(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 549 104**

(51) Int. CI.:

G06F 7/04 (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 13771788 (0)**

(97) Fecha y número de publicación de la solicitud europea: **11.02.2015 EP 2834729**

(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:
23.10.2015

(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 multi-parte**

ES 2 549 104 T1

REIVINDICACIONES

1. Método de autentificación de un usuario de red a otra entidad de red, que comprende:

ejecutar, en un primer dispositivo operado por el usuario, un primer programa para:
recibir información de validación introducida por el usuario;
archivar una credencial de usuario en el primer dispositivo operado por el usuario;
ejecutar, en un segundo dispositivo operado por el usuario, un segundo programa para:
recibir información de otra entidad de red a través de la red;
ejecutar además el primer programa para:
recibir una entrada que transfiera, al primer programa, la información recibida por el segundo programa desde la otra entidad de red;
ordenar la transmisión, al servidor de autentificación a través de la red, de la información transferida;
recibir, del servidor de autentificación a través de la red, un identificador de la otra entidad de red, otras informaciones, y requisitos de política de autentificación de la otra entidad de red;
ordenar la transmisión, al servidor de autentificación a través de la red, de la información de validación de entrada que corresponde con los requisitos de política de autentificación de la otra entidad de red recibidos;
recibir, del servidor de autentificación a través de la red después de ordenar la transmisión de la información de validación, una solicitud de una credencial de usuario;
firmar un mensaje, que incluye la información transferida y las otras informaciones recibidas, con la credencial de usuario almacenada; y
ordenar la transmisión, al servidor de autentificación a través de la red, del mensaje firmado para autentificar el usuario; y
ejecutar además el segundo programa para:
recibir, de al menos un del servidor de autentificación y de la otra entidad de red a través de la red, una indicación de que el usuario se ha autentificado correctamente.

2. Método según la reivindicación 1, donde:

el primer dispositivo operado por el usuario y el segundo dispositivo operado por el usuario son el mismo dispositivo;
la información es un número aleatorio que sirve como identificador de sesión; y
la otra información es otro número aleatorio.

3. Método según la reivindicación 1, que comprende además ejecutar además el primer programa para:

generar un par de claves privada/pública para el usuario, donde la credencial de usuario almacenada es la clave privada del par de claves de usuario privada/pública generadas; y
ordenar la transmisión, al servidor de autentificación a través de la red, de la clave pública del par de claves de usuario privada/pública generadas.

4. Método según la reivindicación 1, que comprende además ejecutar además el primer programa para:

generar datos secretos de usuario;
dividir los datos secretos generados en partes múltiples que incluyen una primera parte y una segunda parte;
cifrar la credencial de usuario con los datos secretos generados, donde la credencial almacenada es la credencial cifrada;
ordenar la transmisión, al servidor de autentificación a través de la red, de la segunda parte de datos secretos;
recibir también, del servidor de autentificación a través de la red después de ordenar la transmisión de la información de validación, la segunda parte de datos secretos;
combinar la primera parte de datos secretos almacenada con la segunda parte de datos secretos recibida; y descifrar la credencial cifrada almacenada con las partes combinadas de los datos secretos;
donde el mensaje se firma con la credencial de usuario descifrada.

5. Método según la reivindicación 1, que comprende además ejecutar además el primer programa para:

recibir los requisitos de política de autentificación de usuario introducidos por el usuario;
ordenar la transmisión de los requisitos de política de autentificación de usuario recibidos al servidor de autentificación;
recibir también del servidor de autentificación con los requisitos de política de autentificación de la otra entidad de red, cualquier requisito de política de autentificación adicional basado en cualquier diferencia entre los requisitos de política de autentificación del usuario y los requisitos de política de autentificación de

la otra entidad de red; y
ordenar también la transmisión, al servidor de autentificación a través de la red, de la información de validación recibida que corresponde con cualquier requisito de política de autentificación adicional recibido.

6. Método según la reivindicación 1, donde la información es la primera información y la otra información es la otra primera información y, además, que comprende, después de que el servidor de autentificación ha recibido la notificación de que el primer dispositivo operado por el usuario ya no está en uso o se ha perdido o ha sido robado o la credencial de usuario se ha visto en peligro de cualquier otro modo:

ejecutar además el segundo programa para:
recibir, de la otra entidad de red a través de la red, la segunda información;
ejecutar, en el primer o en un tercer dispositivo operado por el usuario, el primer programa para:
recibir una entrada que transfiere, al primer programa, la segunda información recibida por el segundo programa de la otra entidad de red;
ordenar la transmisión, al servidor de autentificación a través de la red, de la segunda información transferida;
recibir, del servidor de autentificación a través de la red, un identificador de la otra entidad de red, la otra segunda información, y los requisitos de política de autentificación de la otra entidad de red;
ordenar la transmisión, al servidor de autentificación a través de la red, de la información de validación de entrada que corresponde con los requisitos de política de autentificación de la otra entidad de red recibidos; y
recibir, del servidor de autentificación a través de la red en respuesta a la información de validación transmitida, una notificación de que el usuario ha sido validado pero no se puede autentificar debido a que la credencial de usuario ha sido invalidada.

7. Método según la reivindicación 6, que comprende además ejecutar además el segundo programa para recibir, del servidor de autentificación a través de la red, una instrucción de redirección, que redirige el usuario al sitio web de reinscripción de la otra entidad de red en la red.

8. Método según la reivindicación 6, que comprende además ejecutar además el primer programa para:

recibir una solicitud de credencial de sustitución del servidor de autentificación a través de la red; y
generar, en respuesta a la solicitud de credencial de sustitución recibida, una credencial de sustitución, almacenar la credencial de sustitución generada, y ordenar la transmisión de la credencial de sustitución generada al servidor de autentificación a través de la red.

9. Método según la reivindicación 6, que comprende además, después de ordenar la transmisión de la credencial de sustitución generada al servidor de autentificación, ejecutar además el primer programa para:

ordenar la transmisión, al servidor de autentificación a través de la red, de otro mensaje, con la segunda información y la otra segunda información, firmado con la credencial de sustitución para autentificar al usuario.

10. Método según la reivindicación 1, que comprende además ejecutar además el segundo programa para:

ordenar una presentación, en una pantalla, de la información recibida; donde la información recibida tiene la forma de un código óptico; y donde la entrada que transfiere la información recibida al primer programa es una fotografía digital del código óptico presentado.

11. Método según la reivindicación 1, que comprende además ejecutar además el segundo programa para:

ordenar la impresión de la información recibida;
donde la entrada que transfiere la información recibida al primer programa es una fotografía digital del código óptico impreso.

