(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 553 220**

(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 13771854 (0)**

(97) Fecha y número de publicación de la solicitud europea: **11.02.2015 EP 2834730**

(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:
07.12.2015

(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 de múltiples partes**

ES 2 553 220 T1

REIVINDICACIONES

1. Método para operar un servidor de autentificación capaz de autentificar cualquiera de varios usuarios diferentes para varios proveedores de servicio a través de una red, que comprende:

almacenar información de validación para el primer usuario;

almacenar requisitos de política de autentificación de un primero de los varios proveedores de servicio, en asociación con un identificador del primer proveedor;

transmitir un primer número aleatorio al primer proveedor a través de la red;

recibir, desde el primer proveedor a través de la red, otra primera información;

recibir, de un usuario solicitante a través de la red, el primer número aleatorio y una solicitud de este usuario de ser autentificado;

transmitir, después de recibir el primer número aleatorio y la solicitud de autentificación, el primer identificador de proveedor almacenado, la otra primera información recibida, y los requisitos de política de autentificación del primer proveedor almacenados, al usuario solicitante a través de la red;

recibir, en respuesta a los requisitos de política de autentificación del primer proveedor transmitidos, un identificador de usuario e información de validación, del usuario solicitante a través de la red;

emparejar el identificador de usuario solicitante recibido con el primer identificador de usuario almacenado;

determinar que la información de validación recibida del usuario solicitante corresponde a los requisitos de política de autentificación del primer proveedor almacenados;

comparar la información de validación recibida del usuario solicitante con la información de validación del primer usuario almacenada para autentificar que el usuario solicitante es el primer usuario;

recibir del usuario solicitante a través de la red un mensaje con el primer número aleatorio y la primera otra información, firmada con una credencial; y

transmitir, al primer proveedor a través de la red, aviso de autentificación del primer usuario y el mensaje firmado recibido.

2. Método según la reivindicación 1, donde:

la credencial es una credencial del primer usuario asociada sólo con el primer proveedor y no con otros de los varios proveedores de servicio;

el primer número aleatorio es un identificador de sesión; y

la otra información primera es un segundo número aleatorio.

3. Método según la reivindicación 1, que comprende además:

recibir, desde el primer usuario a través de la red, una credencial del primer usuario;

almacenar la credencial de primer usuario recibida; y

verificar el primer número aleatorio y la otra información primera aplicando la credencial de primer usuario almacenada con el mensaje firmado recibido para autentificar adicionalmente al usuario solicitante como el primer usuario.

4. Método según la reivindicación 3, donde la primera credencial de usuario recibida es una clave pública de un par de claves privada/pública del primer usuario, una clave privada del primer par de claves privada/pública de usuario la conoce sólo el primer usuario, y el mensaje firmado recibido se firma con la clave privada, y que además comprende:

transmitir con el aviso de autentificación y el mensaje firmado recibido, un certificado que incluye la primera clave pública de usuario y se firma con una clave privada de un par de claves privada/pública del servidor de autentificación.

5. Método según la reivindicación 1, que comprende además:

recibir un aviso de que la primera credencial de usuario ha sido comprometida;

invalidar la credencial de primer usuario almacenada en respuesta al aviso recibido;

después de invalidar la credencial de primer usuario almacenada, transmitir un segundo número aleatorio al primer proveedor a través de la red;

recibir, desde el primer proveedor a través de la red, otras segundas informaciones;

recibir, de un usuario solicitante a través de la red, el segundo número aleatorio y una solicitud de este usuario para ser autentificado;

nuevamente transmitir, después de la recepción del segundo número aleatorio y de esta solicitud de autentificación, el identificador de primer proveedor almacenado, la otra segunda información recibida, y los primeros requisitos de política de autentificación del proveedor almacenados, para este usuario solicitante a través de la red;

recibir, en respuesta a los primeros requisitos de política de autentificación del proveedor nuevamente transmitidos, otro identificador de usuario y otra información de validación de este usuario solicitante a través de la red;

emparejar el otro identificador de usuario recibido con el primer identificador de usuario almacenado;

determinar que la otra información de validación recibida corresponde a los primeros requisitos de política de autentificación del proveedor almacenados;

comparar la otra información de validación recibida con la información de validación del primer usuario almacenado para autentificar que este usuario solicitante es el primer usuario; y

determinar que la credencial de primer usuario almacenado es inválida.

6. Método según la reivindicación 5, que comprende además:
después de determinar que la credencial del primer usuario almacenado es inválida, transmitir, al primer proveedor a través de la red, aviso de autentificación de que el usuario solicitante es el primer usuario y de la incapacidad para autentificar adicionalmente al primer usuario debido a la invalidez de la primera credencial de usuario.

7. Método según la reivindicación 5, que comprende además:
después de determinar que la credencial del primer usuario almacenada es inválida, transmitir una solicitud de una credencial de sustitución al usuario solicitante a través de la red;
recibir, en respuesta a la solicitud transmitida para la credencial de sustitución, una credencial de sustitución del usuario solicitante a través de la red;
almacenar la credencial de sustitución recibida en asociación con el primer identificador de usuario;
generar un certificado para la credencial de sustitución recibida; y
transmitir al primer usuario a través de la red el certificado generado para el uso en la reinscripción del primer usuario con el primer proveedor.

8. Método según la reivindicación 7, que comprende además:
después de recibir la credencial de sustitución, recibir, del usuario solicitante a través de la red, otro mensaje, con el segundo número aleatorio y las otras segundas informaciones, firmado con una credencial del usuario solicitante;
verificar el segundo número aleatorio y las otras segundas informaciones aplicando la credencial de sustitución de primer usuario almacenada al otro mensaje firmado recibido para autentificar adicionalmente que el usuario solicitante es el primer usuario; y
transmitir, al primer proveedor a través de la red, aviso de autentificación del primer usuario y el otro mensaje firmado.

