(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 993 217**

(51) Int. Cl.:

H04W 12/06 (2011.01)
H04W 12/48 (2011.01)
H04W 12/71 (2011.01)
H04W 12/72 (2011.01)
H04L 9/40 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **30.05.2017 E 21200338 (8)**

(97) Fecha y número de publicación de la concesión europea: **25.09.2024 EP 3955617**

(54) Título: **Autenticación de dispositivos móviles utilizando diferentes canales**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
26.12.2024

(73) Titular/es:

BELGIAN MOBILE ID SA/NV (100.00%)
Sint Goedeleplein 5
1000 Brussels, BE

(72) Inventor/es:

MASURE, MARC y
KNECHT, REMY

(74) Agente/Representante:

SÁEZ MAESO, Ana

DESCRIPCIÓN

Autenticación de dispositivos móviles utilizando diferentes canales

Campo de la invención

La presente invención se refiere a la autenticación.

Antecedentes

El comercio electrónico, el acceso a las redes sociales y otras formas de actividad o servicio digital en línea suelen requerir algún tipo de autenticación o identificación del usuario. Por ejemplo, un usuario que desee acceder a un sitio web o aplicación bancaria puede tener que introducir un nombre de usuario y una contraseña. Este enfoque, sin embargo, se considera generalmente no solo inconveniente, ya que requiere que el usuario recuerde su nombre de usuario y contraseña, sino también vulnerable a accesos fraudulentos, ya que el usuario puede elegir una contraseña simple y/o fácil de adivinar o encontrar por alguien que no sea el usuario adecuado. Además, el usuario puede necesitar muchos nombres de usuario y contraseñas diferentes para distintas actividades o servicios, lo que dificulta que el usuario recuerde los nombres de usuario y las contraseñas y, por lo tanto, hace más probable que utilice el mismo nombre de usuario y las mismas contraseñas para varios servicios.

La seguridad puede aumentarse utilizando más de un factor, como una contraseña u otra forma de factor de conocimiento, y un generador de tókenes u otra forma de factor de posesión. En particular, cada vez es más popular la autenticación de dos factores a través del teléfono móvil (mediante la cual se puede utilizar el teléfono móvil de un usuario para proporcionar una contraseña de un solo uso).

La comodidad puede mejorarse utilizando un método que, por ejemplo, no requiera contraseña o permita un único inicio de sesión. Por ejemplo, GSMA Mobile Connect permite a un usuario iniciar sesión en un sitio web o una aplicación sin nombre de usuario ni contraseña. Encontrará más información en https://mobileconnect.io/.

El documento US 2011/093920 A1 describe un sistema para crear tolerancia en la autenticación de un dispositivo informático, que incluye un medio para ejecutar, desde un medio legible por ordenador, pasos implementables por ordenador de: (a) recibir y almacenar una primera huella dactilar del dispositivo durante un primer arranque de un software de autenticación en el dispositivo, la primera huella dactilar basada en un primer conjunto de componentes del dispositivo, (b) recibir una segunda huella dactilar del dispositivo en un momento posterior, (c) comparar la segunda huella dactilar con una pluralidad de huellas digitales almacenadas de dispositivos conocidos, (d) en respuesta a la comparación que indica una falta de coincidencia entre la segunda huella dactilar y la pluralidad de huellas digitales almacenadas, generar un código de solicitud que comprende instrucciones para que el dispositivo genere una tercera huella dactilar utilizando el primer conjunto de componentes del dispositivo, (e) enviar el código de solicitud al dispositivo remoto, (f) recibir la tercera huella dactilar del dispositivo remoto en respuesta al código de solicitud, y (g) autenticar el dispositivo basándose en una comparación de la primera y la tercera huellas digitales.

El documento US 2013/244614 A1 divulga un sistema y un método para vincular en forma segura un número de teléfono y un código de identificación de usuario en una base de datos de directorio. Un método implementado por ordenador que comprende: recibir una primera solicitud de un primer dispositivo de usuario para registrarse en un primer servicio, en donde la solicitud identifica un número de teléfono del dispositivo de usuario e incluye un código de huella dactilar que identifica en forma única el primer dispositivo de usuario; registrar el número de teléfono en un servicio de directorio; recibir una segunda solicitud del primer dispositivo de usuario para registrarse en un segundo servicio, en donde la solicitud incluye un código de identificación de usuario que no es un número de teléfono y el código de huella dactilar; registrar el código de identificación de usuario en el servicio de directorio; detectar que la primera y la segunda solicitud proceden del mismo dispositivo móvil utilizando el código de huella dactilar; y vincular en forma reactiva el número de teléfono y el código de identificación de usuario en la base de datos del directorio.

El documento US 2017/149777 A1 describe un sistema que facilita la comunicación segura entre un dispositivo de usuario autorizado y dos o más servidores a través de dos o más canales que están asociados con los respectivos servidores. Para cada canal de comunicación, el sistema recibe un identificador de dispositivo para el dispositivo de usuario autorizado y vincula los identificadores de dispositivo entre sí a través de otro identificador, lo que permite al sistema reconocer que los diferentes identificadores de dispositivo identifican el mismo dispositivo de usuario autorizado. El sistema puede identificar un dispositivo no autorizado que se hace pasar por el dispositivo de usuario autorizado determinando que una comunicación del dispositivo no autorizado no incluye otro identificador que vincule los dos o más identificadores de dispositivo y/o determinando que un identificador de dispositivo calculado durante el proceso de registro es diferente de un identificador vinculado.

El documento US 2011/086616 A1 describe un método y un sistema para autenticar transacciones seguras entre un usuario que realiza una transacción y un host de transacciones seguras. El sistema incluye una aplicación de software para teléfonos móviles instalada en el teléfono móvil del usuario que realiza la

transacción, configurada para componer una huella dactilar asociada en forma exclusiva con el teléfono móvil específico en donde está instalada. El sistema incluye, además, un proveedor de servicios de autenticación en donde los usuarios del sistema pueden inscribirse registrando al menos los identificadores digitales compuestos por las aplicaciones instaladas en sus dispositivos de comunicación móvil en una base de datos de autenticación. El proveedor de servicios de autenticación está configurado para autenticar transacciones seguras a petición de los hosts de transacciones seguras mediante el envío de solicitudes de confirmación de transacciones a los teléfonos móviles de los usuarios inscritos solicitándoles que confirmen o rechacen transacciones seguras antes de que se permita finalizar dichas transacciones.

Síntesis

La invención se define por las reivindicaciones adjuntas.

De acuerdo con un primer aspecto de la presente invención, se proporciona un sistema de autenticación configurado, en una fase de inscripción, para intercambiar datos con una aplicación que se ejecuta en un terminal móvil a través de un segundo canal para recibir una huella dactilar del terminal móvil de la aplicación a través del segundo canal y para intercambiar datos con un elemento seguro incluido en el terminal móvil a través de un primer canal diferente para determinar, a través del primer canal, un identificador de elemento seguro y un identificador de hardware del terminal móvil. El sistema de autenticación está configurado, además, en la fase de inscripción, en respuesta a la recepción, desde una fuente, de una solicitud de inscripción de un usuario que comprende un identificador de usuario y un identificador del terminal móvil, para transmitir una primera contraseña a la fuente para su presentación al usuario y/o al terminal móvil, en respuesta a la recepción, desde la aplicación que se ejecuta en el terminal móvil, una primera clave (K1), la primera huella dactilar del terminal y una copia de la primera contraseña a través del segundo canal, para vincular el identificador del usuario, el identificador del terminal móvil, la aplicación y el terminal móvil, para transmitir un número aleatorio al elemento seguro del terminal móvil a través del primer canal, enviar una segunda clave (K2) al elemento seguro a través del primer canal, en respuesta a la recepción, desde el elemento seguro a través del primer canal, de un mensaje cifrado que comprenda una segunda huella dactilar del terminal cifrada con la segunda clave, en donde la segunda huella dactilar del terminal comprende el identificador del elemento seguro y el identificador del hardware, transmitir una segunda contraseña al elemento seguro a través del primer canal, y en respuesta a la recepción, desde la aplicación a través del segundo canal, una copia de la segunda contraseña y en dependencia de la copia de la segunda contraseña que coincida con la segunda contraseña, para vincular el identificador de usuario y la segunda huella dactilar del terminal o los datos incluidos en la segunda huella dactilar del terminal.