12. Artículo de producción para autentificar un usuario de red a otra entidad de red, que comprende:

medio de almacenamiento no transitorio; y
lógica almacenada en el medio de almacenamiento, donde la lógica almacenada se configura de modo que sea legible por un procesador y haga así que el procesador funcione para:
recibir información de validación introducida por el usuario;
almacenar una credencial de usuario;
recibir una entrada de información, donde la información la obtuvo el usuario a partir de otra entidad de red;
ordenar la transmisión, al servidor de autentificación a través de la red, de la información de entrada;
recibir, del servidor de autentificación a través de la red después de ordenar la transmisión de la información, un identificador de la otra entidad de red, otras Informaciones, y requisitos de política de

autentificación de la otra entidad de red;
ordenar la transmisión, al servidor de autentificación a través de la red, la información de validación de entrada que corresponde con los requisitos de política de autentificación de la otra entidad de red recibidos;
recibir, del servidor de autentificación a través de la red después de ordenar la transmisión de la información de validación, una solicitud de credencial de usuario;
firmar un mensaje, que incluye la información transferida obtenida de la otra entidad de red y la otra información recibida del servidor de autentificación, con la credencial de usuario almacenada; y
ordenar la transmisión, al servidor de autentificación a través de la red, del mensaje firmado para autentificar el usuario.

13. Artículo de producción según la reivindicación 12, donde la lógica almacenada está además configurada para que haga que el procesador funcione para:

generar un par de claves privada/pública para el usuario, donde la credencial de usuario almacenada es la clave privada del par de claves de usuario privada/pública generadas; y
ordenar la transmisión, al servidor de autentificación a través de la red, de la clave pública del par de claves privada/pública de usuario generadas.

14. Artículo de producción según la reivindicación 12, donde la lógica almacenada está además configurada para que haga que el procesador funcione para:

generar datos secretos de usuario;
dividir los datos secretos generados en partes múltiples que incluyen una primera parte y una segunda parte;
cifrar la credencial de usuario con los datos secretos, donde la credencial de usuario almacenada es la credencial cifrada;
ordenar la transmisión, al servidor de autentificación a través de la red, la segunda parte de datos secretos;
recibir también, del servidor de autentificación a través de la red después de ordenar la transmisión de la información de validación, la segunda parte de datos secretos;
combinar la primera parte de datos secretos con la segunda parte de datos secretos recibida; y
descifrar la credencial cifrada almacenada con las partes combinadas de datos secretos, donde el mensaje firmado se firma con la credencial de usuario descifrada.

15. Artículo de producción según la reivindicación 12, donde la lógica almacenada es posteriormente configurada para que haga funcionar el procesador para:

recibir los requisitos de política de autentificación de usuario introducidos por el usuario;
ordenar la transmisión de los requisitos de política de autentificación de usuario recibidos al servidor de autentificación a través de la red;
recibir, del servidor de autentificación a través de la red con los requisitos de política de autentificación de la otra entidad de red, cualquier requisito de política de autentificación adicional basado en cualquier diferencia entre los requisitos de política de autentificación de usuario y los requisitos de política de autentificación de la otra entidad de red; y
también ordenar la transmisión, al servidor de autentificación a través de la red, de la información de validación de entrada que corresponde con cualquier requisito de política de autentificación adicional recibido.

16. Artículo de producción según la reivindicación 12, donde la información es la primera información y la otra información es la otra primera información y, después de que el servidor de autentificación ha recibido la notificación de que la credencial de usuario se ha puesto en peligro, la lógica almacenada se configura posteriormente para hacer que el procesador funcione para:

recibir una segunda información de entrada, donde la segunda información la obtuvo el usuario de la otra entidad de red;
ordenar la transmisión, al servidor de autentificación a través de la red, de la segunda información de entrada;
recibir, del servidor de autentificación a través de la red después de ordenar la transmisión de la segunda información, un identificador de la otra entidad de red, la otra segunda información, y los requisitos de política de autentificación de la otra entidad de red;
ordenar la transmisión, al servidor de autentificación a través de la red, de información de validación de entrada que corresponde con los requisitos de política de autentificación de la otra entidad de red recibidos; y
recibir, del servidor de autentificación a través de la red después de ordenar la transmisión de la información de validación, una notificación de que el usuario ha sido validado pero no se puede autentificar debido a que la credencial de usuario ha sido invalidada.

17. Artículo de producción según la reivindicación 16, donde la lógica almacenada es posteriormente configurada para que haga que el procesador funcione para:

recibir una solicitud de una credencial de sustitución del servidor de autentificación a través de la red;
en respuesta a la solicitud de la credencial de sustitución recibida, generar una credencial de sustitución, almacenar la credencial de sustitución generada y ordenar la transmisión de la credencial de sustitución generada al servidor de autentificación a través de la red; y
ordenar la transmisión, al servidor de autentificación a través de la red, de otro mensaje, que incluye la segunda información de entrada de la otra entidad de red y la otra segunda información del servidor de autentificación, firmado con la credencial de sustitución para autentificar el usuario.

18. Método de operar un dispositivo de red de usuario para inscribir un usuario de red con otra entidad de red, que comprende:

recibir un conjunto de identidades de usuario introducidas por el usuario, datos de inscripción introducidos por el usuario y una selección del usuario de los datos de inscripción particulares introducidos que se deben asociar a cada identidad respectiva en el conjunto de identidades recibido;
almacenar cada identidad respectiva en asociación con los datos de inscripción particulares seleccionados para ser asociados a esa identidad;
recibir una entrada de información obtenida por el usuario de otra entidad de red en respuesta a una solicitud de inscripción;
transmitir la información de entrada al servidor de autentificación a través de la red;
recibir un identificador de la otra entidad de red y requisitos de datos de inscripción de la otra entidad de red del servidor de autentificación a través de la red;
recibir una entrada de usuario que selecciona una de las identidades de usuario almacenadas;
en respuesta a la recepción de la identidad seleccionada introducida, recuperar de forma automática los datos de inscripción particulares almacenados en asociación con la identidad de usuario seleccionada; y
transmitir los datos de inscripción recuperados al servidor de autentificación a través de la red para inscribir al usuario con la otra entidad de red.

