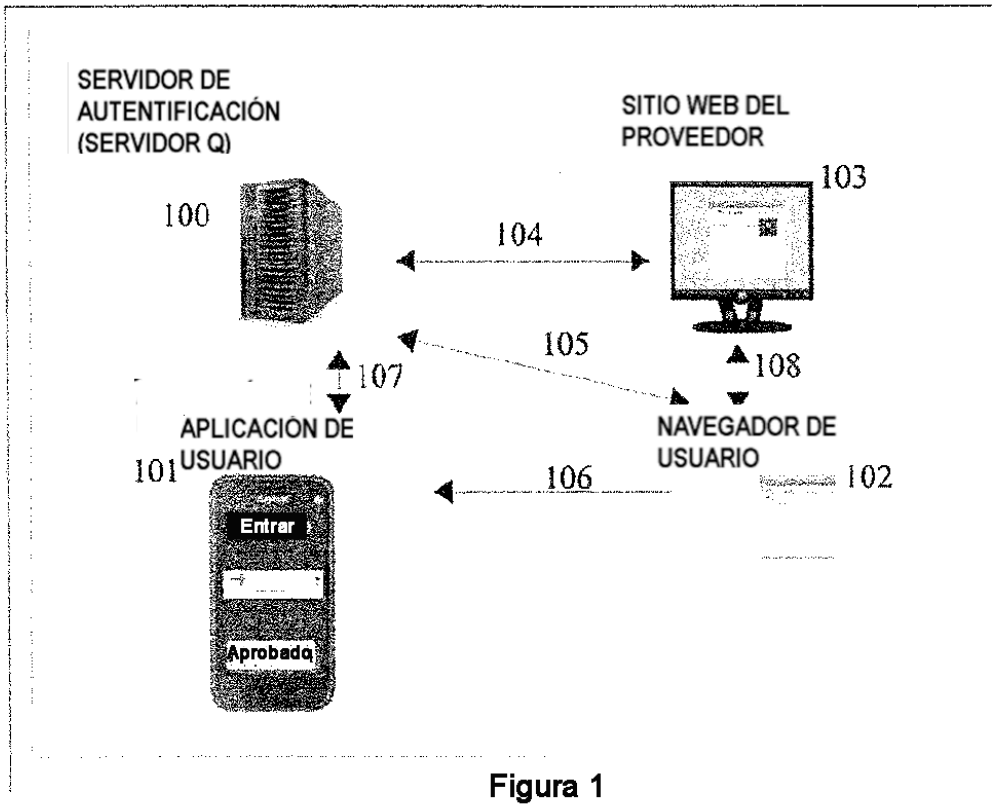
SERVIDOR DE AUTENTIFICACIÓN (SERVIDOR Q)
SITIO WEB DEL PROVEEDOR
100
103
104
105
107
108
APLICACIÓN DE USUARIO
NAVEGADOR DE USUARIO
101
102
106
Entrar
Aprobado