De acuerdo con un segundo aspecto de la presente invención, se proporciona un terminal móvil para su uso en la autenticación de una transacción que comprende un elemento seguro y una aplicación que se ejecuta en el terminal móvil, la aplicación configurada, en una fase de inscripción, para intercambiar datos con un sistema de autenticación a través de un segundo canal con el fin de proporcionar una primera huella dactilar del terminal móvil al sistema de autenticación a través del segundo canal. El elemento seguro está configurado, en una fase de inscripción, para intercambiar datos con el sistema de autenticación a través de un primer canal diferente, con el fin de proporcionar un identificador de elemento seguro y un identificador de hardware del terminal móvil al sistema de autenticación a través del primer canal. El terminal móvil está configurado, además, en la fase de inscripción, en respuesta a que el sistema de autenticación recibe, de una fuente, una solicitud de inscripción de un usuario que comprende un identificador de usuario y un identificador del terminal móvil, y a que el sistema de autenticación transmite una primera clave a la fuente para su presentación al usuario y/o al terminal móvil, para enviar una primera clave (K1), la primera huella dactilar del terminal y una copia de la primera contraseña a través del segundo canal desde la aplicación que se ejecuta en el terminal móvil al sistema de autenticación, en donde el sistema de autenticación está configurado para vincular el identificador del usuario, el identificador del terminal móvil, la aplicación y el terminal móvil en respuesta a la recepción de la primera clave, la segunda huella dactilar del terminal y la copia de la primera contraseña, en respuesta al elemento seguro que recibe un número aleatorio y una segunda clave del sistema de autenticación a través del primer canal, enviar un mensaje cifrado que comprende una segunda huella dactilar del terminal cifrada con la segunda clave, en donde la segunda huella dactilar del terminal comprende el identificador del elemento seguro y el identificador del hardware, desde el elemento seguro a través del primer canal al sistema de autenticación, en respuesta al elemento seguro que recibe una segunda contraseña del sistema de autenticación a través del primer canal, enviar una copia de la segunda contraseña desde la aplicación a través del segundo canal al sistema de autenticación, en donde el sistema de autenticación está configurado para vincular el identificador de usuario y la segunda huella dactilar del terminal o los datos incluidos en la segunda huella dactilar del terminal en función de que la copia de la segunda contraseña coincida con la segunda contraseña.

Breve descripción de los dibujos

Algunas realizaciones de la presente invención se describirán a continuación, a modo de ejemplo, con referencia a los dibujos adjuntos, en los que:

Figura 1 ilustra esquemáticamente la vinculación de seguridad por la que la identidad de un usuario se vincula

a una pluralidad de activos que pueden utilizarse para asegurar una transacción;

Figura 2 es un diagrama de bloques de un sistema de autenticación que incluye un servidor de identidad central (o "servidor de autenticación"), un terminal móvil y una red móvil, en donde un usuario puede vincular su identidad a una pluralidad de activos y utilizar al menos algunos de esos activos para autenticar una transacción;

Figura 3 es un diagrama de bloques más detallado del soporte de identidad central de la Figura 1;

Figuras 4a a 4d muestran los pasos de un proceso de inscripción de un usuario en el sistema de autenticación mostrado en la Figura 1;

Figura 5 ilustra un ejemplo de un primer conjunto de páginas presentadas a un usuario durante la inscripción;

Figura 6 ilustra un ejemplo de un segundo conjunto de páginas presentadas a un usuario durante la inscripción;

Figuras 7a a 7c ilustran un ejemplo de un tercer conjunto de páginas presentadas a un usuario durante la inscripción;

Figuras 8a a 8c muestran los pasos de un proceso de autenticación de un usuario que desea realizar una transacción, como iniciar sesión en el sitio web de una aplicación, compartir datos de identidad, proporcionar aprobación o proporcionar una firma electrónica cualificada;

Figura 9 ilustra un ejemplo de un primer conjunto de páginas presentadas a un usuario durante la autenticación; y

Figura 10 ilustra un ejemplo de un segundo conjunto de páginas presentadas a un usuario durante la autenticación.

Descripción detallada de algunas realizaciones

Refiriéndose a la Figura 1, un usuario 1 tiene una identidad 2 que puede vincularse a una pluralidad de activos (o "factores") 3, 4, 5, 6, 7, 8, 9, 10 que pueden utilizarse para corroborar la identidad 2 del usuario 1 y, por lo tanto, servir para autenticar al usuario 1.

Los activos 3, 4, 5, 6, 7, 8, 9, 10 pueden incluir una aplicación (o "app") 3 instalada en un terminal 4 móvil (en lo sucesivo denominado simplemente "terminal") que se utiliza como interfaz para que el usuario 1 confirme las transacciones, el terminal 4, un elemento 5 seguro como un módulo 5 de identificación del abonado (SIM) en el terminal 4, un applet 6, como un applet del SIM en el elemento 5 seguro (en el presente documento, el applet 6 también se denomina applet del SIM), una o varias características 7 biométricas, un número 8 de identificación personal (PIN) (que no tiene por qué ser puramente numérico, sino que puede incluir letras u otros tipos de caracteres), una contraseña 9 de un solo uso (OTP) y la ubicación 10. Ejemplos de terminales 4 móviles son un ordenador portátil, un teléfono inteligente, una tableta, un dispositivo portable u otro tipo de dispositivo conectado a la red, incluido un dispositivo de Internet de las Cosas (o IoT) o un dispositivo integrado. Algunos ejemplos de características biométricas son la huella dactilar, el escáner de iris, el reconocimiento de voz, el comportamiento gestual, etc. En el presente documento, el término "SIM" abarca un módulo universal de identidad del abonado ("Universal Subscriber Identity Module", USIM), una tarjeta de circuito integrado universal ("Universal Integrated Circuit Card", UICC), una SIM virtual (como un entorno de ejecución de confianza ("trusted execution environment", TEE)) y otros tipos similares de elementos seguros de terminales móviles.

Los activos 3, 4, 5, 6, 7, 8, 9, 10 pueden pertenecer a una de varias categorías 11, 12, 13, 14 que definen una relación con el usuario. Por ejemplo, un activo 3, 4, 5, 6 puede ser una posesión 11 del usuario, es decir, lo que el usuario tiene. Un activo 7 puede ser una característica 12 física del usuario (en lo sucesivo denominada "característica biométrica"), es decir, lo que el usuario "es". Un activo 8, 9 puede ser el conocimiento 13 del usuario, es decir, lo que el usuario sabe. Un activo 10 puede ser la ubicación 14 del usuario, es decir, dónde está el usuario.

Estos activos 3, 4, 5, 6, 7, 8, 9, 10 pueden proporcionar una autenticación de n factores, donde n = 2, 3, 4 o más, utilizando al menos un activo 3, 4, 5, 6, 7, 8, 9, 10 en cada una de al menos dos, preferiblemente al menos tres, categorías diferentes de definición de relaciones 11, 12, 13, 14, como la aplicación 3 y el terminal 4, y el PIN 8 y/o la característica 7 biométrica.

En referencia a la Figura 2, se muestra un sistema 20.

El sistema 20 incluye un sistema 21 de autenticación (en lo sucesivo también denominado "un soporte de identidad central") que puede comprender uno o más servidores y que incluye una base 22 de datos que almacena una tabla 23 que incluye una entrada 24 para cada usuario registrado en el sistema. Como se explicará con más detalle más adelante, una entrada 24 incluye una pluralidad de campos 26, 27, 28, 29, 30, 31, 32 relacionados con el usuario y sus activos de corroboración de identidad 3, 4, 5, 6, 7, 8, 9, 10 (Figura 1).

El sistema 21 de autenticación está provisto de un módulo 32 de seguridad de hardware (HSM) que puede generar o almacenar claves K1, K2 específicas del usuario. Un ejemplo de HSM 32 adecuado es el Ezio Confirm Authentication Server comercializado por Gemalto N.V., Ámsterdam, Países Bajos.

La aplicación 3 que se ejecuta en el terminal 4 contiene un kit de desarrollo de software (SDK) correspondiente que puede gestionar la creación de claves, asegurar una conexión entre la aplicación 3 y el soporte 21 de identidad central, detectar dispositivos rooteados o con jailbreak, detectar antienganches, ofuscar código, tomar huellas digitales del terminal en el lado del sistema operativo (OS) y otras funciones de seguridad, como deshabilitar la captura de pantalla durante la introducción del PIN, bloc de PIN seguro, no ver las teclas pulsadas, etcétera. Como se explicará con más detalle a continuación, se puede utilizar una clave como semilla y un PIN en el software para generar una OTP basada en el tiempo (TOTP), que se envía junto con una carga útil firmada que contiene una huella dactilar del terminal generada en el lado del sistema operativo del terminal y un contexto de la transacción. La huella dactilar del terminal es un conjunto de datos exclusivo del terminal móvil del usuario final. El contexto puede firmarse utilizando OCRA, y la TOTP y el contexto firmado por OCRA pueden enviarse al soporte 21 y cotejarse con los valores correspondientes calculados.