19. Método según la reivindicación 18, que comprende además:

transmitir, al servidor de autentificación a través de la red, una credencial nueva para el uso con la otra entidad de red y una solicitud para que el servidor de autentificación firme el nuevo certificado transmitido con una clave privada de un par de claves privada/pública del servidor de autentificación para crear un certificado, donde la clave pública del par de claves privada/pública del servidor de autentificación es conocida por la otra entidad de red; y
recibir el certificado del servidor de autentificación a través de la red.

20. Método de operar un dispositivo de red de usuario para notificar a un usuario de una transacción con otra entidad de red a través de una red, que comprende:

recibir, de un servidor de autentificación a través de la red, un identificador de transacción, una aprobación de transacción y unos requisitos de autentificación, y un mensaje con respecto a la transacción, donde el mensaje está (i) cifrado con una clave pública de un par de claves privada/pública del usuario, donde una clave privada del par de claves privada/pública del usuario la conoce sólo el usuario, y (ii) también firmado con una clave privada de un par de claves privada/pública de la otra entidad de red, donde una clave pública del par de claves privada/pública de la otra entidad de red la conoce el usuario;
validar y cifrar el mensaje aplicando la clave pública del par de claves privada/pública de la otra entidad de red y la clave privada del par de claves privada/pública de usuario al mensaje cifrado firmado;
ordenar la presentación del mensaje descifrado validado al usuario;
recibir, basándose en la aprobación de la transacción y requisitos de autentificación recibidos, una entrada de usuario que representa una aprobación de transacción, o información de autentificación, o ambos; y
transmitir, al servidor de autentificación a través de la red basada en la entrada de usuario recibida, al menos una de entre una aprobación de transacción y una información de autentificación.

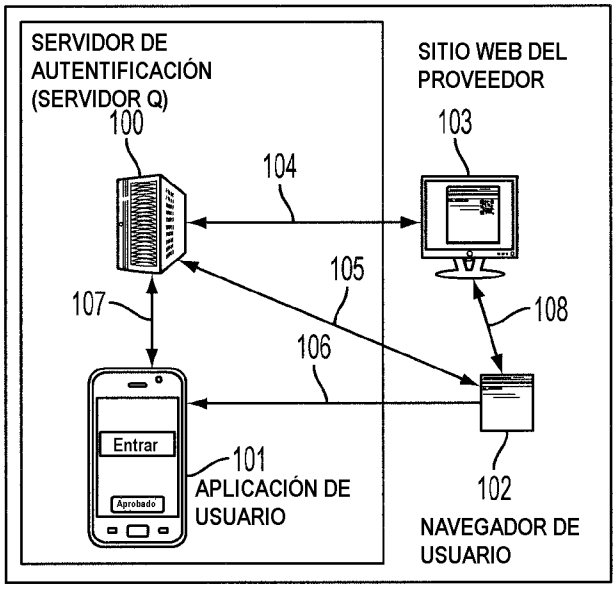
SERVIDOR DE AUTENTIFICACIÓN (SERVIDOR Q)
100
SITIO WEB DEL PROVEEDOR
103
104
105
106
107
108
Entrar
Aprobado
101
APLICACIÓN DE USUARIO
102
NAVEGADOR DE USUARIO

FIG. 1

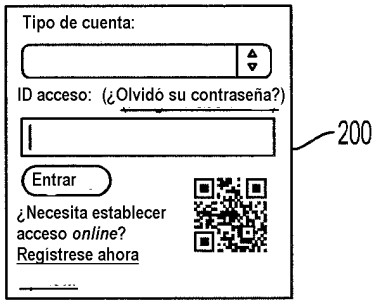
Tipo de cuenta:
ID acceso: (¿Olvidó su contraseña?)
200
Entrar
¿Necesita establecer acceso *online*?
Registrese ahora

FIG. 2

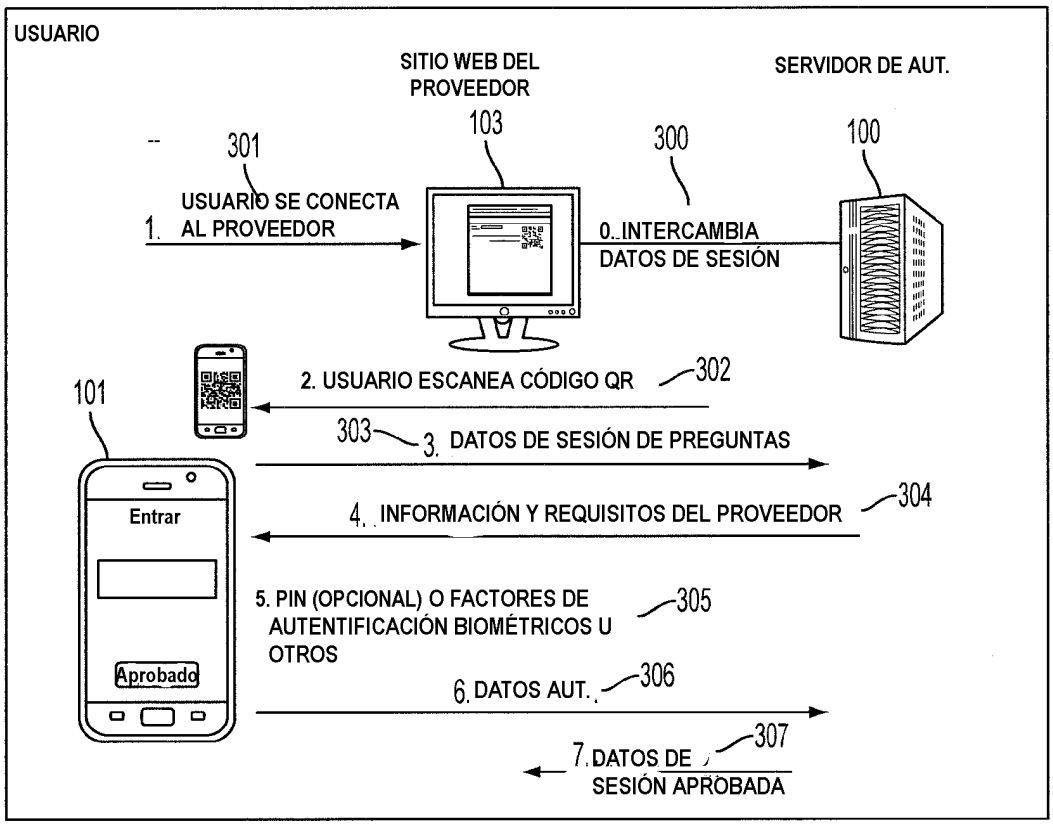
USUARIO
SITIO WEB DEL PROVEEDOR
SERVIDOR DE AUT.
103
300
100
301
USUARIO SE CONECTA
1. AL PROVEEDOR
0. INTERCAMBIA
DATOS DE SESIÓN
101
2. USUARIO ESCANEA CÓDIGO QR
302
303
3. DATOS DE SESIÓN DE PREGUNTAS
Entrar
4. INFORMACIÓN Y REQUISITOS DEL PROVEEDOR
304
5. PIN (OPCIONAL) O FACTORES DE AUTENTIFICACIÓN BIOMÉTRICOS U OTROS
305
Aprobado
6. DATOS AUT.
306
7. DATOS DE SESIÓN APROBADA
307