9. Método según la reivindicación 1, que comprende además:
recibir, del primer usuario a través de la red, otra credencial del primer usuario;
almacenar la otra credencial de primer usuario recibida, y la primera información de validación de usuario, en asociación con otro identificador para el primer usuario;
almacenar los requisitos de política de autentificación de un segundo de varios proveedores de servicio, en asociación con un identificador del segundo proveedor;
transmitir un segundo número aleatorio al segundo proveedor a través de la red;
recibir, del segundo proveedor a través de la red, segunda otra información;
recibir, de un usuario solicitante a través de la red, el segundo número aleatorio y una solicitud de este usuario para ser autentificado;
transmitir, después de la recepción del segundo número aleatorio y esta solicitud de autentificación, el segundo identificador de proveedor almacenado, la otra segunda información recibida, y los requisitos de política de autentificación del segundo proveedor almacenados, a este usuario solicitante a través de la red;
recibir, en respuesta a los requisitos de política de autentificación del segundo proveedor transmitidos, otro identificador de usuario y otra información de validación;
emparejar el otro identificador de usuario recibido con el otro identificador del primer usuario almacenado;
determinar que la otra información de validación recibida de este usuario solicitante se corresponde con los requisitos de política de autentificación del segundo proveedor almacenados;
comparar la otra información de validación recibida con la información de validación del primer usuario almacenada para autentificar que este usuario solicitante es el primer usuario;
recibir, de este usuario solicitante a través de la red, otro mensaje, con el segundo número aleatorio y las otras segundas informaciones, firmado con otra credencial; y
transmitir, al segundo proveedor a través de la red, aviso de autentificación del primer usuario y el otro mensaje firmado recibido.

10. Método según la reivindicación 1, que comprende además:
recibir, desde el primer usuario a través de la red, requisitos de política de autentificación del primer usuario;
almacenar los requisitos de política de autentificación del primer usuario recibidos;
comparar los requisitos de política de autentificación del primer proveedor almacenados con los requisitos de política de autentificación del primer usuario almacenados;
determinar cualquiera de los requisitos de política de autentificación adicional basados en la comparación;
transmitir cualquiera de los requisitos de política de autentificación adicional determinada al usuario solicitante a través de la red; y
también determinar que la información de validación recibida del usuario solicitante corresponde a cualquier requisito de política de autentificación adicional determinado.

11. Método según la reivindicación 1, que comprende además:

recibir, del primer usuario a través de la red, una primera de varias porciones de datos secretos del primer usuario;
almacenar la primera porción recibida de datos secretos; y
después de autentificar que el usuario solicitante es el primer usuario, transmitir la primera porción de datos secretos almacenados al primer usuario a través de la red;
donde el mensaje firmado se recibe después de la transmisión de la primera porción de datos secretos.

12. Artículo de producción para la autentificación de cualquiera de varios usuarios diferentes a cualquiera de varios proveedores de servicios diferente a través de una red, que comprende:
medio de almacenamiento no transitorio; y
lógica almacenada en el medio de almacenamiento, donde la lógica almacenada se configura para ser legible por un procesador y así hacer que el procesador funcione para:
transmitir un primer número aleatorio a un primero de los varios proveedores a través de la red;
recibir, desde el primer proveedor a través de la red, una primera información;
recibir, de un usuario solicitante a través de la red, el primer número aleatorio y una solicitud de este usuario para ser autentificado;
transmitir, después de recibir el primer número aleatorio y la solicitud de autentificación, un primer identificador de proveedor, la otra primera información recibida, y los primeros requisitos de política de autentificación del proveedor, al usuario solicitante a través de la red;
recibir, en respuesta a los primeros requisitos de política de autentificación del proveedor transmitidos, un identificador de usuario e información de validación del usuario solicitante a través de la red;
determinar que la información de validación recibida corresponde a los requisitos de política de autentificación del primer proveedor;
comparar, basándose en el identificador de usuario recibido, la información de validación recibida con la información de validación almacenada de un primero de los varios usuarios para autentificar que el usuario solicitante es el primer usuario;
recibir, del usuario solicitante a través de la red, un mensaje, con el primer número aleatorio y la primera otra información, firmado con una credencial; y
transmitir, al primer proveedor a través de la red, aviso de autentificación del primer usuario y el mensaje recibido firmado.

13. Artículo de producción según la reivindicación 12, donde la lógica almacenada es posteriormente configurada para obligar al procesador a operar para:
verificar el primer número aleatorio y la primera otra información aplicando, basándose en el identificador de usuario recibido, una credencial almacenada del primer usuario al mensaje recibido firmado para autentificar adicionalmente el usuario solicitante como el primer usuario.

14. Artículo de producción según la reivindicación 13, 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 primer par de claves privada/pública de usuario la conoce sólo el primer usuario, y el mensaje recibido firmado se firma con la clave privada; y
la lógica almacenada es posteriormente configurada para obligar al procesador a operar para transmitir, con el aviso de autentificación y el mensaje recibido firmado, un certificado que incluye la primera clave pública de usuario y se firma con una clave privada de un par de claves privada/pública del servidor de autentificación.

15. Artículo de producción según la reivindicación 12, donde la lógica almacenada es posteriormente configurada para obligar al procesador a operar para:
recibir un aviso de que la primera credencial de usuario ha sido comprometida;
transmitir un segundo número aleatorio al primer proveedor a través de la red;
recibir, desde el primer proveedor a través de la red, otra segunda información;
después de la recepción del aviso, recibir, de un usuario solicitante a través de la red, el segundo número aleatorio y una solicitud de este usuario solicitante de ser autentificado;
transmitir nuevamente, después de la recepción del segundo número aleatorio y la solicitud de autentificación, el primer identificador de proveedor, la otra segunda información recibida, y los requisitos de política de autentificación del primer proveedor, a este usuario solicitante a través de la red;
recibir, en respuesta a los requisitos de política de autentificación del primer proveedor nuevamente transmitidos, otro identificador de usuario y otra información de validación de este usuario solicitante a través de la red;
determinar que la otra información de validación recibida corresponde a los requisitos de política de autentificación del primer proveedor;
comparar la otra información de validación recibida con la información de validación del primer usuario almacenada para autentificar que este usuario solicitante es el primer usuario; y
transmitir, al primer proveedor a través de la red, aviso de autentificación del primer usuario y que la credencial del primer usuario es inválida.

16. Artículo de producción según la reivindicación 15, donde la lógica almacenada es posteriormente configurada para obligar al procesador a operar para:

transmitir una solicitud para una credencial de sustitución a este usuario solicitante a través de la red;

recibir, en respuesta a la solicitud transmitida para la credencial de sustitución, una credencial de sustitución de este usuario solicitante a través de la red;

almacenar la credencial de sustitución recibida en asociación con el identificador del primer usuario;

generar un certificado para la credencial de sustitución del primer usuario recibidos; y

transmitir, al primer usuario a través de la red, el certificado generado para usar en la reinscripción del primer usuario con el primer proveedor.