El sistema 20 incluye, por ejemplo, un registrador 37 de identidad que puede ser proporcionado por una oficina gubernamental, una agencia gubernamental, un banco u otra entidad de confianza. Como se explicará con más detalle a continuación, el registrador 37 de identidad permite a un usuario 1 final (Figura 1) transferir su identidad verificada en forma segura al soporte 21 de identidad central. El usuario 1 (Figura 1) puede presentar una prueba de identidad 38, por ejemplo, en forma de documento de identidad o pasaporte, en persona, en el registrador 37 de identidad, o desde una ubicación remota al registrador 35 de identidad (es decir, sin estar presente en el registrador 38 de identidad) utilizando un lector de tarjetas (no mostrado). La prueba de identidad 38 puede adoptar la forma de un dispositivo electrónico, como una tarjeta inteligente, que puede ser leída por un lector de tarjetas (no mostrado). El servidor 21 de autenticación y el registrador 37 de identidad se comunican en forma segura a través de una interfaz 40.

El sistema 20 incluye un proveedor 41 de servidor, como un banco, un vendedor en línea, etc., que puede comunicarse con una aplicación 42 de proveedor de servicios que se ejecuta en el terminal 4 u otro dispositivo, o servir páginas web a un navegador web que se ejecuta en el terminal 4 u otro dispositivo. El proveedor 41 de servicios es un socio externo que presta servicios al usuario 1 final y que integra los servicios de autenticación proporcionados por el sistema 20 de autenticación, incluidas la autenticación, la autorización, la identificación y la firma digital. El proveedor 41 de servicios se comunica en forma segura con el servidor 21 de autenticación a través de una interfaz 45. El soporte 21 de identidad central y el proveedor 41 de servicios pueden intercambiar mensajes de acuerdo con un protocolo adecuado, como Simple Object Access Protocol (SOAP), OpenID o Security Assertion Markup Language (SAML).

El sistema 21 de autenticación puede comunicarse con el terminal 4 a través de una red 51 móvil terrestre pública (en lo sucesivo denominada simplemente “red móvil”) que comprende sistemas 52 de red móvil básica que incluyen, entre otras cosas, un registro 53 de ubicación de origen (“home location register”, HLR), una infraestructura 54 por aire (“over-the-air”, OTA) que puede asegurar la comunicación con una clave K3, y un centro 56 de servicio de mensajes cortos (SMS) (u otro centro de servicio de mensajería).

El HLR 53 almacena, para cada usuario abonado a la red móvil, un número 57 internacional de abonado de estación móvil (“Mobile Station International Subscriber Directory Number”, MSISDN), una identidad 58 internacional de abonado móvil (“International Mobile Subscriber Identity”, IMSI) y una identidad 59 internacional de equipo móvil (“International Mobile Equipment Identity”, IMEI). El MSISDN 57 suele denominarse número de teléfono móvil del usuario final, el IMSI 58 es un identificador único de la tarjeta SIM 5 y el IMEI 59 es un identificador único del terminal 4.

El soporte 21 de identidad central y la red 51 móvil se comunican en forma segura a través de una pasarela 60 de red móvil.

El terminal 4 comprende un controlador 61 basado en CPU, memoria 62 volátil y memoria 63 no volátil, una pantalla 64, dispositivo(s) 65 de entrada de usuario, un dispositivo 66 de entrada de características biométricas, un dispositivo 67 de posicionamiento (por ejemplo, en forma de receptor GPS), una interfaz 68 de red móvil y una interfaz 69 de red de área local inalámbrica. La pantalla 64 y al menos un dispositivo 65 de entrada de usuario pueden estar integrados en una pantalla táctil. Otros dispositivos 66 de entrada pueden incluir interruptores. En este ejemplo, el dispositivo 66 de entrada de características biométricas adopta la forma de un escáner de huellas digitales para proporcionar identificación táctil. Para mayor claridad y brevedad, no se describen otras partes del terminal 4, como la batería, el altavoz, el micrófono, etc.

El terminal 4 ejecuta un sistema 70 operativo (OS) y puede cargar y ejecutar otras aplicaciones, incluida la aplicación 42 del proveedor de servicios, un navegador 71 y la aplicación 3 de autenticación (en este documento también denominada “aplicación Belgian Mobile ID” o “aplicación BMID”). El terminal 4 puede ejecutar un sistema operativo iOS, Android u otro. El terminal 4 móvil puede soportar la comunicación mediante protocolos de comunicación de segunda generación de velocidad de datos mejorada para la evolución GSM (EDGE),

protocolos de comunicación de tercera generación (3G), protocolos de comunicación HSDPA, protocolos de comunicación de cuarta generación (4G) y/o protocolos de comunicación 4G LTE y protocolos de comunicación posteriores (como los protocolos de comunicación 5G).

Al ser un terminal 4 móvil que puede conectarse a la red 51 móvil, el terminal 4 almacena datos 72 de banda base que contienen información utilizada para servicios móviles, incluyendo, por ejemplo, IMEI, código de país móvil (MCC), código de red móvil (MNC), código de área de localización (LAC) e ID de célula (CID). Uno o más datos 72 de banda base pueden utilizarse como activo 10 de localización (Figura 1).

El terminal 4 ejecuta un software 73 para recibir y enviar mensajes SMS o cualquier otra forma adecuada de mensaje que pueda recibirse de la red 51 móvil. El terminal 4 también ejecuta un elemento seguro para recibir y enviar mensajes SMS. El terminal 4 también ejecuta un kit 74 de desarrollo de software (SDK) de elemento seguro (en lo sucesivo, "kit de desarrollo de software SIM"). El terminal 4 contiene un elemento 5 seguro que puede adoptar la forma de una tarjeta de inserción extraíble de un factor de forma determinado, como una micro-SIM (3FF) o una nano-SIM (4FF), o puede adoptar la forma de una SIM integrada, como una eSIM, o una SIM virtual (como TEE). La SIM 5 almacena un sistema 75 de archivos elementales (EF) y una copia de la clave OTA K3.

El applet 6 del SIM puede almacenar un par de claves pública-privada K2 y también un valor 76 de contador. Como se explicará con más detalle más adelante, el valor 76 del contador puede utilizarse para generar una OTP. El applet 6 del SIM puede instalarse en el elemento 5 seguro, pero no inicializarse cuando el usuario toma posesión del SIM 5 (por ejemplo, cuando el usuario compra el terminal o un contacto de telefonía móvil). Alternativamente, el applet 6 del SIM puede descargarse e instalarse después de que el usuario tome posesión del elemento 5 seguro.

Como se explicará con más detalle a continuación, la aplicación 3 de autenticación o el sistema 70 operativo pueden generar una huella dactilar del terminal 4 que sea única para el terminal del usuario final.

El usuario 1 (Figura 1) puede utilizar el terminal 4 y otros activos 3, 4, 5, 6, 7, 8, 9, 10 (Figura 1) para inscribirse en el soporte 21 de identidad central y autenticar su identidad utilizando el servidor 21 soporte de identidad central para asegurar una transacción con el proveedor 41 de servicios.

Se utilizan dos canales diferentes 78, 79 tanto para configurar una cuenta de autenticación como durante la autenticación. En el primer canal 78, el applet 6 del SIM y el soporte 21 de identidad central se comunican utilizando el canal OTA de la red 51 móvil. En un segundo canal 79, la aplicación 3 BMID y el soporte 21 de identidad central se comunican a través de la Internet 36 mediante una conexión WiFi o de datos móviles. Ambos canales 78, 79 están protegidos y las cargas útiles se cifran mediante las claves de aplicación y applet K1, K2.

El usuario 1 (Figura 1) puede inscribirse y/o solicitar una transacción utilizando el terminal 4. El usuario 1 (Figura 1) puede inscribirse y/o solicitar una transacción a través de otro dispositivo 81 (en lo sucesivo denominado simplemente "ordenador"), como un ordenador de sobremesa, un ordenador portátil o una tableta, que se utiliza junto con el terminal 4.