FIG. 3

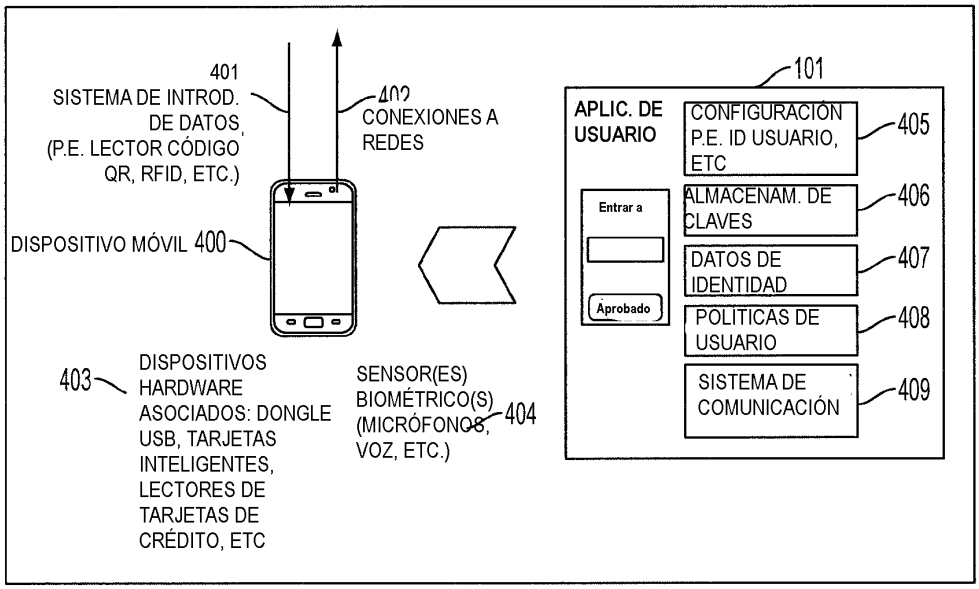
401
SISTEMA DE INTROD. DE DATOS, (P.E. LECTOR CÓDIGO QR, RFID, ETC.)
402
CONEXIONES A REDES
DISPOSITIVO MÓVIL 400
403
DISPOSITIVOS HARDWARE ASOCIADOS: DONGLE USB, TARJETAS INTELIGENTES, LECTORES DE TARJETAS DE CRÉDITO, ETC
SENSOR(ES) BIOMÉTRICO(S) (MICRÓFONOS, VOZ, ETC.)
404
101
APLIC. DE USUARIO
Entrar a
Aprobado
CONFIGURACIÓN P.E. ID USUARIO, ETC
405
ALMACENAM. DE CLAVES
406
DATOS DE IDENTIDAD
407
POLITICAS DE USUARIO
408
SISTEMA DE COMUNICACIÓN
409

FIG. 4

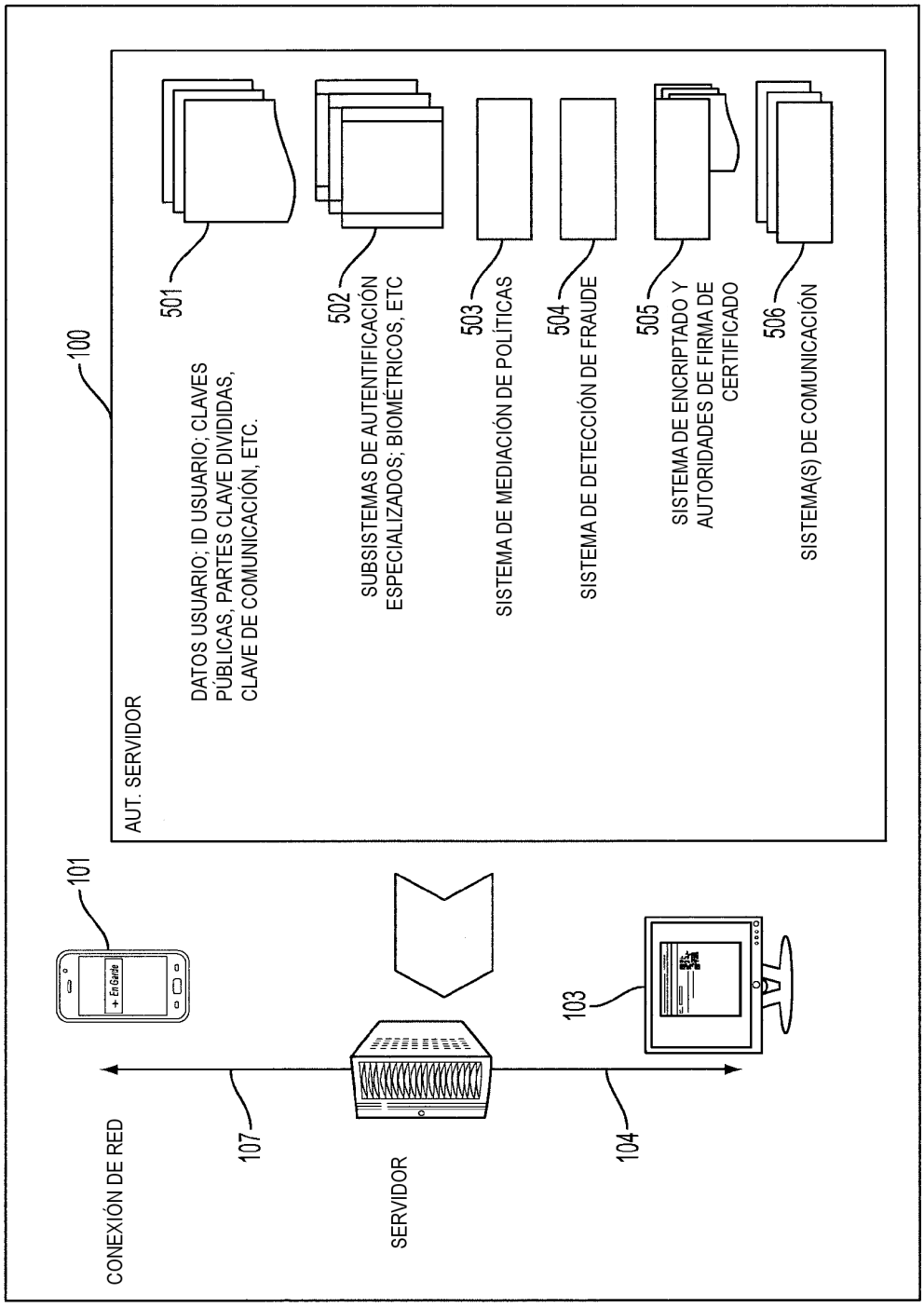
100
AUT. SERVIDOR
501
DATOS USUARIO; ID USUARIO; CLAVES PÚBLICAS, PARTES CLAVE DIVIDIDAS, CLAVE DE COMUNICACIÓN, ETC.
502
SUBSISTEMAS DE AUTENTIFICACIÓN ESPECIALIZADOS; BIOMÉTRICOS, ETC
503
SISTEMA DE MEDIACIÓN DE POLÍTICAS
504
SISTEMA DE DETECCIÓN DE FRAUDE
505
SISTEMA DE ENCRIPTADO Y AUTORIDADES DE FIRMA DE CERTIFICADO
506
SISTEMA(S) DE COMUNICACIÓN
101
103
107
104
SERVIDOR
CONEXIÓN DE RED