Figura 1

Figura 2

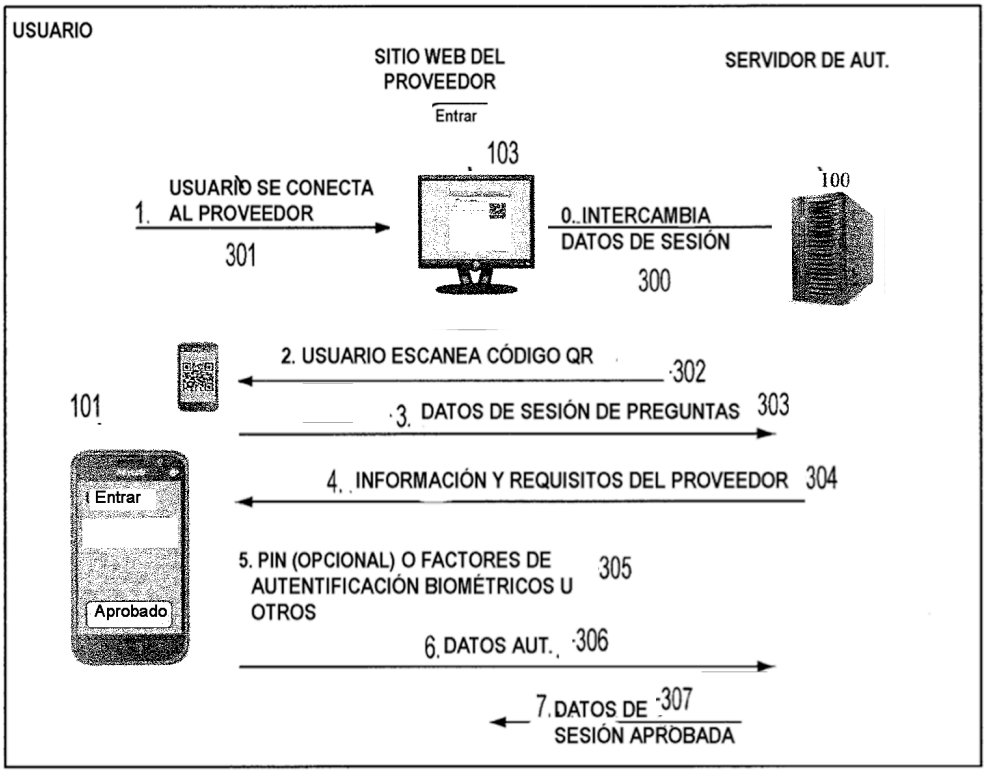

Figura 3

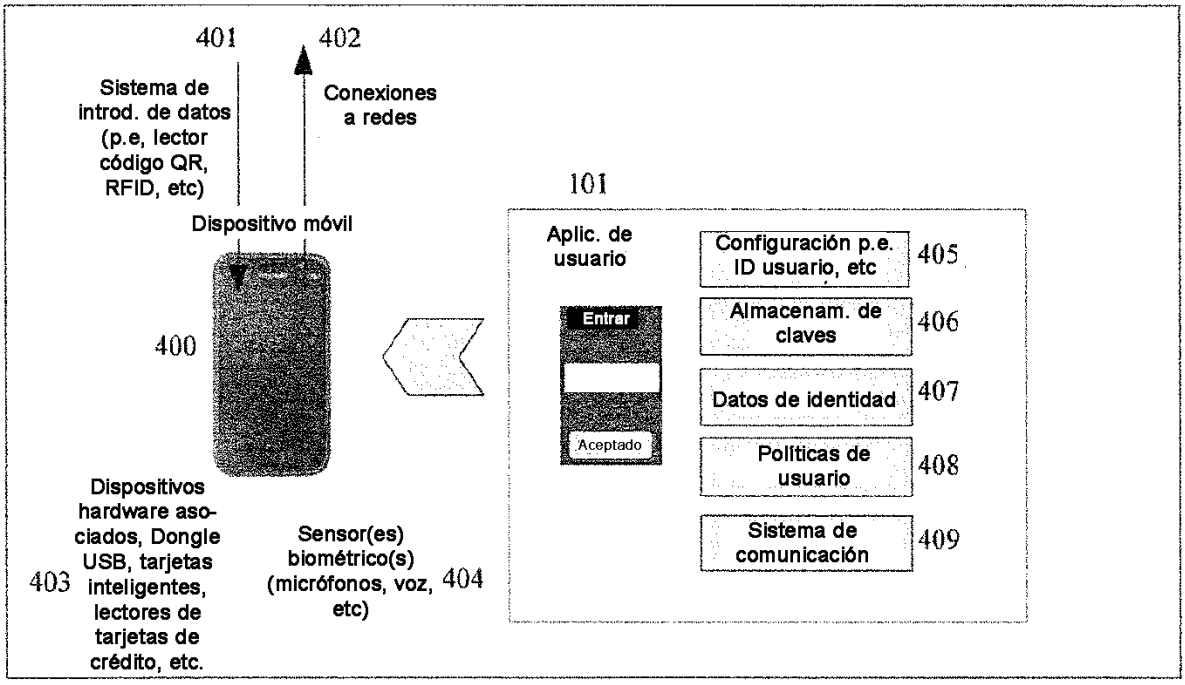
401
402
Sistema de introd. de datos (p.e, lector código QR, RFID, etc)
Conexiones a redes
101
Dispositivo móvil
Aplic. de usuario
Configuración p.e. ID usuario, etc
405
Entrar
Almacenam. de claves
406
400
Datos de identidad
407
Aceptado
Políticas de usuario
408
Sistema de comunicación
409
Dispositivos hardware asociados, Dongle USB, tarjetas inteligentes, lectores de tarjetas de crédito, etc.
403
Sensor(es) biométrico(s) (micrófonos, voz, etc)
404