El ordenador 81 incluye al menos un procesador 82, memoria 83, almacenamiento 84 (por ejemplo, en forma de SSD), una pantalla 85, uno o más dispositivos 86 de entrada de usuario y al menos una interfaz 87 de red (que puede ser por cable o inalámbrica). El ordenador 81 puede ejecutar un navegador 88 que puede utilizarse para comunicarse con el registro 37 de identidad y/o el proveedor 41 de servicios.

En referencia a la Figura 3, el sistema 21 de autenticación se muestra con más detalle.

El soporte 21 de identidad central puede adoptar la forma de un servidor que comprende al menos un procesador 92, memoria 93, almacenamiento 94, una pantalla 95, uno o más dispositivos 96 de entrada de usuario y al menos una interfaz 97 de red.

El soporte 21 de identidad central incluye un módulo 98 de inscripción. El módulo 98 de inscripción incluye un gestor 99 de inscripción, un gestor 100 de contraseñas y un gestor 101 de tablas. El servidor 21 de autenticación también incluye un módulo 102 de aprobación. El módulo 102 de aprobación incluye un gestor 103 de aprobaciones, un gestor 104 de contraseñas y un gestor 105 de tablas. Pueden utilizarse otras configuraciones.

Como se explicará con más detalle a continuación, el soporte 21 genera dos desafíos, uno para el applet 6 del SIM y otro para la aplicación 4. El desafío del applet del SIM se basa en IMSI, IMEI y una OTP basada en tiempo o contador. El desafío de la aplicación se basa en una huella dactilar del terminal y un contexto de transacción, en donde la huella dactilar del terminal comprende una lista de parámetros técnicos o características relacionadas con el sistema operativo, el dispositivo, la aplicación y similares, y una clave de aplicación K1, siendo el resultado una OTP que se envía al soporte 21. El desafío del applet 6 del SIM se envía al soporte central a través del operador UMTS (OTA/SMS). El desafío/OTP de la aplicación se envía al soporte central a través de Internet (WiFi o datos móviles). Por lo tanto, hay dos canales separados (es decir,

independientes). El soporte 21 comprueba ambos retos para validar si la transacción puede llevarse a cabo.

Inscripción

En referencia a las Figuras 1, 2, Figuras 4a a 4d, 5, 6 y Figuras 7a a 7c, un usuario 1 final se inscribe para utilizar el servicio de autenticación. Durante la inscripción, el soporte 21 de identidad central vincula la identidad del usuario 2 a una pluralidad de activos 3, 4, 5, 6, 7, 8, 9, 10.

Un usuario inicia la inscripción a través de un registrador 37 de identidad (paso S401).

La Figura 5 muestra un ejemplo de cómo el usuario 1 puede inscribirse para utilizar el servicio de autenticación utilizando un navegador 88 en un ordenador 81 y el terminal 4. No obstante, el usuario 1 puede inscribirse utilizando una aplicación 42 del proveedor de servicios que se ejecuta en el ordenador 81 junto con el terminal 4 o utilizando una aplicación 42 del proveedor de servicios o el navegador 71 que se ejecuta en el terminal 4, o incluso en persona en, por ejemplo, el registro 37 de identidad utilizando el terminal 4.

En este caso, un banco sirve un registro 37 de identidad en donde el usuario tiene al menos una cuenta bancaria y ha demostrado previamente su identidad mediante un documento 38 de identidad u otra forma de prueba de identidad.

A continuación se muestra un ejemplo de conjunto de páginas web 111, 113, 116, 121, 126, 130, 135 que se presentan al usuario 1. Las páginas web, incluido su orden y contenido, pueden diferir.

Refiriéndose en particular a las Figuras 2 y 5, el servidor 37 de registro de identidad presenta al usuario 1 una primera página 111 web que incluye un enlace 112 a una segunda página 113 web. Es posible que el usuario ya haya presentado sus credenciales para acceder a la primera página web 111. La segunda página 113 incluye un campo 114 para introducir un número de tarjeta de débito o crédito, y un enlace 115 a una tercera página 116 web. La tercera página 116 web incluye información 117 sobre la(s) cuenta(s), uno o más enlaces 118, 119 para realizar acciones respectivas, como transferir fondos, realizar pagos en línea, y un enlace 120 para crear una cuenta de servicio de autenticación, que enlaza con una cuarta página 121 web. La cuarta página 121 web incluye un campo 122 para introducir el número de teléfono, es decir, el MSISDN 27, del terminal 4 que posee el usuario 1. La cuarta página 121 web puede incluir, en respuesta a un desafío (no mostrado), una respuesta 124. La cuarta página web 121 incluye un enlace 125 a una quinta página 126 web. La quinta página 126 web incluye un resumen 127 de los detalles del usuario, una casilla 128 de verificación para aceptar los términos y condiciones, y un enlace 129 para continuar.

Refiriéndose ahora a las Figuras 2 y 6, el servidor 37 de registro de identidad puede presentar una sexta página 130 web al usuario 1 que confirma la solicitud de crear una cuenta de autenticación e incluye información 131 relevante, como el MSISDN 27, y un enlace 132 que invita al usuario a continuar a la página siguiente.

Refiriéndose de nuevo a las Figuras 2, 4a y 6, en respuesta a la recepción de la aceptación de los términos y condiciones y la confirmación para continuar, el registrador 37 de identidad (en este caso, el banco) transmite una solicitud 133 para crear una cuenta de autorización al soporte 21 de identidad central (paso S402). La solicitud 133 incluye la identidad 26 del usuario y el MSISDN 27.

El soporte 21 de identidad central genera una OTP 134 (en lo sucesivo denominada “token”) para proteger la sesión entre el registrador 37 de identidad y la aplicación 3 BMID (paso S403) y envía el token 134 a través de una conexión segura al registrador 37 de identidad (paso S404). El registrador 37 de identidad presenta el token 134 en una séptima página 135 web en el navegador 88 del ordenador 81 (paso S405).

Si aún no lo ha hecho, el usuario hace que el terminal 4 descargue e instale la aplicación 3 (paso S406).

Refiriéndose en particular a las Figuras 2, 4a y 7, el usuario final abre la aplicación 3 BMID e introduce su MSISDN 27 (paso S407). Al abrirse por primera vez, la aplicación 3 puede presentar una ventana 141 que incluye un botón 142 que solicita al usuario que cree una cuenta. La aplicación 3 pide al usuario, en una pantalla 143, que introduzca el MSISDN 27 en un campo 144 y un enlace 145 para continuar. Una vez que el usuario ha introducido el MSISDN 27, la aplicación 3 puede presentar una pantalla 146 que indica que el MSISDN 27 está siendo verificado.

La aplicación 3 crea un par de claves pública-privada K1 que comprende pk, sk (paso S408) y envía la clave pública pk, junto con el MSISDN 27, al soporte 21 de identidad central (paso S409). El soporte 21 de identidad central puede entonces vincular el MSISDN 27 a una sesión existente con el registro 37 de identidad. La aplicación 3 crea una huella dactilar de terminal 147 en el lado del sistema operativo del terminal 4 (paso S410) y la envía al soporte 21 de identidad central para vincular la aplicación 3 y el terminal 4 con la identidad 26 y el MSISDN 27 (paso S411). En este caso, la huella 147 digital del terminal creada por la aplicación 3 se denomina “primera huella dactilar del terminal” o “huella dactilar del terminal del lado del sistema operativo”.

La aplicación 3 solicita al usuario que introduzca el token 134 en la aplicación 3 (paso S412). Por ejemplo, la

aplicación 3 presenta una pantalla 148 que incluye un campo 149 en donde el usuario puede introducir el token 134 y un botón 150 para indicar que el usuario desea continuar. Una vez que el usuario ha introducido el código 134, la aplicación 3 puede presentar una pantalla 151 indicando que el código 134 está siendo verificado. La aplicación 3 envía la copia del token 134 al soporte 21 de identidad central (paso S413).

El token 134 se utiliza para asegurar la sesión entre el registrador 37 de identidad y la aplicación 4 porque el usuario 1 final podría estar conectado a través del ordenador 81 en el sitio web del registrador de identidad y a la aplicación 3 BMID en su terminal 4. Sin embargo, si el registrador 37 de identidad dispone de una aplicación en el mismo terminal 4 que la aplicación 3 BMID, el token 134 puede transferirse en forma silenciosa y cifrada en modo aplicación-a-aplicación. En otras palabras, no es necesario pedir al usuario que introduzca el token 134 en la aplicación 3.