17. Artículo de producción según la reivindicación 16, donde la lógica almacenada es posteriormente configurada para obligar al procesador a operar para:

después de la transmisión del certificado generado, recibir, de este usuario solicitante a través de la red, otro mensaje, con el segundo número aleatorio y las otras segundas informaciones, firmadas con una credencial de este usuario solicitante; y

transmitir, al primer proveedor a través de la red, el otro mensaje firmado.

18. Artículo de producción según la reivindicación 12, donde la lógica almacenada es posteriormente configurada para obligar al procesador a operar para:

recibir, del primer usuario a través de la red, los requisitos de política de autentificación del primer usuario;

almacenar los requisitos de política de autentificación del usuario recibidos;

comparar los requisitos de política de autentificación del primer proveedor almacenados con los requisitos de política de autentificación del primer usuario almacenados;

determinar cualquier requisito de política de autentificación adicional basados en la comparación;

transmitir cualquier requisito de política de autentificación adicional determinado al usuario solicitante a través de la red; y

también determinar que la información de validación recibida del usuario solicitante corresponde con cualquier requisito de política de autentificación adicional determinado.

19. Artículo de producción según la reivindicación 12, donde la lógica almacenada es posteriormente configurada para obligar al procesador a operar para:

recibir, desde el primer usuario a través de la red, una primera de varias porciones de datos secretos del primer usuario;

almacenar la primera porción recibida de datos de secreto; y

después de autentificar que el usuario solicitante es el primer usuario, transmitir la primera porción de datos secretos almacenada al primer usuario a través de la red;

donde el mensaje firmado se recibe después de la transmisión de la primera porción de datos secretos.

20. Método de operar un servidor de autentificación para notificar a una entidad de red de una transacción a través de una red, que comprende:

recibir, de una primera entidad de red a través de la red, un identificador de una segunda entidad de red, un identificador de transacción, aprobación de transacción y requisitos de autentificación, y un mensaje con respecto a la transacción, donde el mensaje está (i) encriptado con una credencial de la segunda entidad de red, y (ii) también firmado con una clave privada de un par de claves privada/pública de la primera entidad de red, donde una clave pública del primer par de claves privada/pública de entidad de red se conoce por la segunda entidad de red;

transmitir, a la segunda entidad de red a través de la red, el identificador de transacción recibido, la aprobación de transacción y cualquier requisito de autentificación y mensaje firmado encriptado;

recibir, de la segunda entidad de red a través de la red después de la transmisión del identificador de transacción, aprobación de transacción y requisitos de autentificación, y mensaje firmado encriptado, al menos uno de una aprobación de transacción e información de autentificación; y

determinar, basándose en cualquier información de autentificación recibida, que la segunda entidad de red es auténtica; y

transmitir a la primera entidad de red una notificación de cualquier determinación y cualquier aprobación de transacción recibida.

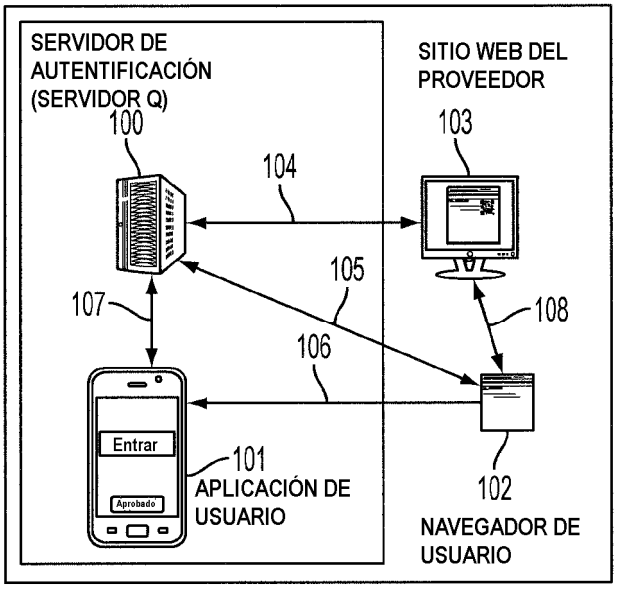
SERVIDOR DE AUTENTIFICACIÓN (SERVIDOR Q)
100
SITIO WEB DEL PROVEEDOR
103
104
105
107
108
106
Entrar
Aprobado
101
APLICACIÓN DE USUARIO
102
NAVEGADOR DE USUARIO

FIG. 1

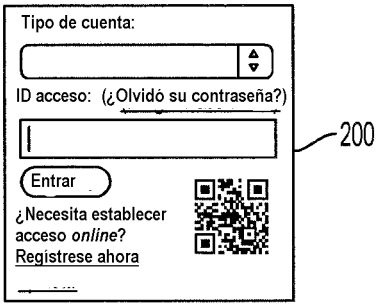
Tipo de cuenta:
ID acceso: (¿Olvidó su contraseña?)
Entrar
¿Necesita establecer acceso *online*?
Registrese ahora
200