Figura 4

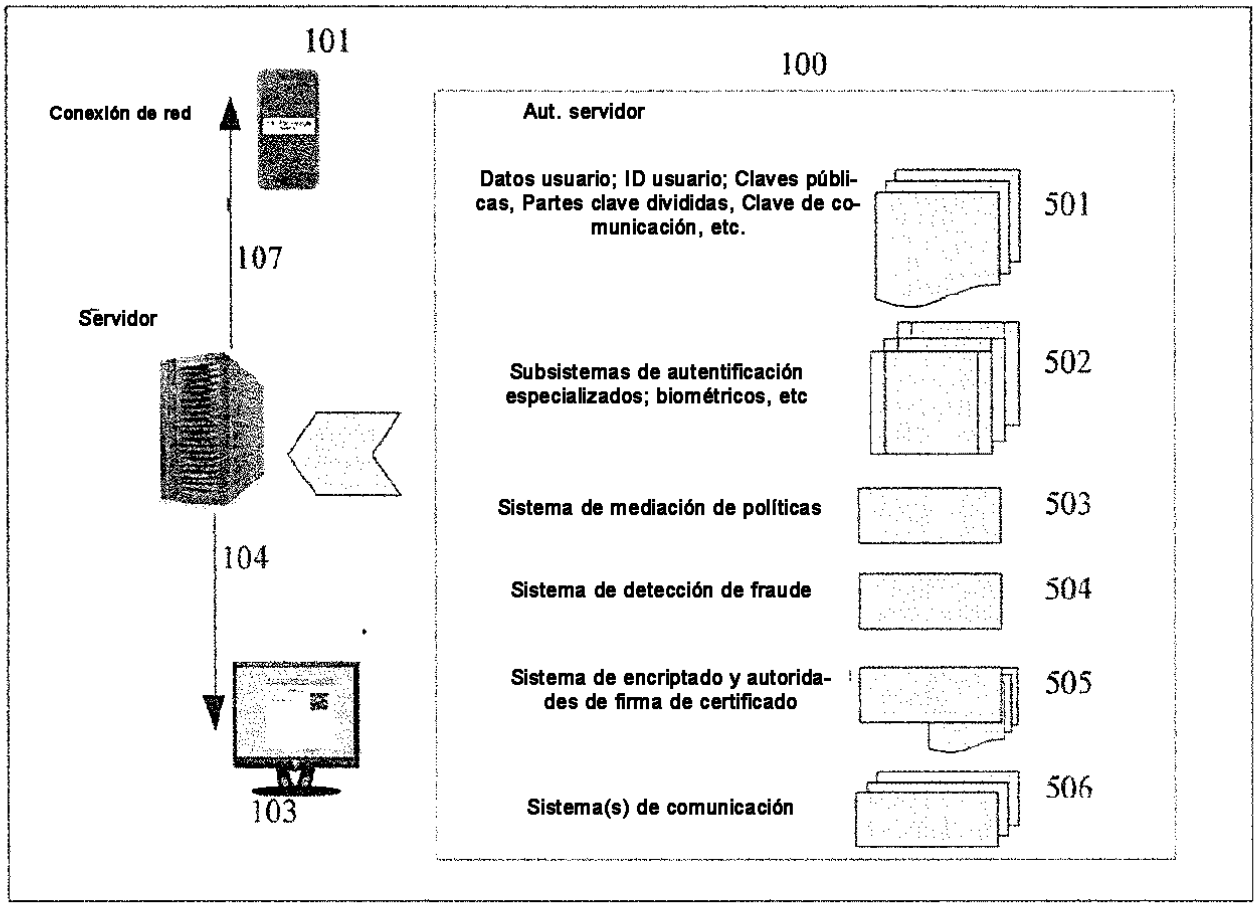
101
Conexión de red
107
Servidor
104
103
100
Aut. servidor
Datos usuario; ID usuario; Claves públicas, Partes clave divididas, Clave de comunicación, etc.
501
Subsistemas de autentificación especializados; biométricos, etc
502
Sistema de mediación de políticas
503
Sistema de detección de fraude
504
Sistema de encriptado y autoridades de firma de certificado
505
Sistema(s) de comunicación
506