FIG. 5

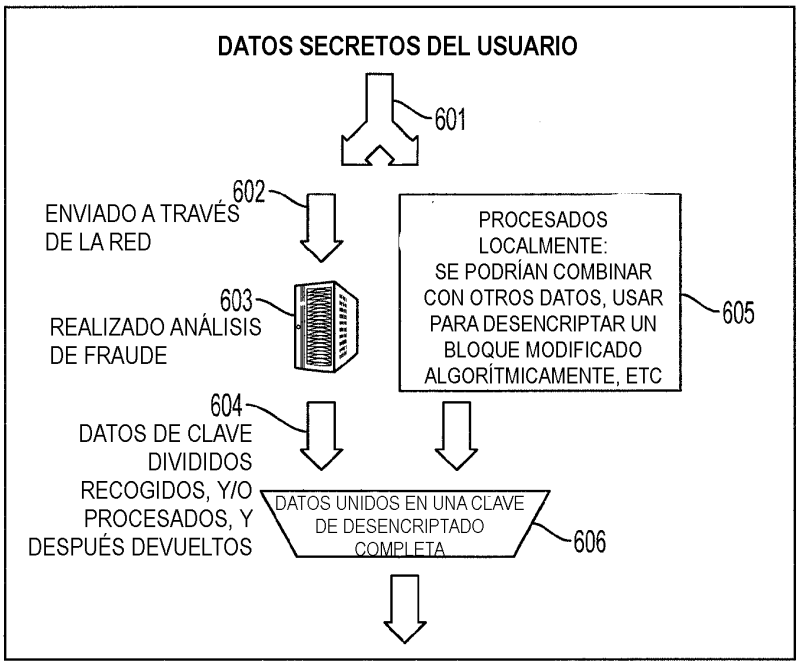
DATOS SECRETOS DEL USUARIO
601
602
ENVIADO A TRAVÉS DE LA RED
603
REALIZADO ANÁLISIS DE FRAUDE
PROCESADOS LOCALMENTE: SE PODRÍAN COMBINAR CON OTROS DATOS, USAR PARA DESENCRIPTAR UN BLOQUE MODIFICADO ALGORÍTMICAMENTE, ETC
605
604
DATOS DE CLAVE DIVIDIDOS RECOGIDOS, Y/O PROCESADOS, Y DESPUÉS DEVUELTOS
DATOS UNIDOS EN UNA CLAVE DE DESENCRIPTADO COMPLETA
606