El soporte 21 de identidad central comprueba el MSISDN 27 y el testigo 134 recibido de la aplicación 3 para determinar si está pendiente un proceso de registro (paso S414). Si el token 134 transmitido y el token 134 recibido coinciden, el soporte 21 de identidad central vincula la identidad 26 del usuario, el MSISDN 27, la aplicación 3 y el terminal 4 en la entrada 24 de la tabla 23 (paso S415).

Refiriéndose en particular a las Figuras 2, 4b y 7, utilizando el HSM 32, el soporte 21 de identidad central genera un PIN 152 inicial temporal (paso S416) y lo envía vía SMS (u otro servicio de mensajería adecuado) como un mensaje 153 SMS al terminal 4 (paso S 417).

El terminal 4 muestra el mensaje 153 que incluye el PIN 152 inicial en la pantalla 154 (paso S418). El usuario 1 final cambia a la aplicación 3 y esta le pide que introduzca el PIN 152 inicial (paso S419). Por ejemplo, la aplicación 3 presenta una pantalla 156 que incluye un campo 157, en donde el usuario puede introducir el PIN 152 inicial y un botón 158 para indicar que el usuario desea continuar. Una vez que el usuario ha introducido el PIN 152 inicial, la aplicación 3 puede presentar una pantalla 159 indicando que el PIN 152 inicial está siendo verificado.

La aplicación 3 BMID utiliza el PIN 152 para realizar un cifrado unidireccional con el fin de generar un hash 160 (paso S420) y el hash 160 se transmite al soporte 21 de identidad central (paso S421). El soporte 21 de identidad central genera su propia versión del hash 160 utilizando el HSM 32 (paso S422) para comprobar si el PIN 152 introducido por el usuario es correcto (paso S423).

Si es correcto, el soporte 21 de identidad central envía un resultado 161 a la aplicación 3 (paso S424).

La aplicación 3 BMID solicita al usuario que cree y confirme un nuevo PIN 162 (paso S425). Por ejemplo, la aplicación 3 presenta una pantalla 163 que incluye un campo 164, en donde el usuario puede introducir un nuevo PIN 162 y un botón 165 para indicar que el usuario desea continuar. La aplicación 3 puede presentar otra pantalla (no mostrada) pidiendo al usuario que vuelva a introducir su nuevo PIN 162. Una vez confirmado el nuevo PIN 162, la aplicación 3 vincula el nuevo PIN 162 mediante un nuevo hash 166 a la clave de aplicación K1. Así, si se introduce el PIN 162 en el futuro, se genera otro hash, se compara con el hash 166 almacenado y, si los hashes coinciden, se desbloquea la clave de la aplicación K1.

La aplicación 3 BMID solicita al usuario que active una función biométrica, como Touch ID o huella dactilar (paso S426). Por ejemplo, la aplicación 3 presenta una pantalla 167 con un primer botón 168 mediante el cual el usuario puede confirmar que desea activar una función biométrica y un segundo botón 169 mediante el cual el usuario rechaza activar una función biométrica. Si el usuario activa una función biométrica, el terminal 4 le pedirá que proporcione datos biométricos, por ejemplo, que pulse el escáner 66 de huellas digitales. Una vez que el usuario ha proporcionado la entrada biométrica, la aplicación 3 puede presentar una pantalla 170 indicando que se está procesando la entrada biométrica.

La aplicación 3 BMID activa la función biométrica (paso S428) y envía un mensaje 171 de confirmación al soporte 21 de identidad central (paso S429).

El soporte 21 de identidad central actualiza el campo 30 de nivel de cuenta en la tabla 23 para indicar que la cuenta de autenticación se ha activado con un primer nivel de seguridad bajo (paso S430). Una cuenta de autenticación con un nivel de seguridad bajo permite al usuario utilizar su terminal 4, en particular la aplicación 3 BMID, para autenticar transacciones de bajo riesgo o de escaso valor, por ejemplo de un valor no superior a 50 EUR.

El soporte 21 de identidad central envía un mensaje 172 al registrador 37 de identidad para indicar que se ha activado la cuenta de autenticación (paso S431).

En este punto, la identidad 2 del usuario se ha vinculado a un activo 4 de software, a saber, la aplicación 3 BMID. Por lo tanto, solo se ha realizado un grado parcial de vinculación. Con el fin de reforzar la seguridad, se llevan a cabo otras vinculaciones, en particular con otras partes del terminal 4 a las que se accede de manera independiente, como se describirá a continuación con más detalle.

El soporte 21 de identidad central puede iniciar automáticamente el proceso de vinculación adicional o puede comprobar primero si es necesario realizar una vinculación adicional (pasos S432 a S434). Esto puede incluir la notificación al operador de red móvil de que el soporte 21 de identidad central pretende realizar la vinculación de hardware y comprobar si el applet 6 ya está instalado en el elemento 5 seguro o, si no está instalado, si el applet 6 puede instalarse en el elemento 5 seguro (pasos S432 y S434).

El soporte 21 de identidad central envía una solicitud 175 para el IMSI58 y el IMEI59 del MSISDN 27 a través de la pasarela 60 de red móvil a los sistemas 52 centrales de red móvil (paso S435). Los sistemas 52 centrales de red móvil envían una respuesta 175 que contiene el IMSI 57 y el IMEI 59 en el momento en que el terminal 4 se conecta a la red 51 móvil y que está vinculado al MSISDN 27 dado, que se conoce en ese momento y que está almacenado en el HLR 53. El IMSI 58 y el IMEI 59 se almacenan en la tabla 23.

El soporte 21 de identidad central recupera la clave de applet K2 del HSM 32 (paso S436) e inicializa el applet 6 del SIM a través de la pasarela 60 de red móvil mediante OTA enviando un mensaje 181 que contiene la clave de applet K2 (pasos S437 a S440). La OTA 54 encapsula el mensaje 181 en una APDU OTA con la clave OTA K3 para garantizar que la clave de subprograma K2 se transmite en forma segura. Tras recibir y descifrar el mensaje 181, el applet 6 del SIM almacena la clave de applet K2 en el SIM 5 (paso S441).

El soporte 21 de identidad central envía entonces una solicitud 182 al applet del SIM 6, a través de la pasarela 60 de red móvil, para enviar una huella 183 digital del terminal 4 desde el lado del elemento seguro (paso S442).

El applet 6 del SIM recupera el IMSI 28 del sistema de archivos 75 EF almacenado en el elemento 5 seguro y el IMEI 29 del terminal 4 de los datos 72 de banda base a través del kit de herramientas SIM 74 para crear la huella 183 digital del terminal (paso S443). En este caso, la huella 183 digital del terminal creada por el applet 6 se denomina “segunda huella dactilar del terminal” o “huella dactilar del terminal del lado del elemento seguro”. El applet 6 del SIM encripta la segunda huella 183 digital, que contiene el IMSI 28, el IMEI 29 y la versión del applet (no mostrada), con las claves del applet K2 (paso S444) y envía la huella 185 digital encriptada al soporte 21 de identidad central (paso S445).

El soporte 21 de identidad central comprueba si el IMSI28 y el IMEI29 se corresponden con el IMSI 58 y el IMEI 59 recibidos a través de la pasarela 60 de red móvil (paso S446).

Si hay una coincidencia, entonces el soporte 21 de identidad central genera una OTP 186 (aquí referido como un “código de verificación”) (paso S447) y envía una solicitud 187 conteniendo el código 186 de verificación al applet 6 de SIM para mostrar el código 186 de verificación (paso S448). Esto ayuda a garantizar que la aplicación 3 y el applet 6 del SIM se encuentran en el mismo terminal 4.

El applet 6 del SIM muestra el código 186 de verificación a través de la API de texto de visualización del kit de herramientas SIM (paso S449). Por ejemplo, el subprograma 6 del SIM muestra el código 186 de verificación en la pantalla 188.

El usuario final cambia a la aplicación 3 y esta le pide que introduzca el PIN 186 inicial (paso S450). Por ejemplo, la aplicación 3 presenta una pantalla 189 que incluye un campo 190, en donde el usuario puede introducir el código 186 de verificación y un botón 191 para indicar que el usuario desea continuar. La aplicación 3 también puede pedir al usuario que introduzca su PIN. Por ejemplo, la aplicación 3 presenta una pantalla 192 que incluye un campo 193, en donde el usuario puede introducir su PIN 162 y un botón 194 para indicar que el usuario desea continuar. Una vez que el usuario 1 ha proporcionado el código 186 de verificación y, opcionalmente, su PIN 162, la aplicación 3 puede presentar una pantalla 195 indicando que el sistema está verificando el código 186.