Figura 5

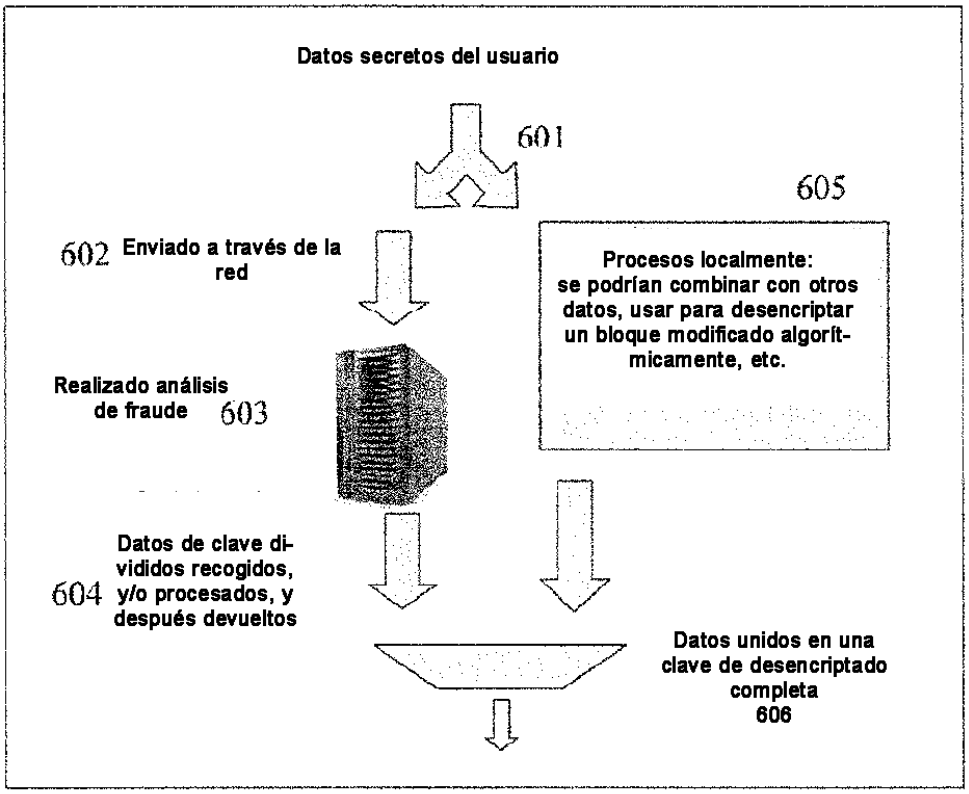
Datos secretos del usuario
601
605
602 Enviado a través de la red
Procesos localmente: se podrían combinar con otros datos, usar para desencriptar un bloque modificado algorítmicamente, etc.
Realizado análisis de fraude 603
Datos de clave divididos recogidos, y/o procesados, y después devueltos
604
Datos unidos en una clave de desencriptado completa
606