FIG. 2

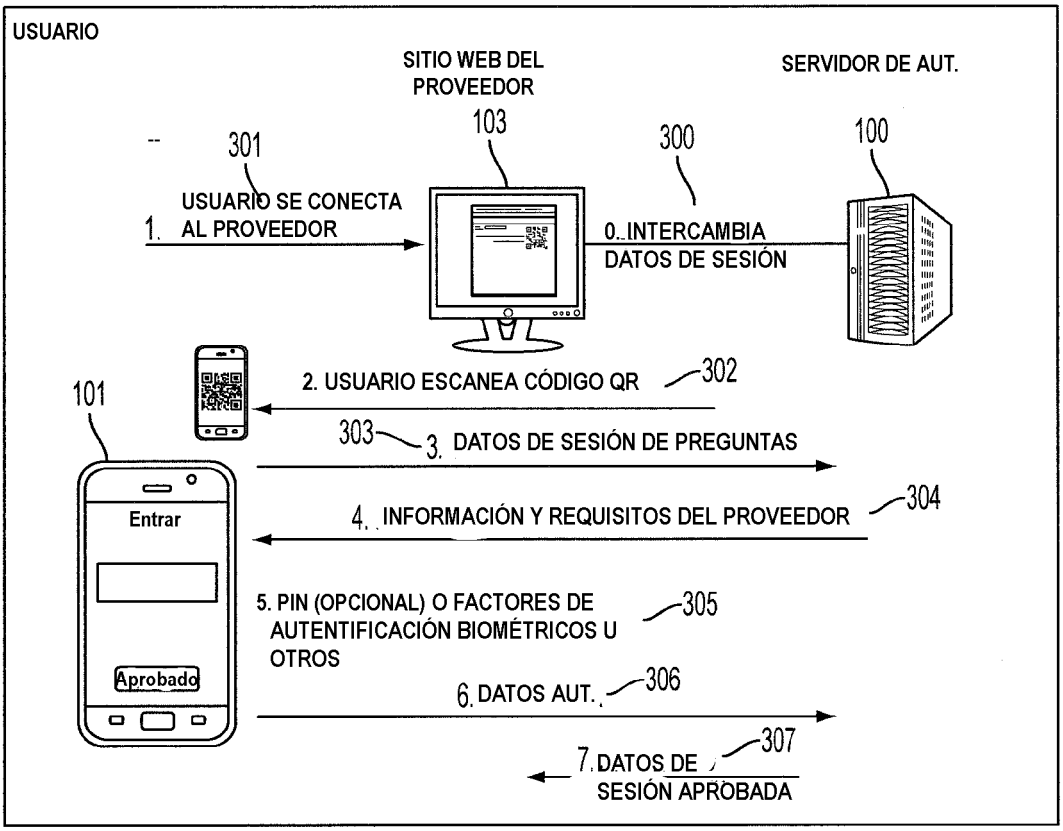
USUARIO
SITIO WEB DEL PROVEEDOR
SERVIDOR DE AUT.
103
300
100
301
USUARIO SE CONECTA AL PROVEEDOR
1.
0. INTERCAMBIA DATOS DE SESIÓN
2. USUARIO ESCANEA CÓDIGO QR
302
101
303
3. DATOS DE SESIÓN DE PREGUNTAS
Entrar
4. INFORMACIÓN Y REQUISITOS DEL PROVEEDOR
304
5. PIN (OPCIONAL) O FACTORES DE AUTENTIFICACIÓN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

FIG. 3

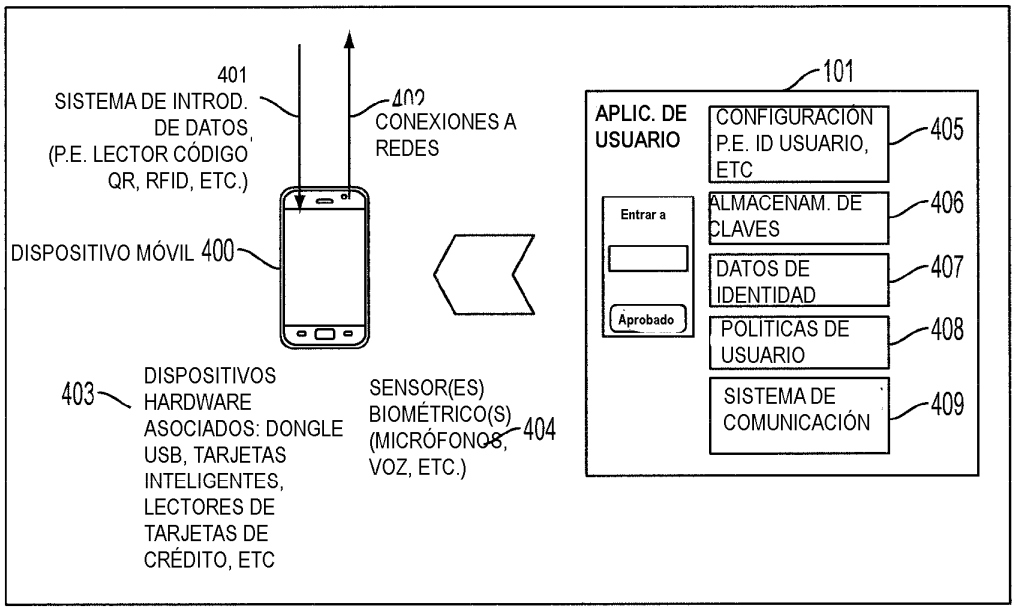
401
SISTEMA DE INTROD. DE DATOS (P.E. LECTOR CÓDIGO QR, RFID, ETC.)
402
CONEXIONES A REDES
DISPOSITIVO MÓVIL 400
403
DISPOSITIVOS HARDWARE ASOCIADOS: DONGLE USB, TARJETAS INTELIGENTES, LECTORES DE TARJETAS DE CRÉDITO, ETC
SENSOR(ES) BIOMÉTRICO(S) (MICRÓFONOS, VOZ, ETC.)
404
101
APLIC. DE USUARIO
Entrar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