La aplicación 3 BMID envía el código 186 de verificación introducido por el usuario al soporte 21 de identidad central (paso S451). El soporte 21 de identidad central comprueba si el código 186 de verificación es correcto (paso S452) y, en caso afirmativo, vincula el IMSI 28 y el IMEI 29 a la identidad, por ejemplo, estableciendo un indicador 31 (paso S453).

El soporte 21 de identidad central envía una confirmación 197 a la aplicación 3 BMID (paso S454).

La aplicación 3 BMID realiza una llamada 198 al applet 6 (paso S455) que activa otra pantalla 199 del kit de herramientas SIM en la que se muestra que la cuenta se ha activado con la seguridad SIM (paso S456). En respuesta a que el usuario haga clic en un botón “continuar” 200, el applet 6 notifica a la app 3 con un mensaje 201 (paso S457). La aplicación 3 BMID muestra una pantalla 202 con un mensaje 203 que indica que el enlace se ha realizado correctamente (paso S458) y, a continuación, vuelve a la pantalla de inicio de la aplicación 204, que incluye un menú 205.

La aplicación 3 BMID envía un mensaje de confirmación 206 al soporte 21 de identidad central (paso S459). El soporte 21 de identidad central actualiza el campo 30 de nivel de cuenta en la tabla 23 para indicar que la cuenta de autenticación ha sido activada con un segundo nivel de seguridad alto (por ejemplo, eIDAS nivel de

seguridad “alto”) (paso S460).

En este punto, la identidad del usuario 2 ha sido vinculada no solo a la aplicación 3 BMID, sino también al applet 6 del SIM en el SIM 5 utilizando el primer y segundo canales 78, 79 independientes, respectivamente. Así, se ha realizado un mayor grado de vinculación y, por lo tanto, el terminal 4 puede utilizarse para autenticar transacciones de mayor valor.

Transacción/autenticación

En referencia a las Figuras 2, 8a y 9, un usuario 1 final (Figura 1) utiliza el servicio de autenticación móvil para autenticar una transacción. En particular, los activos 3, 4, 5, 6, 7, 8, 9, 10 se utilizan para corroborar la identidad del usuario 2 (Figura 1).

El usuario 1 final solicita una transacción en una aplicación del proveedor de servicios (paso S801). Por ejemplo, es posible que el usuario desee iniciar sesión en una aplicación (como una aplicación bancaria) o sitio web (como un sitio web bancario), compartir datos de identidad (por ejemplo, para crear una cuenta en un sitio web de comercio electrónico), proporcionar aprobación (por ejemplo, para aprobar una transacción financiera en una aplicación bancaria o sitio web, para aprobar la transferencia de información médica de un médico a una aseguradora, etc.) o proporcionar una firma electrónica cualificada, o similar.

En relación con una aprobación, se puede crear un hash compuesto por parte del contexto que se firma (similar a un hash que se crea para una transacción bancaria con un cheque seguro 3D mediante el cual un usuario utiliza un lector de tarjetas bancarias para teclear un importe y una parte de la cuenta bancaria del beneficiario, que a continuación genera un desafío tras el cual el hash se envía al banco). En este caso, sin embargo, no se utiliza un lector de tarjetas. En su lugar, la aplicación 3 BMID desempeña esa función.

En relación con la firma electrónica cualificada, el contexto completo se firma con un certificado cualificado. Utilizando el proceso aquí descrito, es posible firmar cumpliendo cualquiera de los tres niveles de seguridad (es decir, bajo, sustancial y alto) especificados por el reglamento eIDAS.

La Figura 9 muestra un ejemplo de cómo el usuario 1 puede solicitar una transacción utilizando un navegador 88 que se ejecuta en un ordenador 81 y puede autenticar la transacción utilizando el terminal 4. En este caso, el proveedor de servicios es un banco.

Refiriéndose en particular a las Figuras 2 y 9, el proveedor 41 de servicios presenta al usuario 1 una primera página web 301 que incluye un enlace 302 para iniciar sesión y un enlace 303 para iniciar sesión utilizando un número de móvil. Por ejemplo, si se utiliza SOAP o SAML, el proveedor 41 de servicios presenta una segunda página web 304 que incluye un campo 305 para introducir el número de teléfono, es decir, el MSISDN 27, del terminal 4 que posee el usuario 1. La página web 304 puede incluir, en respuesta a un desafío (no mostrado), una respuesta 307. La página web 304 incluye un enlace 308 para continuar. Si se utiliza OpenID, el proveedor 41 de servicios redirige a una página OpenID centralizada alojada por el soporte 21 de identidad central. En el caso de una aplicación que se ejecuta en el terminal 4, el número de teléfono puede transferirse de aplicación a aplicación.

El proveedor 41 de servicios envía una solicitud 311 para autenticar una transacción al soporte 21 de identidad central a través de la interfaz de proveedor de servicios 45 (paso S802). La solicitud 311 incluye el MSISDN 27 y una solicitud (no mostrada) para el nivel de seguridad requerido para la transacción. Los niveles de seguridad pueden incluir (1) solo PIN, (2) solo biometría, (3) PIN y biometría, (4) PIN y OTP vía SMS, (5) PIN y biometría y OTP vía SMS.

El soporte 21 de identidad central recupera el IMSI28 y el IMEI29 del terminal (paso S803). El soporte 21 de identidad central envía una solicitud 313 (o “primer desafío”) al applet 6 del SIM a través del primer canal 78, es decir, a través de la pasarela 60 de red móvil y la red OTA, para la huella dactilar del terminal del lado SIM (paso S804).

El applet 6 del SIM recupera el IMSI 28 del SIM 5 y el IMEI 29 de los datos de banda base 72 a través del kit de herramientas SIM (paso S805) y determina su ubicación a través del kit de herramientas SIM (paso S806). El applet 6 del SIM genera una huella 314 digital del terminal que incluye el IMSI 28, el IMEI 29, la versión del applet (no mostrada) y la ubicación (no mostrada) (paso S807). El applet 6 del SIM también genera una OTP 315, por ejemplo usando un valor del contador 76, y que puede ser firmado usando encriptación unidireccional OCRA (paso S808). Un mensaje 316 (o “primera respuesta”) que comprende la huella 314 digital del terminal y la OTP 315 se encripta utilizando las claves de aplicación K2 del applet del SIM y las claves K3 de la OTA y se transmite por el primer canal 78 (paso S809). El mensaje encriptado 316 se transmite al soporte 21 de identidad central a través del segundo canal 79, es decir, a través de la red OTA de la red 52 móvil (paso S810).

El soporte 21 de identidad central comprueba si la huella 314 digital del terminal se corresponde con el IMSI28 y el IMEI29 mantenidos localmente (paso S811). El soporte 21 de identidad central también comprueba si la OTP 315 corresponde a una generada localmente (pasos S812 y S813). Si falla la comprobación de la huella

dactilar del terminal o la comprobación de la OTP, la transacción se cancela.

El soporte 21 de identidad central también puede comprobar la ubicación del terminal 4 (paso S814).

En particular, el soporte 21 de identidad central puede comprobar si el terminal 4 está situado en un país o región aceptable de un país, está situado en un país o región inaceptable de un país, o si la ubicación de inicio de sesión y la ubicación del terminal 4 o las ubicaciones entre dos transacciones difieren en más de una distancia determinada o en más de una distancia determinada en un tiempo determinado (por ejemplo, inicio de sesión en el país A y aprobación en el país B, que está a más de 1.000 km de distancia, 2 minutos más tarde). Así pues, la ubicación puede utilizarse como parámetro de riesgo para la detección de fraudes y/o como factor adicional para la autenticación.

Si la huella dactilar del terminal se corresponde con la obtenida durante el proceso de vinculación, el soporte 21 de identidad central transmite una notificación 317 a la aplicación (paso S815).

La aplicación 3 envía una solicitud 318 para conocer el contexto de la transacción (paso S816) y el soporte 21 de identidad central transmite un mensaje 319 (“un segundo reto”) a través del segundo canal 79 (es decir, a través de Internet) que contiene información 320 sobre el contexto de la transacción, como el nombre del proveedor de servicios, la naturaleza de la transacción (por ejemplo, inicio de sesión, identificador compartido, aprobación, firma), hora y fecha, información sobre la transacción, etc. (paso S817). Puede utilizarse una plantilla estándar (como la plantilla CAP para transacciones bancarias).