Figura 6

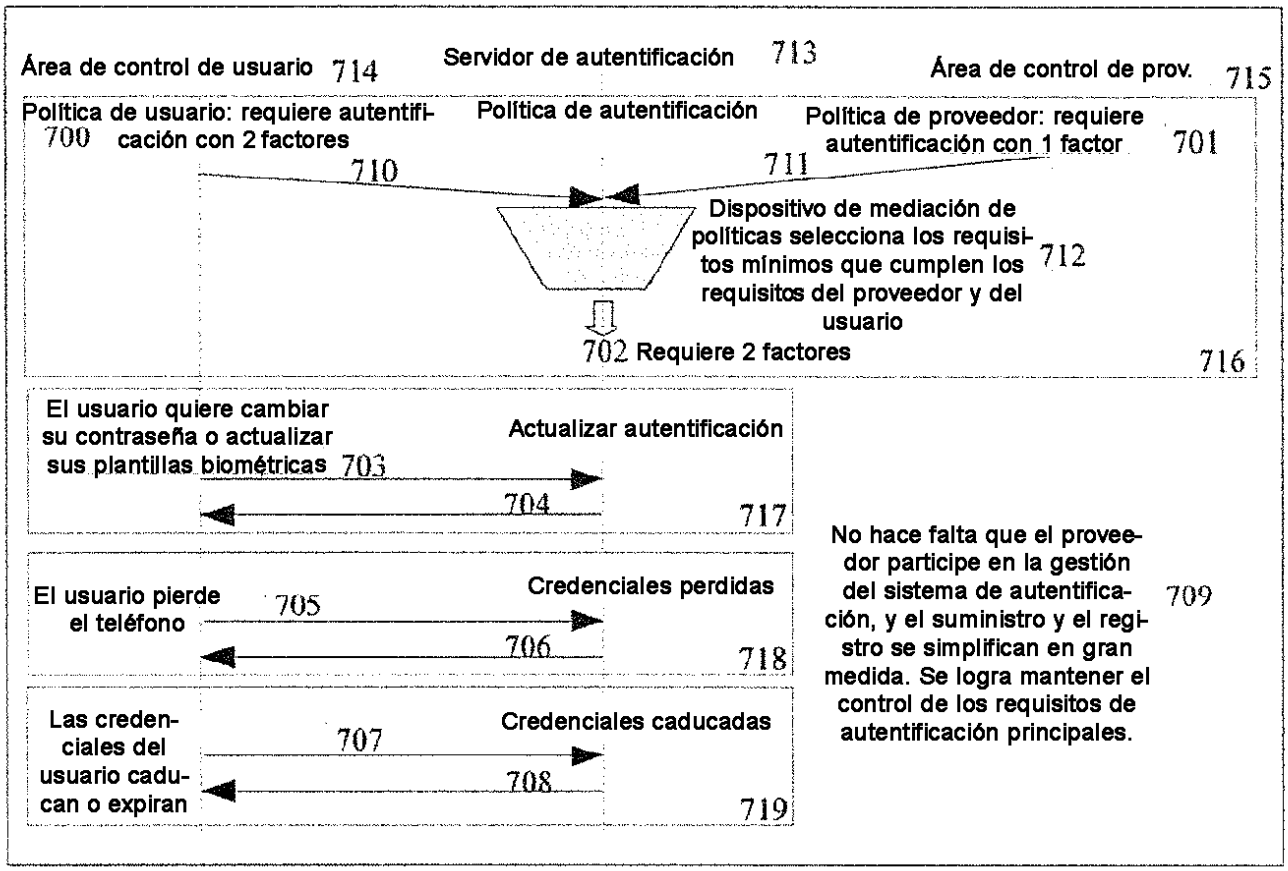
Área de control de usuario 714
Servidor de autentificación 713
Área de control de prov. 715
Política de usuario: requiere autentificación con 2 factores
700
Política de autentificación
Política de proveedor: requiere autentificación con 1 factor
701
710
711
Dispositivo de mediación de políticas selecciona los requisitos mínimos que cumplen los requisitos del proveedor y del usuario
712
702 Requiere 2 factores
716
El usuario quiere cambiar su contraseña o actualizar sus plantillas biométricas
703
Actualizar autentificación
704
717
El usuario pierde el teléfono
705
Credenciales perdidas
706
718
Las credenciales del usuario caducan o expiran
707
Credenciales caducadas
708
719
No hace falta que el proveedor participe en la gestión del sistema de autentificación, y el suministro y el registro se simplifican en gran medida. Se logra mantener el control de los requisitos de autentificación principales.
709