FIG. 4

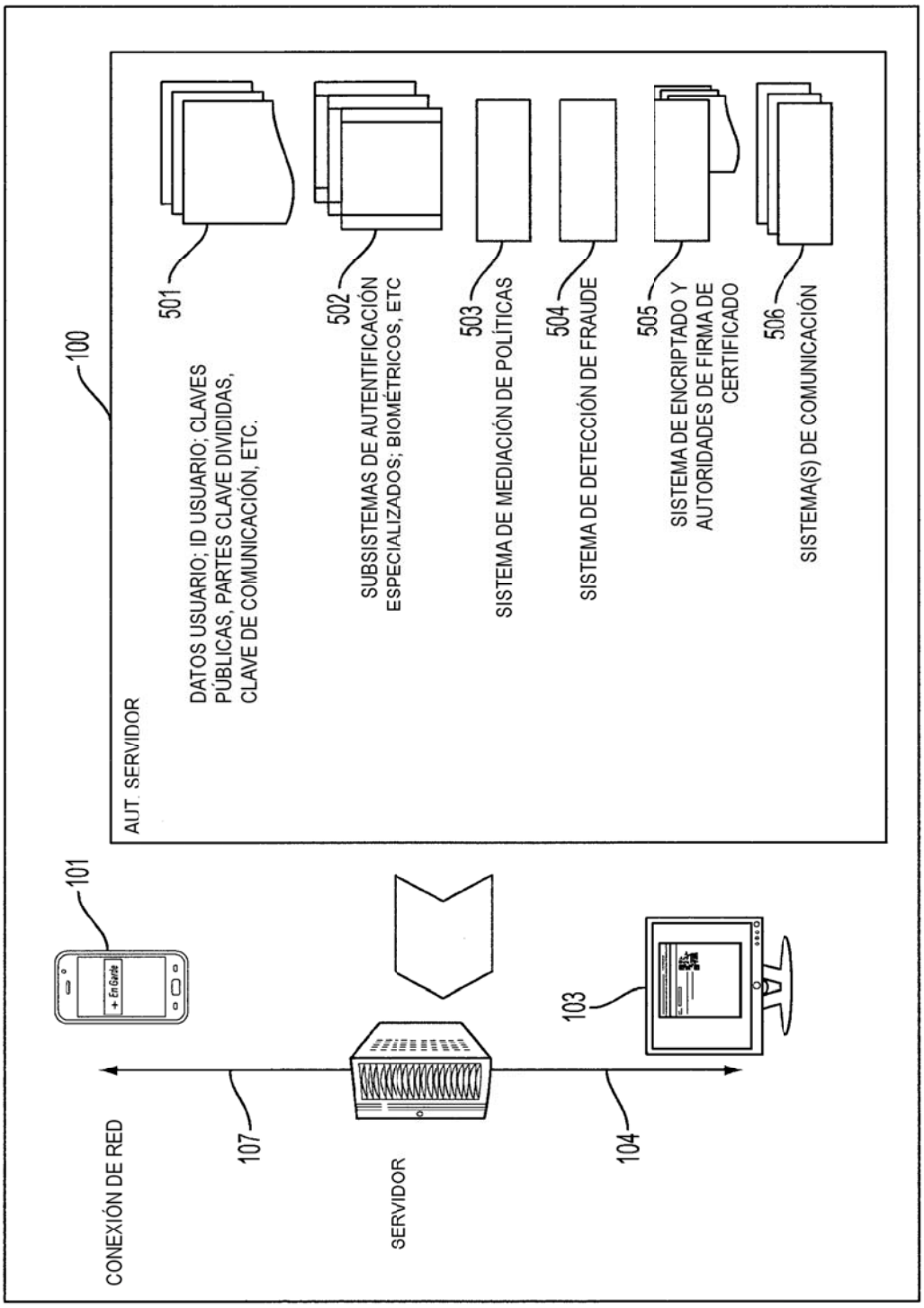
100
AUT SERVIDOR
501
DATOS USUARIO; ID USUARIO; CLAVES PÚBLICAS, PARTES CLAVE DIVIDIDAS, CLAVE DE COMUNICACIÓN, ETC.
502
SUBSISTEMAS DE AUTENTIFICACIÓN ESPECIALIZADOS; BIOMÉTRICOS, ETC
503
SISTEMA DE MEDIACIÓN DE POLÍTICAS
504
SISTEMA DE DETECCIÓN DE FRAUDE
505
SISTEMA DE ENCRIPTADO Y AUTORIDADES DE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

FIG. 5

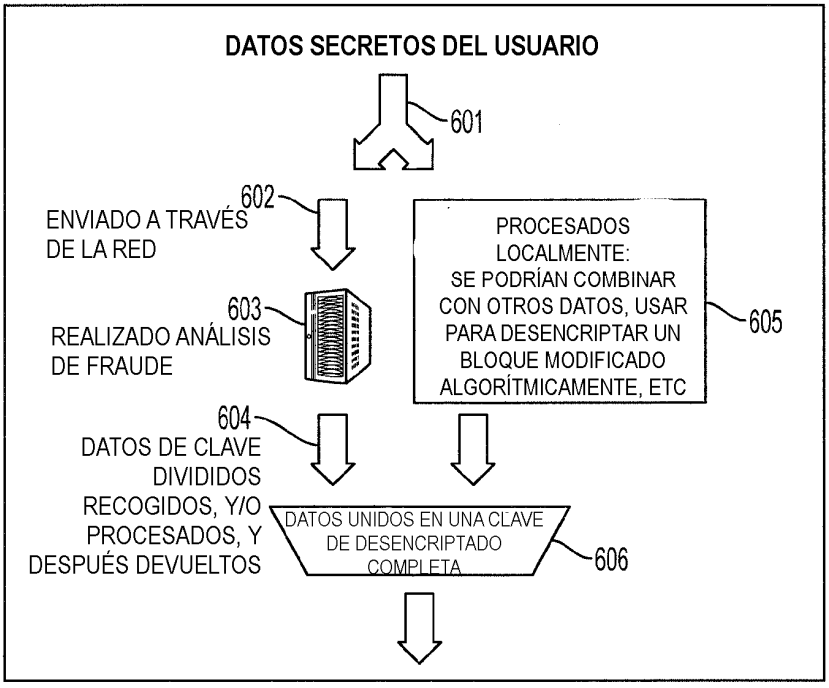
DATOS SECRETOS DEL USUARIO
601
602
ENVIADO A TRAVÉS DE LA RED
603
REALIZADO ANÁLISIS DE FRAUDE
PROCESADOS LOCALMENTE: SE PODRÍAN COMBINAR CON OTROS DATOS, USAR PARA DESENCRIPTAR UN BLOQUE MODIFICADO ALGORÍTMICAMENTE, ETC
605
604
DATOS DE CLAVE DIVIDIDOS RECOGIDOS, Y/O PROCESADOS, Y DESPUÉS DEVUELTOS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