La aplicación 3 solicita al usuario que inicie sesión en el terminal 4 en una primera pantalla 321 (pasos S818 y S819). Si el usuario pulsa un botón de continuar 322, la aplicación 3 presenta una segunda pantalla 322 (una pantalla denominada “lo que ves es lo que firmas” o “WYSIWYS”) al usuario que incluye la información 320 sobre el contexto de la transacción y las opciones 324, 325 para aceptar o rechazar la transacción (paso S820). Si se acepta (paso S821), la aplicación 3 presenta una tercera pantalla 326 que indica que se está verificando la transacción.

A continuación, la aplicación 3 solicita al usuario que proporcione hasta tres (o más) tipos de autenticación, como PIN, OTP y biométrica (pasos S821 a S824).

La aplicación 3 puede pedir al usuario que introduzca su PIN 162 (paso S821). Por ejemplo, la aplicación 3 puede presentar una cuarta pantalla 327 que incluya un campo 328 para introducir el PIN 162 y un botón 329 para continuar. La aplicación 3 presenta una quinta pantalla 331 que indica que la transacción está siendo verificada.

La aplicación 3 puede pedir al usuario que introduzca datos biométricos (paso S823). Por ejemplo, la aplicación 3 puede presentar una sexta pantalla 333 que incluya un mensaje 334 indicando al usuario, por ejemplo, que utilice la huella dactilar. La pantalla 333 puede incluir una opción de cancelación 335. El terminal 4 comprueba la entrada biométrica.

La aplicación 3 (en particular el SDK Ezio de Gemalto) utiliza el PIN 162 para realizar un cifrado unidireccional y generar un hash 330 (paso S824). La aplicación 3 (en particular el SDK Ezio de Gemalto) comprueba el hash 330 (paso S825). Si es correcto, entonces la aplicación 3 (en particular el SDK Ezio de Gemalto) genera una OTP 336 (“una segunda respuesta”) en forma de TOTP basada en una huella dactilar del terminal 332 y el contexto recibido 319 (paso S826) y firma la carga útil 327 mediante OCRA utilizando la clave K1 (paso S827). La huella dactilar de terminal 332 del lado del sistema operativo es generada por el SDK Ezio de Gemalto.

La aplicación 3 envía la carga útil 337 al soporte 21 de identidad central a través del segundo canal 79 (paso S328), donde se verifica con el resultado del mismo cálculo realizado en el soporte 21 (pasos S829 y S830). En particular, el HSM 32 puede realizar el mismo cálculo.

Si los resultados no coinciden, se interrumpe la transacción. Si los resultados coinciden, el soporte 21 de identidad central envía una confirmación 338 al proveedor 41 de servicios (paso S831), que presenta una página web 339 adecuada (paso S832), y una confirmación 340 a la aplicación 3, que presenta una pantalla 341 con un mensaje 342 que confirma que la transacción ha sido autorizada.

Modificaciones

Se apreciará que pueden realizarse diversas modificaciones a las realizaciones descritas con anterioridad. Tales modificaciones pueden implicar características equivalentes y otras que ya se conocen en el diseño, fabricación y uso de terminales de autenticación, banca en línea y comunicación móvil y partes componentes de los mismos y que pueden utilizarse en lugar o además de las características ya descritas en el presente documento. Las características de una realización pueden sustituirse o complementarse con características de otra realización.

El proceso de escaneado de huellas digitales en el lado OS del terminal puede ser configurable y puede hacerse

más o menos estricto activando parámetros OS adicionales o pocos en número.

La aplicación del proveedor de servicios, aunque se ejecute en un navegador, no necesita instalarse ni ejecutarse en el terminal. Puede ejecutarse en otro dispositivo diferente, como un dispositivo IoT de ordenador personal.

El soporte de identidad central puede comprender uno o más servidores.

Aunque en la presente solicitud se han formulado reivindicaciones para combinaciones particulares de características, debe entenderse que el alcance de la divulgación de la presente invención también incluye cualquier característica novedosa o cualquier combinación novedosa de características divulgadas en el presente documento, ya sea explícita o implícitamente, o cualquier generalización de las mismas, esté o no relacionada con la misma invención que se reivindica actualmente en cualquier reivindicación y mitigue o no alguno o todos los mismos problemas técnicos que la presente invención. Los solicitantes notifican por la presente que pueden formularse nuevas reivindicaciones para dichas características y/o combinaciones de dichas características durante la tramitación de la presente solicitud o de cualquier otra solicitud derivada de la misma.

REIVINDICACIONES

1. Un sistema (21) de autenticación configurado, en una fase de inscripción:

para intercambiar datos con una aplicación (3) que se ejecuta en un terminal (4) móvil a través de un segundo canal (79) para recibir de la aplicación, a través del segundo canal, una primera huella dactilar del terminal; y

para intercambiar datos con un elemento (5) seguro comprendido en el terminal móvil a través de un primer canal (78) diferente, a fin de determinar, a través del primer canal, un identificador (58) de elemento seguro y un identificador (59) de hardware del terminal móvil a través del primer canal;

y en donde el sistema de autenticación está configurado, además, en la fase de inscripción:

en respuesta a la recepción, desde una fuente (37), de una solicitud (133) de inscripción de un usuario que comprende un identificador (26) de usuario y un identificador (27, 57) del terminal móvil, para transmitir una primera contraseña a la fuente para su presentación al usuario y/o al terminal móvil;

en respuesta a la recepción, desde la aplicación (3) que se ejecuta en el terminal móvil, de una primera clave (K1), la primera huella dactilar del terminal y una copia de la primera contraseña a través del segundo canal (79), para vincular el identificador del usuario, el identificador del terminal móvil, la aplicación y el terminal móvil, para transmitir un número (153) aleatorio al elemento (5) seguro del terminal móvil a través del primer canal (78);

para enviar una segunda clave (K2) al elemento (5) seguro a través del primer canal; en respuesta a la recepción, desde el elemento (5) seguro a través del primer canal, de un mensaje cifrado (185) que comprende una segunda huella dactilar del terminal cifrada con la segunda clave, en donde la segunda huella dactilar del terminal comprende el identificador del elemento seguro y el identificador del hardware, para transmitir una segunda contraseña, al elemento seguro a través del primer canal; y

en respuesta a la recepción, desde la aplicación a través del segundo canal, de una copia de la segunda contraseña y en función de que la copia de la segunda contraseña coincida con la segunda contraseña, para vincular el identificador de usuario y la segunda huella dactilar del terminal o los datos incluidos en la segunda huella dactilar del terminal.

2. Un terminal móvil destinado a autenticar una transacción, que comprende un elemento (5) seguro y una aplicación (3) que se ejecuta en el terminal móvil, la aplicación configurada, en una fase de inscripción:

para intercambiar datos con un sistema (21) de autenticación a través de un segundo canal (79) para proporcionar una primera huella dactilar del terminal del terminal móvil al sistema de autenticación a través del segundo canal; y

el elemento seguro configurado, en una fase de inscripción:

para intercambiar datos con el sistema de autenticación a través de un primer canal (8) diferente para proporcionar un identificador (58) de elemento seguro y un identificador (59) de hardware del terminal móvil al sistema de autenticación a través del primer canal;

y en donde el terminal móvil está configurado, además, en la fase de inscripción:

en respuesta a que el sistema de autenticación recibe, de una fuente (37), una solicitud (133) de inscripción de un usuario que comprende un identificador (26) de usuario y un identificador (27, 57) del terminal móvil, y el sistema de autenticación transmite una primera contraseña a la fuente para su presentación al usuario y/o al terminal móvil, para enviar una primera clave (K1), la primera huella dactilar del terminal y una copia de la primera contraseña a través del segundo canal (79) desde la aplicación (3) que se ejecuta en el terminal móvil al sistema de autenticación, en donde el sistema de autenticación está configurado para vincular el identificador del usuario, el identificador del terminal móvil, la aplicación y el terminal móvil en respuesta a la recepción de la primera clave, la segunda huella dactilar del terminal y la copia de la primera contraseña;

en respuesta a que el elemento (5) seguro recibe un número (153) aleatorio y una segunda clave (78) del sistema de autenticación a través del primer canal (78), para enviar un mensaje (185) cifrado que comprende una segunda huella dactilar del terminal cifrada con la segunda clave, en donde la segunda huella dactilar del terminal comprende el identificador del elemento seguro y el identificador del hardware, desde el elemento seguro a través del primer canal al sistema de autenticación;

en respuesta al elemento seguro que recibe una segunda contraseña del sistema de autenticación a través del primer canal, para enviar una copia de la segunda contraseña desde la aplicación a través del segundo canal al sistema de autenticación, en donde el sistema de autenticación está configurado para vincular el identificador de usuario y la segunda huella dactilar del terminal o los datos incluidos en la segunda huella dactilar del terminal en función de que la copia de la segunda contraseña coincida con la segunda contraseña.