Figura 7

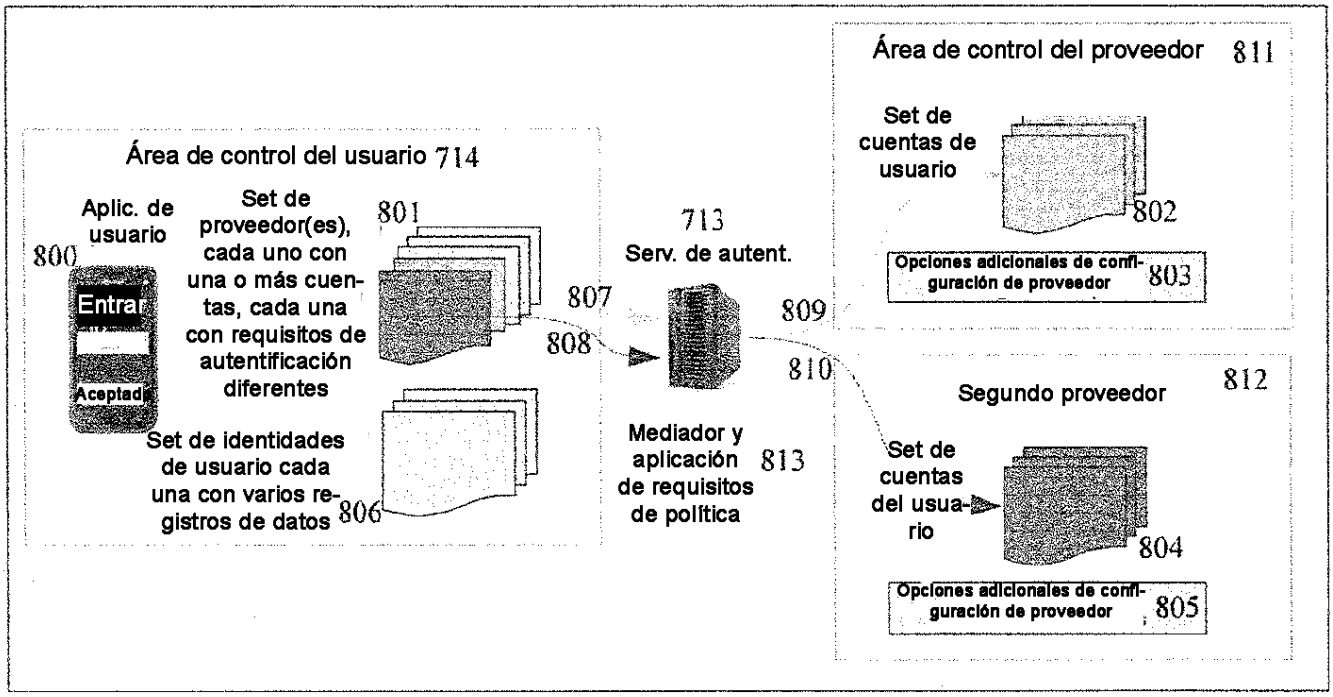
Área de control del usuario 714
Aplic. de usuario
800
Entrar
Aceptado
Set de proveedor(es), cada uno con una o más cuentas, cada una con requisitos de autentificación diferentes
801
Set de identidades de usuario cada una con varios registros de datos
806
807
808
713
Serv. de autent.
Mediador y aplicación de requisitos de política
813
809
810
Área de control del proveedor 811
Set de cuentas de usuario
802
Opciones adicionales de configuración de proveedor
803
Segundo proveedor
812
Set de cuentas del usuario
804
Opciones adicionales de configuración de proveedor
805

Figura 8

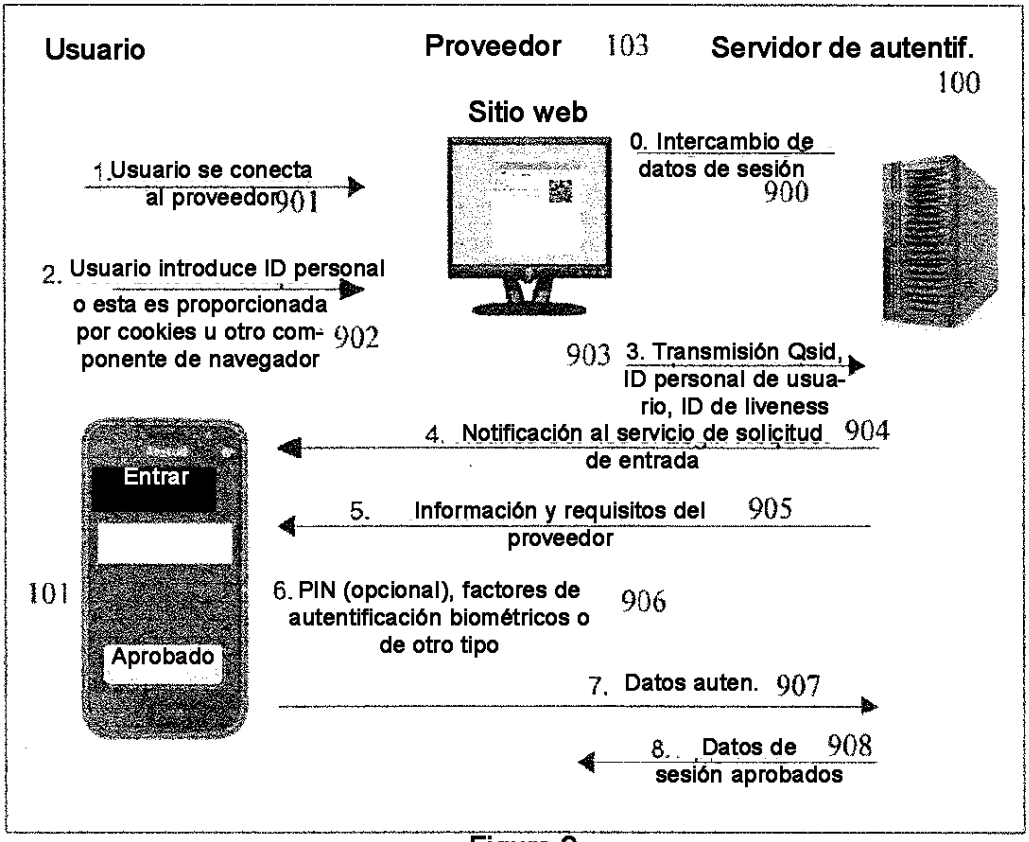
Usuario
Proveedor 103
Servidor de autentif. 100
Sitio web
0. Intercambio de datos de sesión 900
1. Usuario se conecta al proveedor 901
2. Usuario introduce ID personal o esta es proporcionada por cookies u otro componente de navegador 902
903 3. Transmisión Qsid, ID personal de usuario, ID de liveness
4. Notificación al servicio de solicitud de entrada 904
5. Información y requisitos del proveedor 905
6. PIN (opcional), factores de autentificación biométricos o de otro tipo 906
7. Datos auten. 907
8. Datos de sesión aprobados 908
101
Entrar
Aprobado