FIG. 6

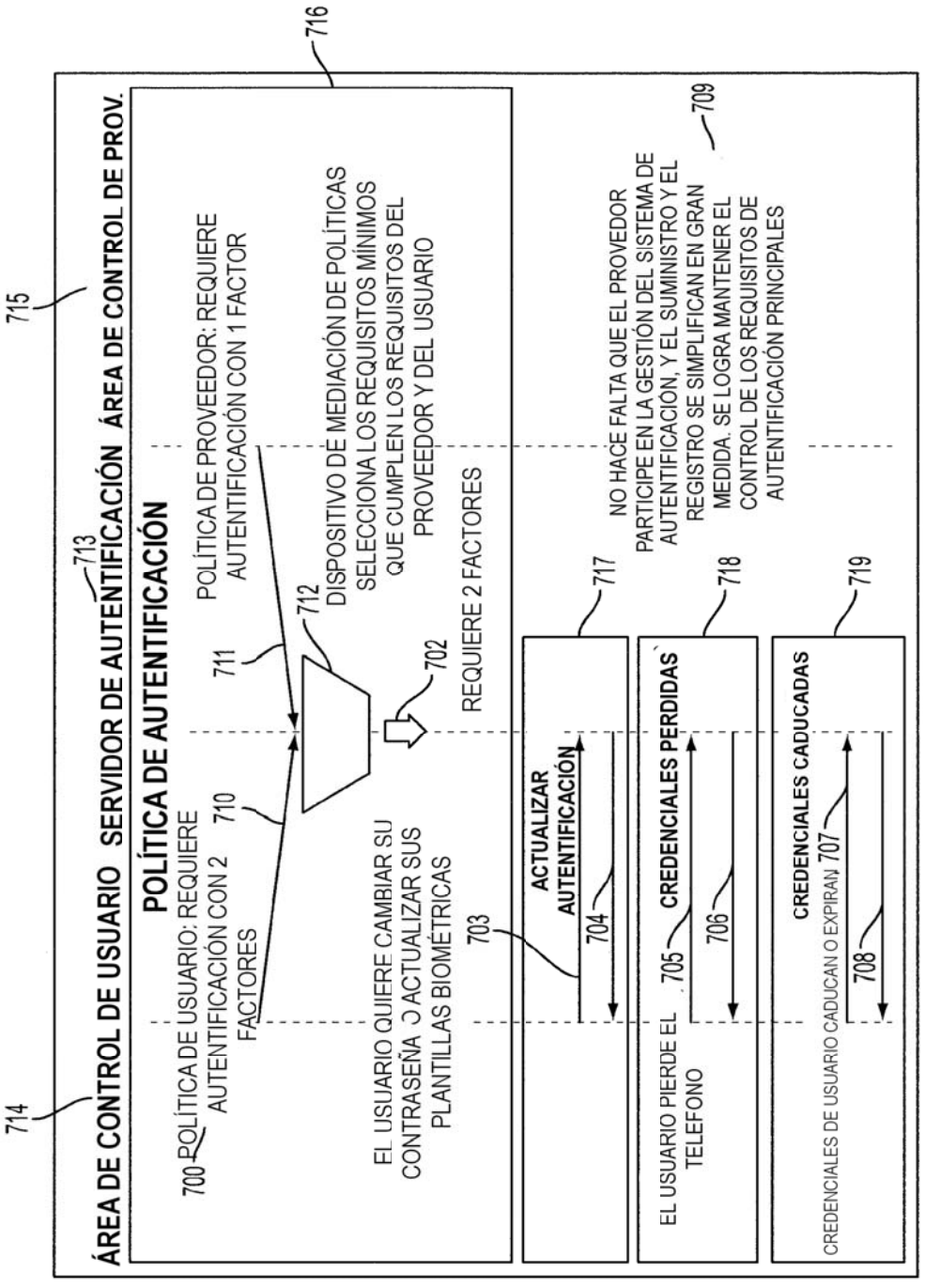
ÁREA DE CONTROL DE USUARIO
SERVIDOR DE AUTENTIFICACIÓN
ÁREA DE CONTROL DE PROV.
POLÍTICA DE AUTENTIFICACIÓN
POLÍTICA DE USUARIO: REQUIERE AUTENTIFICACIÓN CON 2 FACTORES
POLÍTICA DE PROVEEDOR: REQUIERE AUTENTIFICACIÓN CON 1 FACTOR
DISPOSITIVO DE MEDIACIÓN DE POLÍTICAS SELECCIONA LOS REQUISITOS MÍNIMOS 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
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719

FIG. 7

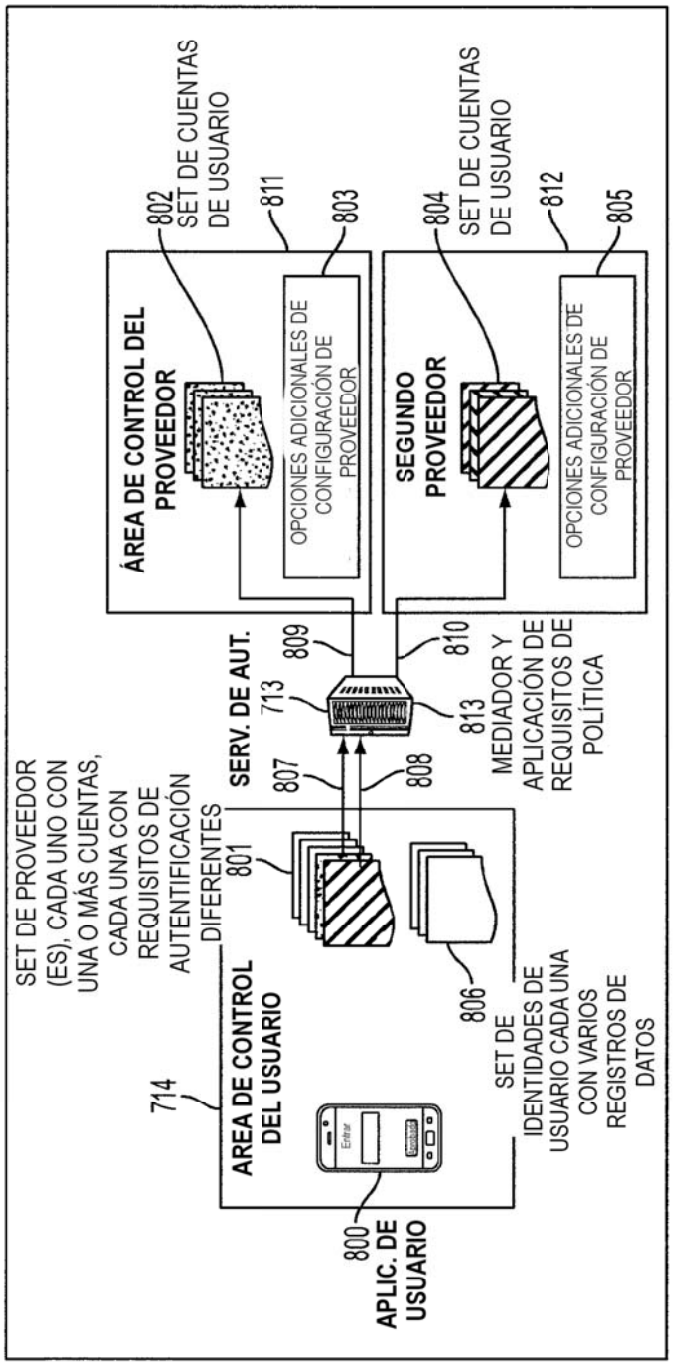
SET DE PROVEEDOR (ES), CADA UNO CON UNA O MÁS CUENTAS, CADA UNA CON REQUISITOS DE AUTENTIFICACIÓN DIFERENTES
801
SERV. DE AUT.
713
807
808
809
810
813
MEDIADOR Y APLICACIÓN DE REQUISITOS DE POLÍTICA
ÁREA DE CONTROL DEL PROVEEDOR
802
SET DE CUENTAS DE USUARIO
811
803
OPCIONES ADICIONALES DE CONFIGURACIÓN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