FIG. 6

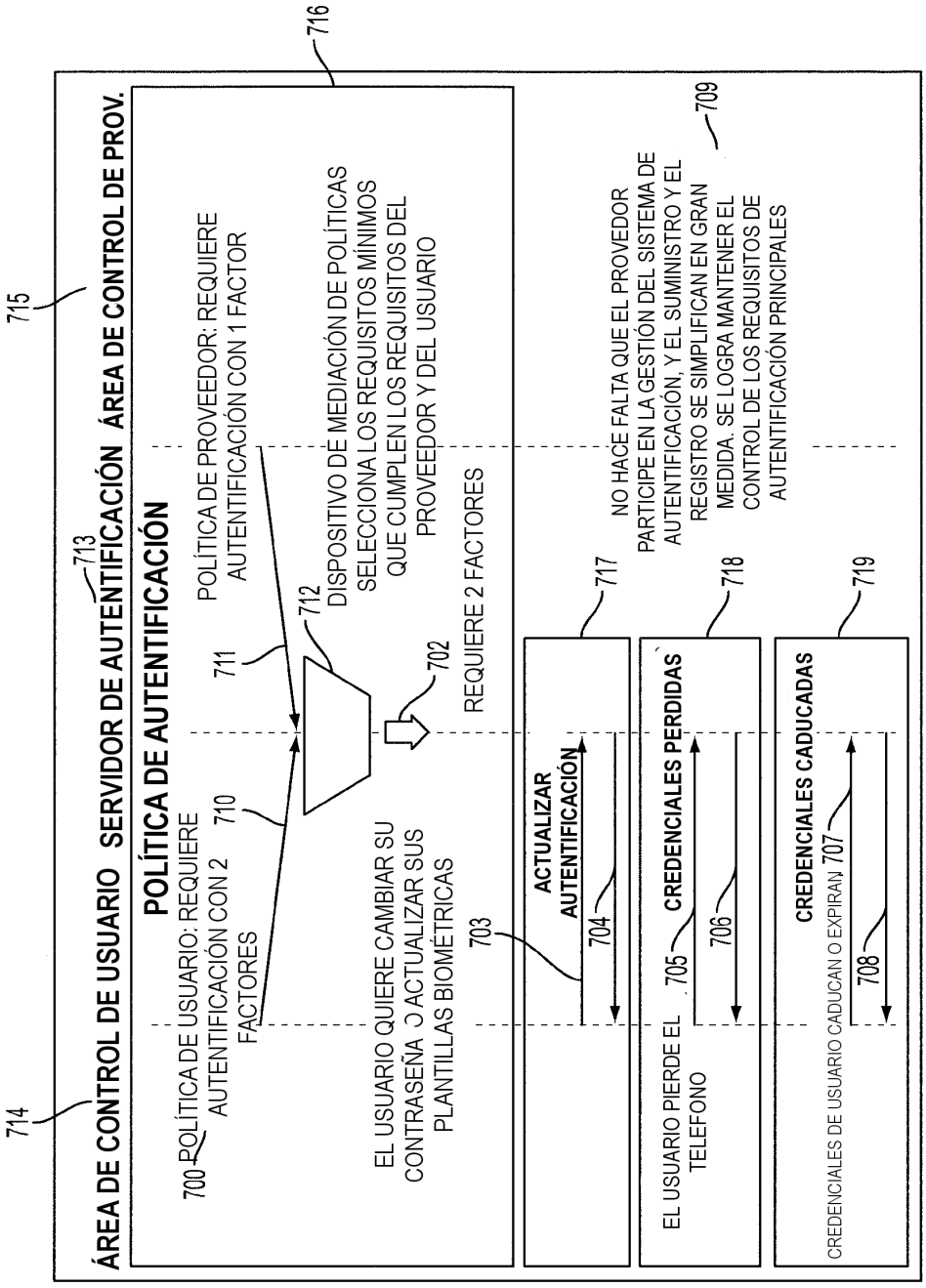
ÁREA DE CONTROL DE USUARIO SERVIDOR DE AUTENTIFICACIÓN ÁREA DE CONTROL DE PROV.
POLÍTICA DE AUTENTIFICACIÓN
POLÍTICA DE USUARIO: REQUIERE AUTENTIFICACIÓN CON 2 FACTORES
POLÍTICA DE PROVEEDOR: REQUIERE AUTENTIFICACIÓN CON 1 FACTOR
DISPOSITIVO DE MEDIACIÓN DE POLÍTICAS SELECCIONA LOS REQUISITOS MÍNIMOS QUE CUMPLEN LOS REQUISITOS DEL PROVEEDOR Y DEL USUARIO
REQUIERE 2 FACTORES
EL USUARIO QUIERE CAMBIAR SU CONTRASEÑA O ACTUALIZAR SUS PLANTILLAS BIOMÉTRICAS
ACTUALIZAR AUTENTIFICACIÓN
NO HACE FALTA QUE EL PROVEDOR 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
EL USUARIO PIERDE EL TELEFONO
CREDENCIALES PERDIDAS
CREDENCIALES DE USUARIO CADUCAN O EXPIRAN
CREDENCIALES CADUCADAS
700
710
711
712
702
703
704
705
706
707
708
709
713
714
715
716
717
718
719

FIG. 7

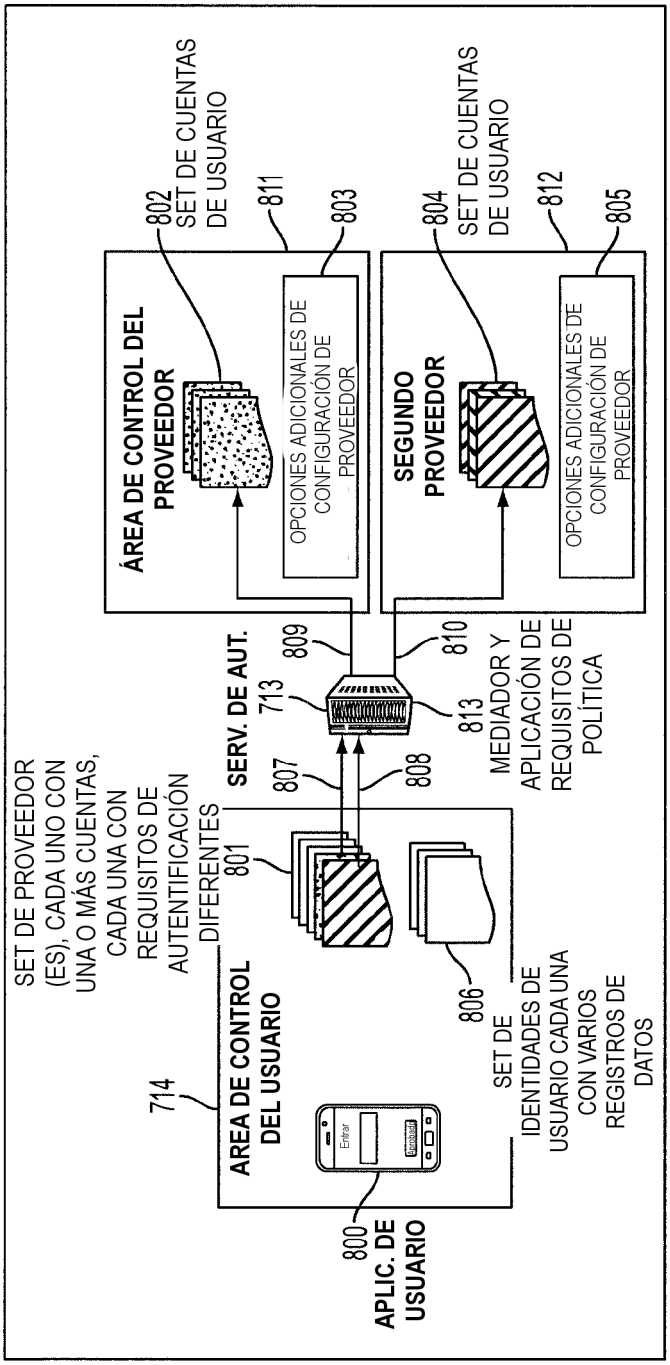
SET DE PROVEEDOR (ES), CADA UNO CON UNA O MÁS CUENTAS, CADA UNA CON REQUISITOS DE AUTENTIFICACIÓN DIFERENTES
ÁREA DE CONTROL DEL PROVEEDOR
802
SET DE CUENTAS DE USUARIO
811
803
OPCIONES ADICIONALES DE CONFIGURACIÓN DE PROVEEDOR
SEGUNDO PROVEEDOR
804
SET DE CUENTAS DE USUARIO
812
805
OPCIONES ADICIONALES DE CONFIGURACIÓN DE PROVEEDOR
SERV. DE AUT.
713
809
810
813
MEDIADOR Y APLICACIÓN DE REQUISITOS DE POLÍTICA
807
808
AREA DE CONTROL DEL USUARIO
714
801
806
SET DE IDENTIDADES DE USUARIO CADA UNA CON VARIOS REGISTROS DE DATOS
800
APLIC. DE USUARIO