Figura 9

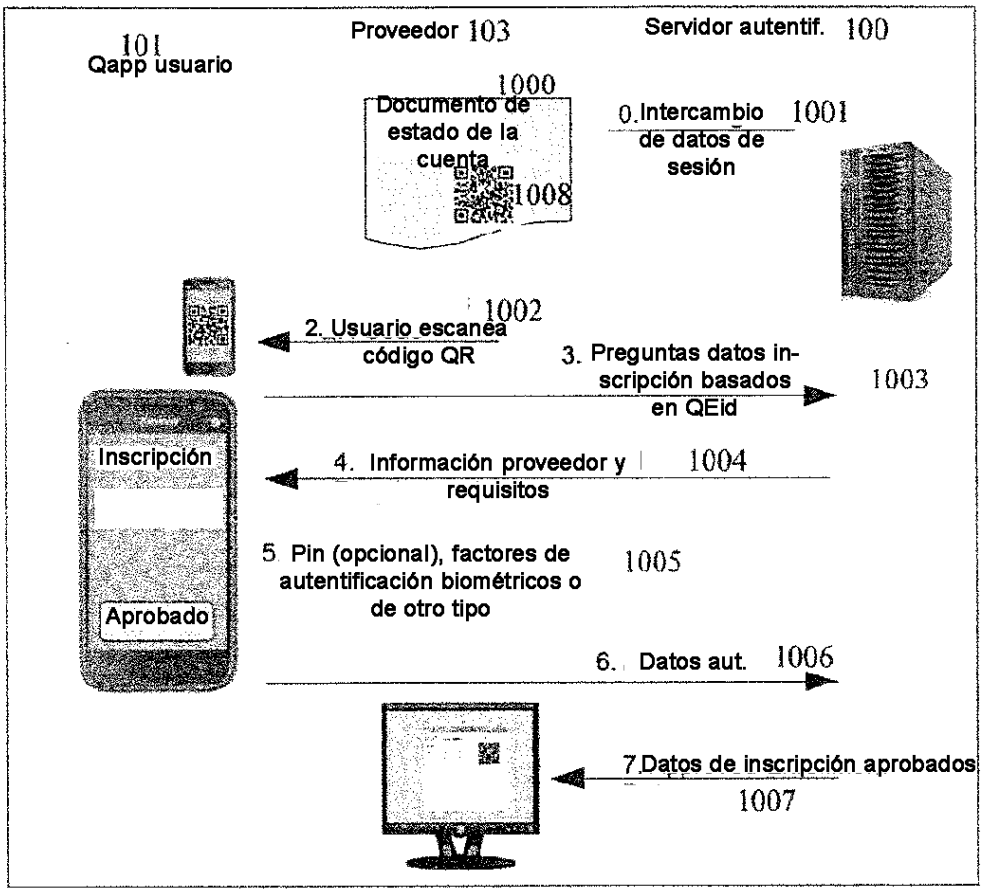
101
Qapp usuario
Proveedor 103
Servidor autentif. 100
1000
Documento de estado de la cuenta
1008
0.Intercambio de datos de sesión
1001
1002
2. Usuario escanea código QR
3. Preguntas datos inscripción basados en QEid
1003
Inscripción
4. Información proveedor y requisitos
1004
5 Pin (opcional), factores de autentificación biométricos o de otro tipo
1005
Aprobado
6. Datos aut.
1006
7.Datos de inscripción aprobados
1007