FIG. 8

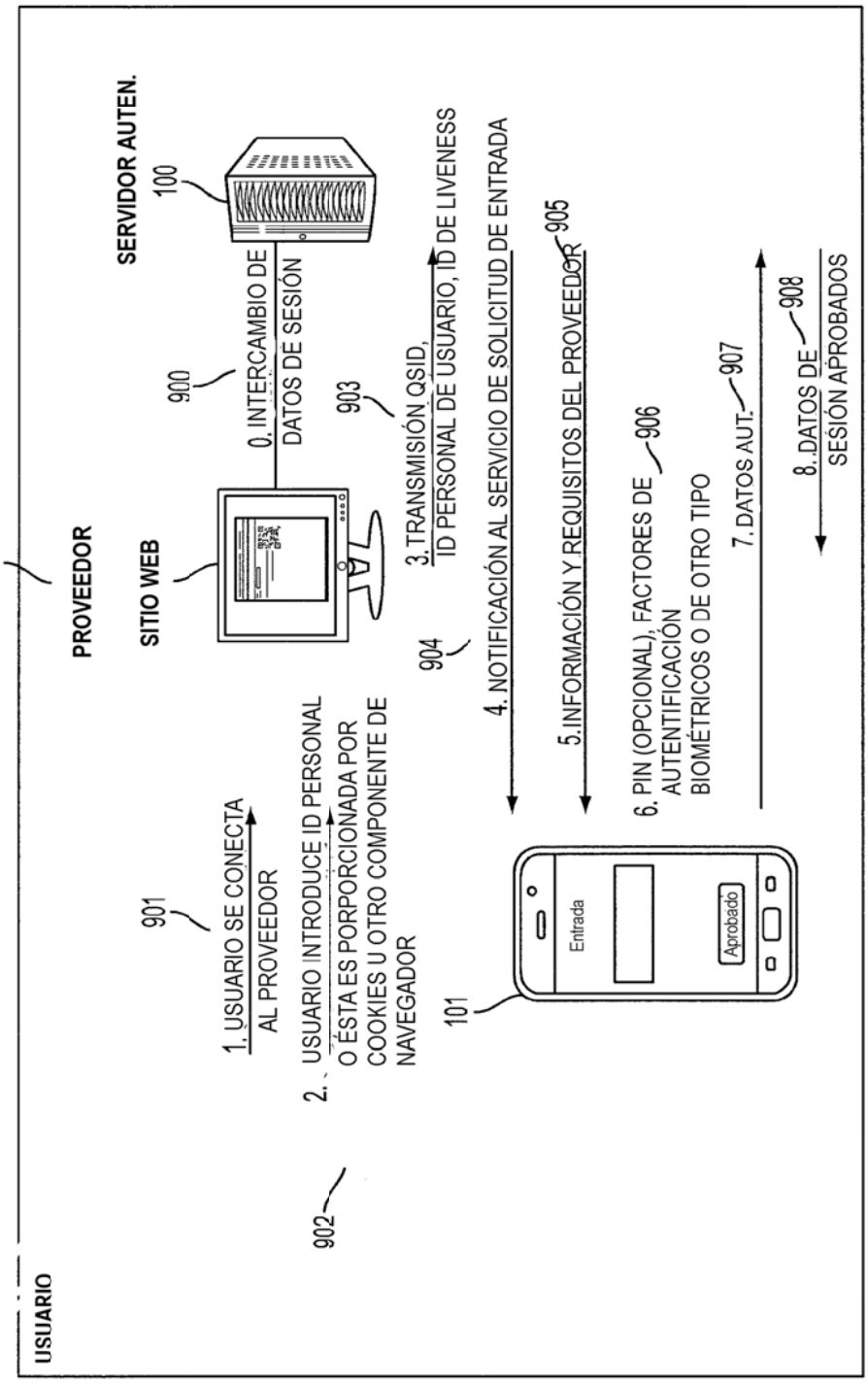
USUARIO
PROVEEDOR
103
SITIO WEB
SERVIDOR AUTEN.
100
900
0. INTERCAMBIO DE DATOS DE SESIÓN
903
3. TRANSMISIÓN QSID, ID PERSONAL DE USUARIO, ID DE LIVENESS
904
4. NOTIFICACIÓN AL SERVICIO DE SOLICITUD DE ENTRADA
905
5. INFORMACIÓN Y REQUISITOS DEL PROVEEDOR
906
6. PIN (OPCIONAL), FACTORES DE AUTENTIFICACIÓN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