FIG. 8

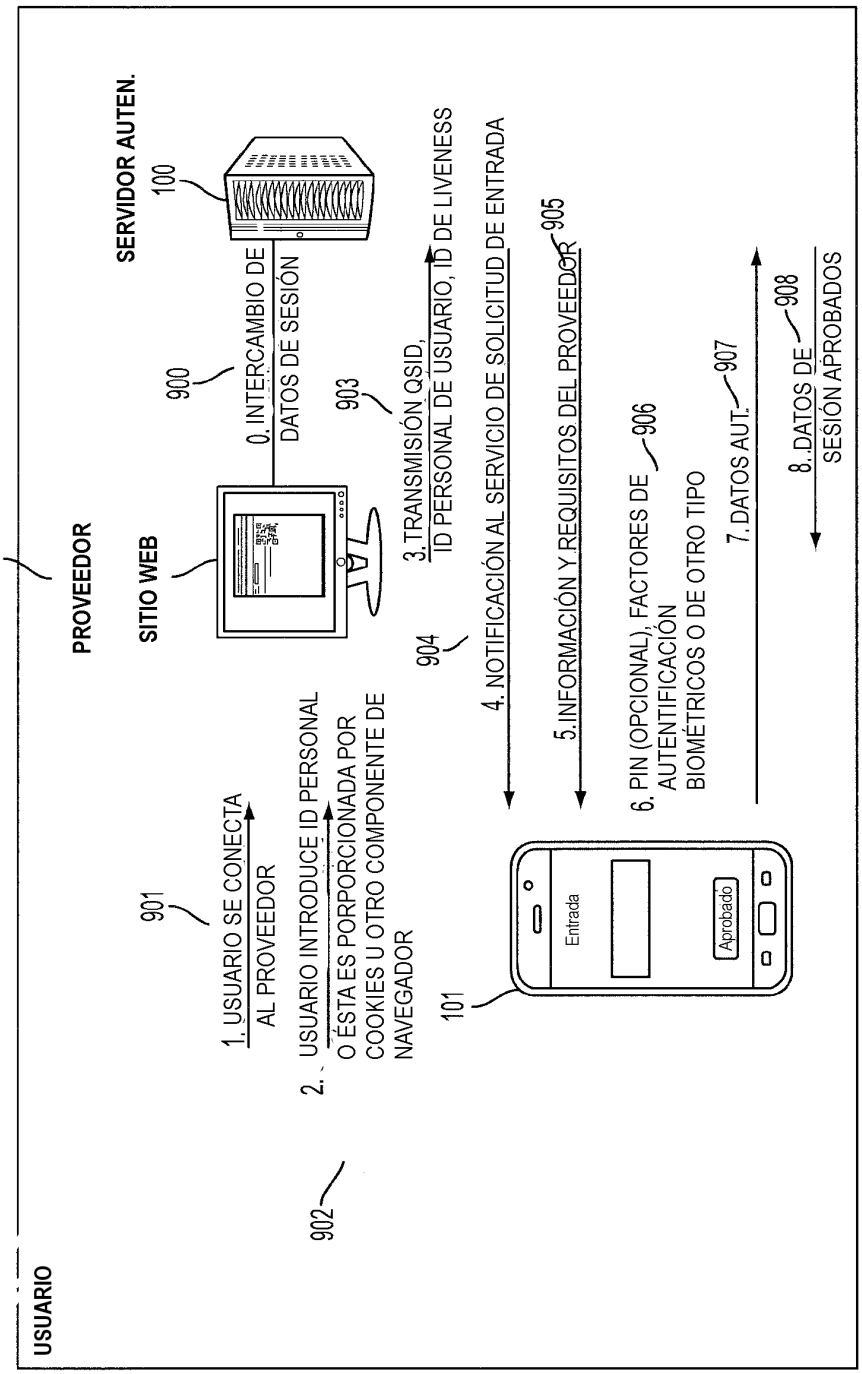
USUARIO
103
PROVEEDOR
SITIO WEB
SERVIDOR AUTEN.
100
900
0. INTERCAMBIO DE DATOS DE SESIÓN
903
3. TRANSMISIÓN QSID, ID PERSONAL DE USUARIO, ID DE LIVENESS
904
4. NOTIFICACIÓN AL SERVICIO DE SOLICITUD DE ENTRADA
905
5.INFORMACIÓN Y REQUISITOS DEL PROVEEDOR
906
6. PIN (OPCIONAL), FACTORES DE AUTENTIFICACIÓN BIOMÉTRICOS O DE OTRO TIPO
907
7. DATOS AUT.
908
8. DATOS DE SESIÓN APROBADOS
901
1. USUARIO SE CONECTA AL PROVEEDOR
902
2. USUARIO INTRODUCE ID PERSONAL O ÉSTA ES PORPORCIONADA POR COOKIES U OTRO COMPONENTE DE NAVEGADOR
101
Entrada
Aprobado