Figura 10

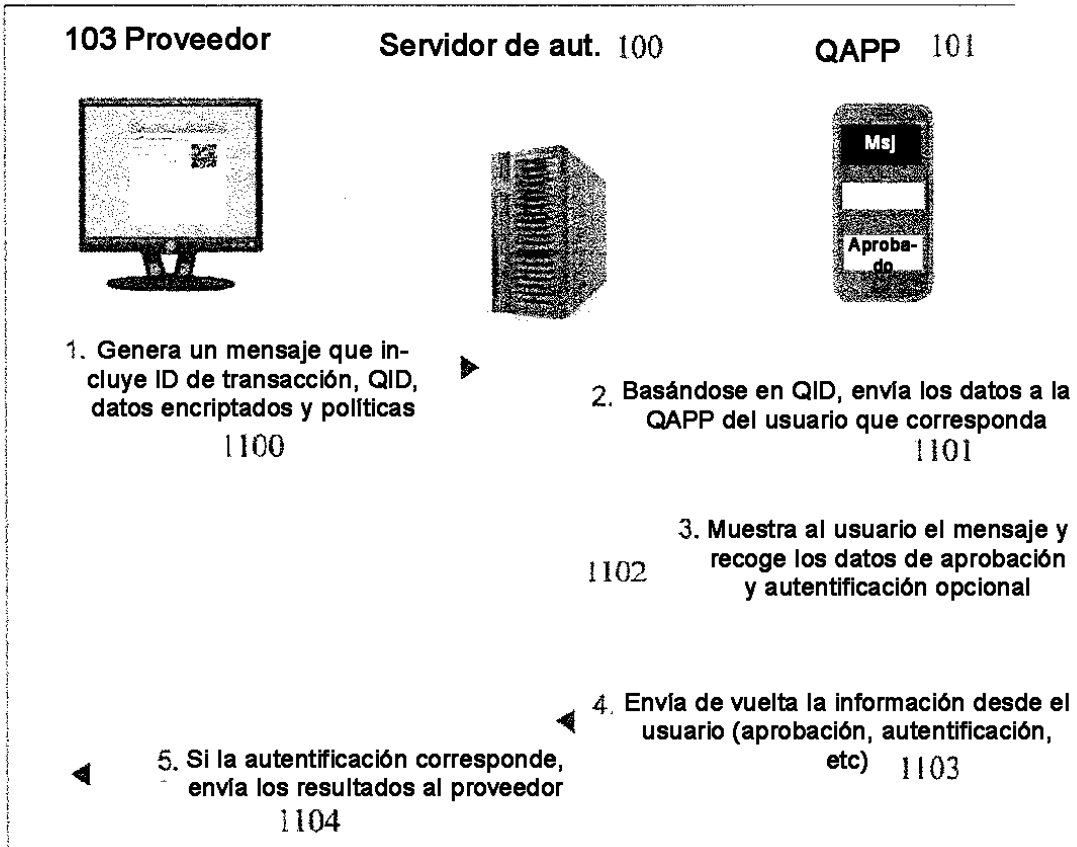
103 Proveedor
Servidor de aut. 100
QAPP 101
Msj
Aproba-
do
1. Genera un mensaje que incluye ID de transacción, QID, datos encriptados y políticas
1100
2. Basándose en QID, envía los datos a la QAPP del usuario que corresponda
1101
3. Muestra al usuario el mensaje y recoge los datos de aprobación y autentificación opcional
1102
4. Envía de vuelta la información desde el usuario (aprobación, autentificación, etc) 1103
5. Si la autentificación corresponde, envía los resultados al proveedor
1104

Figura 11