FIG. 9

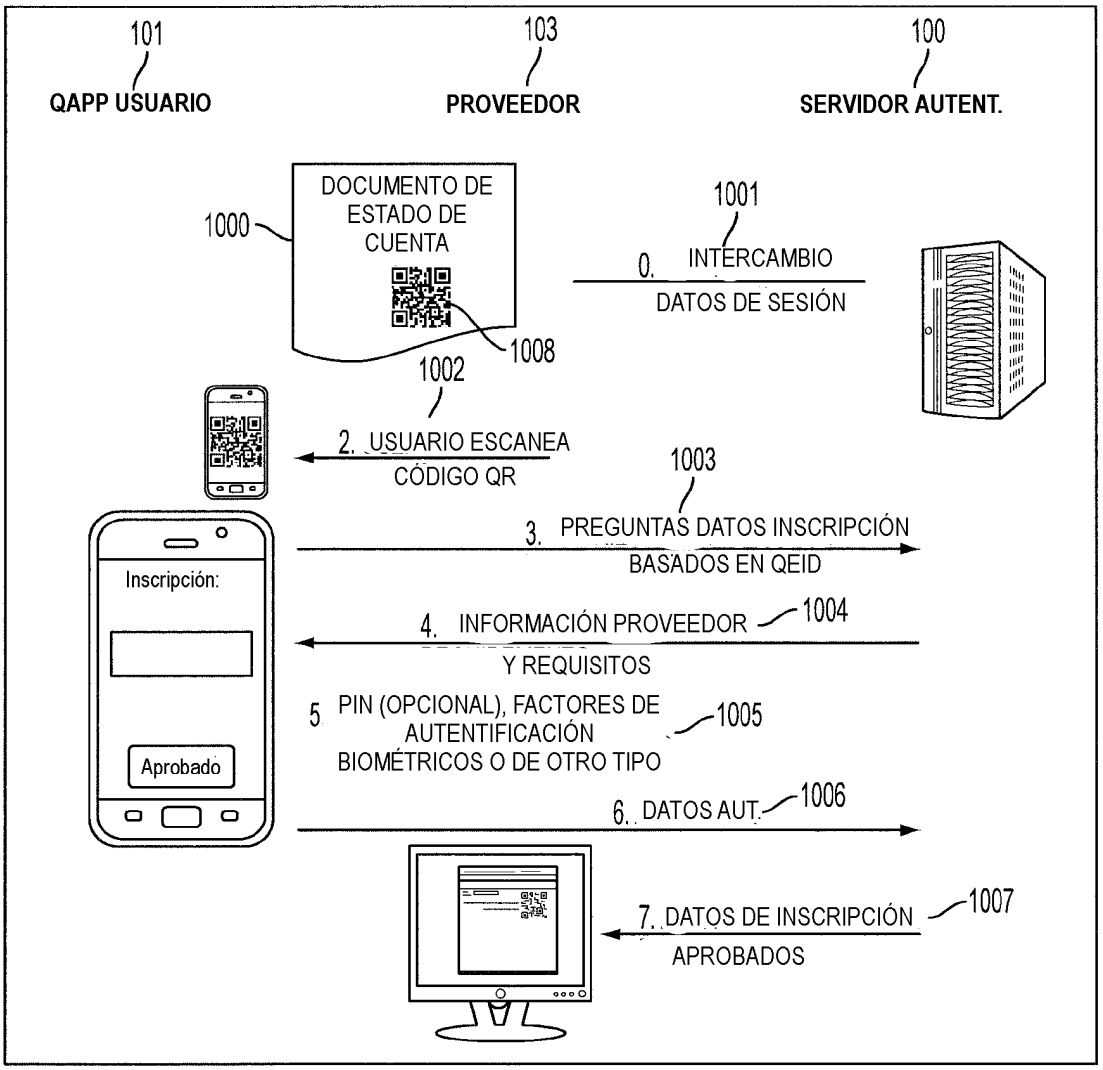
101
QAPP USUARIO
103
PROVEEDOR
100
SERVIDOR AUTENT.
DOCUMENTO DE ESTADO DE CUENTA
1000
1008
1001
0. INTERCAMBIO DATOS DE SESIÓN
1002
2. USUARIO ESCANEA CÓDIGO QR
1003
3. PREGUNTAS DATOS INSCRIPCIÓN BASADOS EN QEID
Inscripción:
Aprobado
4. INFORMACIÓN PROVEEDOR Y REQUISITOS
1004
5 PIN (OPCIONAL), FACTORES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

FIG. 10

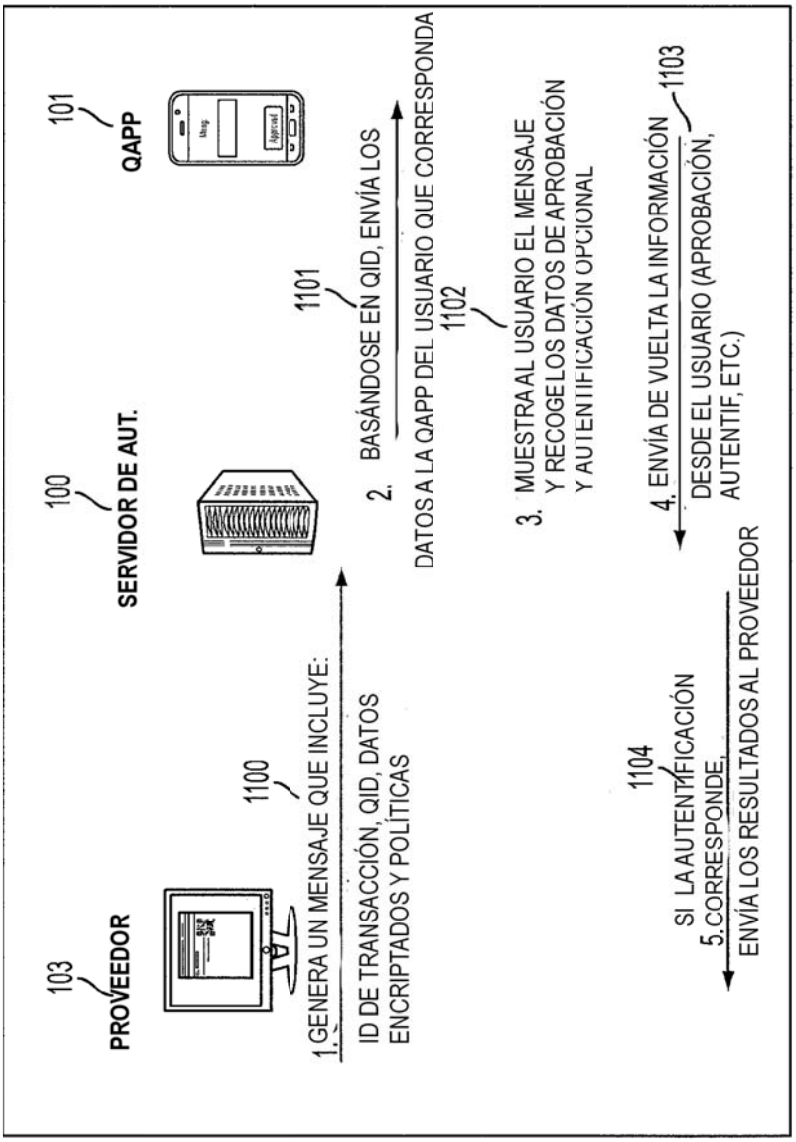
103
PROVEEDOR
100
SERVIDOR DE AUT.
101
QAPP
1100
1. GENERA UN MENSAJE QUE INCLUYE:
ID DE TRANSACCIÓN, QID, DATOS ENCRIPTADOS Y POLÍTICAS
1101
2. BASÁNDOSE EN QID, ENVÍA LOS DATOS A LA QAPP DEL USUARIO QUE CORRESPONDA
1102
3. MUESTRA AL USUARIO EL MENSAJE Y RECOGE LOS DATOS DE APROBACIÓN Y AUTENTIFICACIÓN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

FIG. 11