FIG. 9

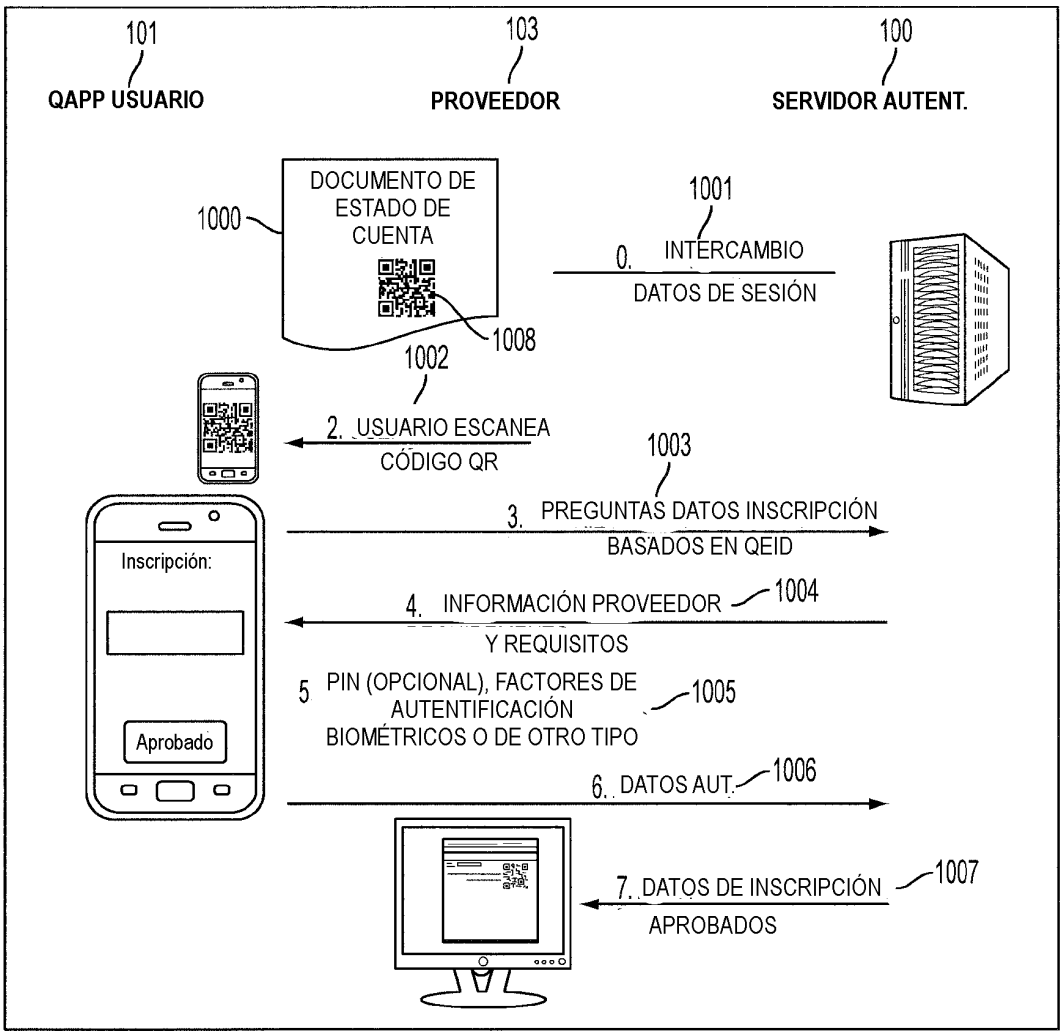
101
QAPP USUARIO
103
PROVEEDOR
100
SERVIDOR AUTENT.
1000
DOCUMENTO DE ESTADO DE CUENTA
1008
1001
0. INTERCAMBIO DATOS DE SESIÓN
1002
2. USUARIO ESCANEA CÓDIGO QR
1003
3. PREGUNTAS DATOS INSCRIPCIÓN BASADOS EN QEID
Inscripción:
Aprobado
4. INFORMACIÓN PROVEEDOR Y REQUISITOS
1004
5 PIN (OPCIONAL), FACTORES DE AUTENTIFICACIÓN BIOMÉTRICOS O DE OTRO TIPO
1005
6. DATOS AUT.
1006
7. DATOS DE INSCRIPCIÓN APROBADOS
1007

FIG. 10

--

-

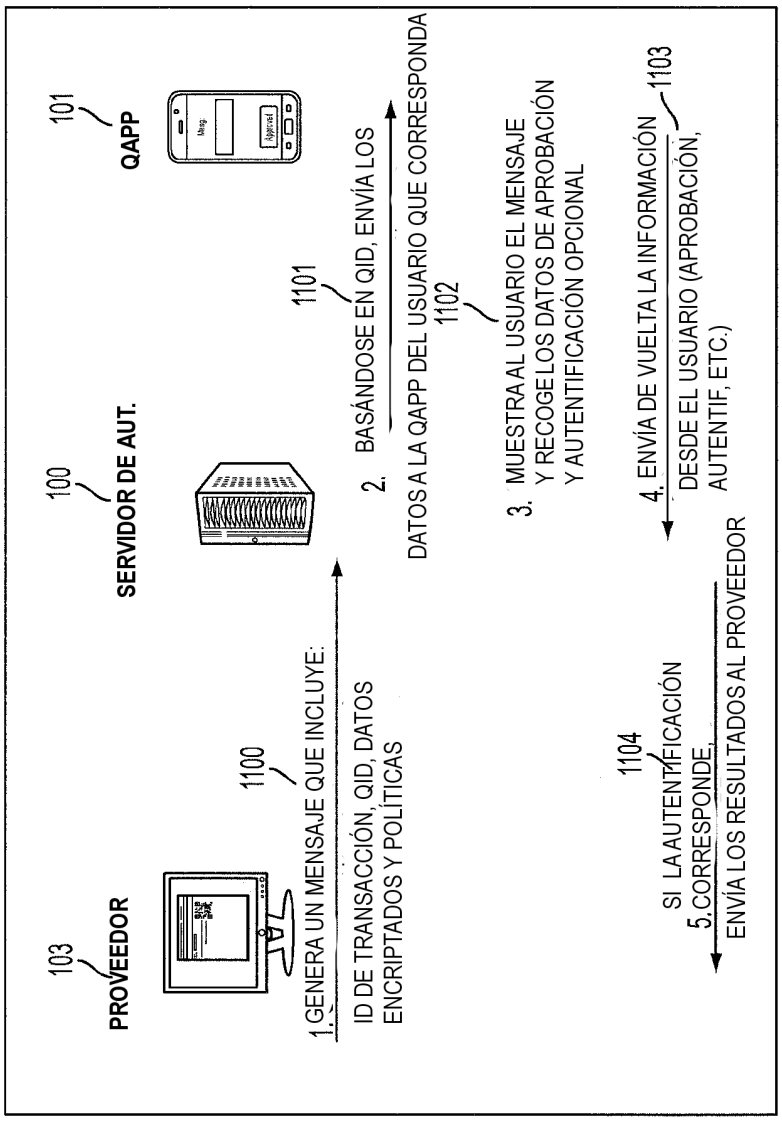
103
PROVEEDOR
100
SERVIDOR DE AUT.
101
QAPP
1100
1101
1102
1103
1104
1. GENERA UN MENSAJE QUE INCLUYE:
ID DE TRANSACCIÓN, QID, DATOS ENCRIPTADOS Y POLÍTICAS
2. BASÁNDOSE EN QID, ENVÍA LOS DATOS A LA QAPP DEL USUARIO QUE CORRESPONDA
3. MUESTRA AL USUARIO EL MENSAJE Y RECOGE LOS DATOS DE APROBACIÓN Y AUTENTIFICACIÓN OPCIONAL
4. ENVÍA DE VUELTA LA INFORMACIÓN DESDE EL USUARIO (APROBACIÓN, AUTENTIF, ETC.)
SI LA AUTENTIFICACIÓN 5. CORRESPONDE, ENVÍA LOS RESULTADOS AL PROVEEDOR

FIG. 11