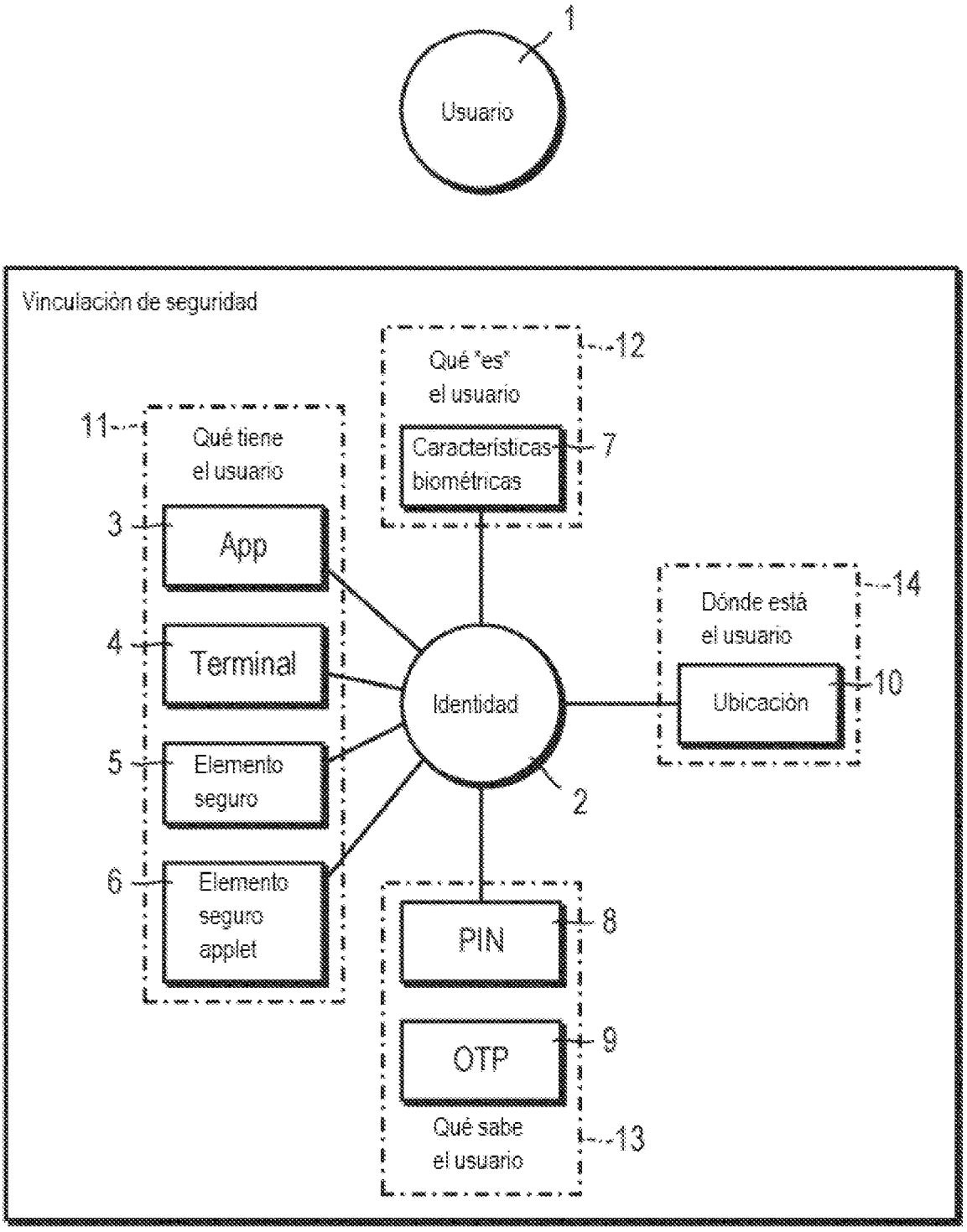

1
Usuario
Vinculación de seguridad
12
Qué "es"
el usuario
Características
biométricas
7
11
Qué tiene
el usuario
3
App
4
Terminal
5
Elemento
seguro
6
Elemento
seguro
applet
Identidad
2
14
Dónde está
el usuario
Ubicación
10
8
PIN
9
OTP
Qué sabe
el usuario
13

Fig. 1

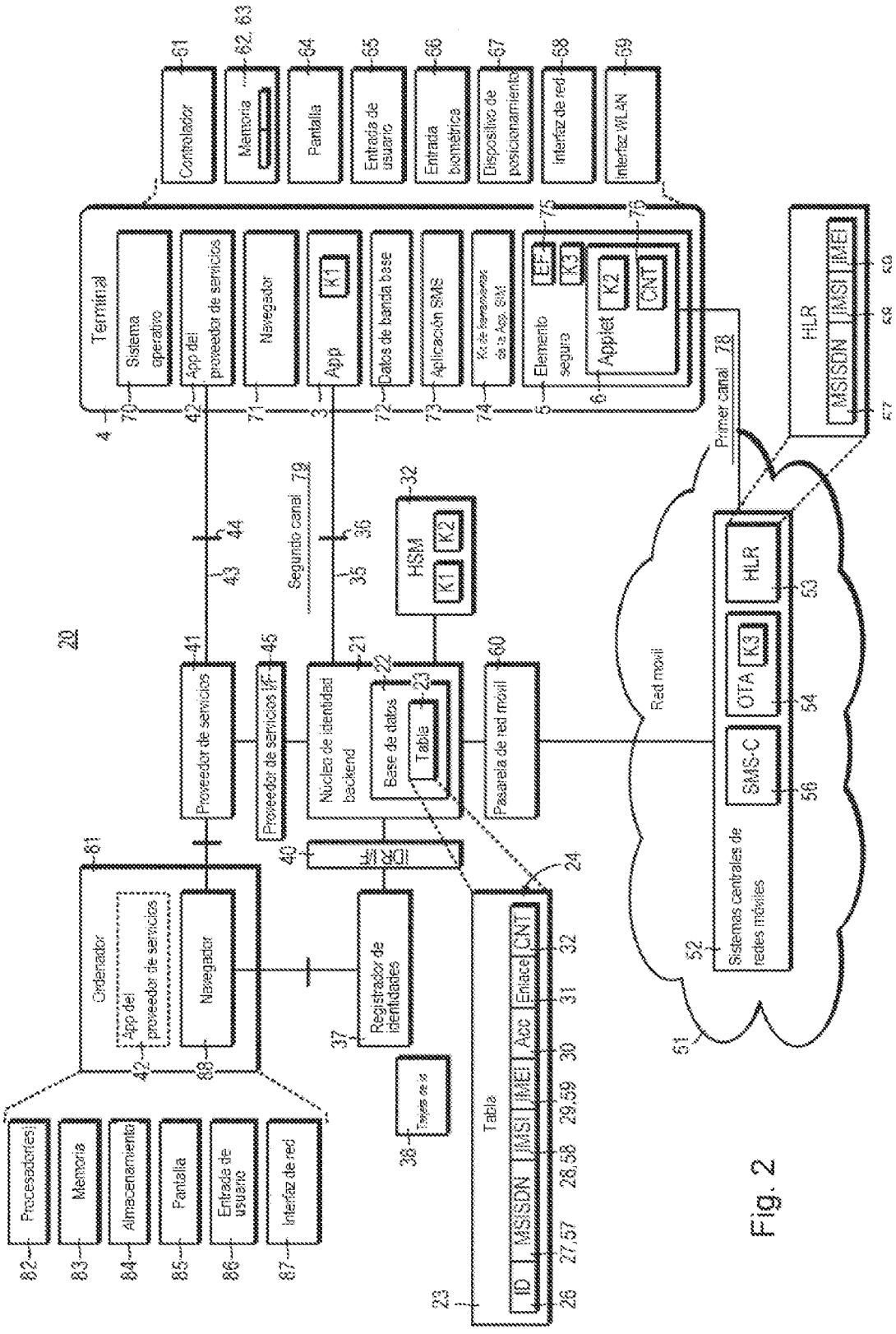
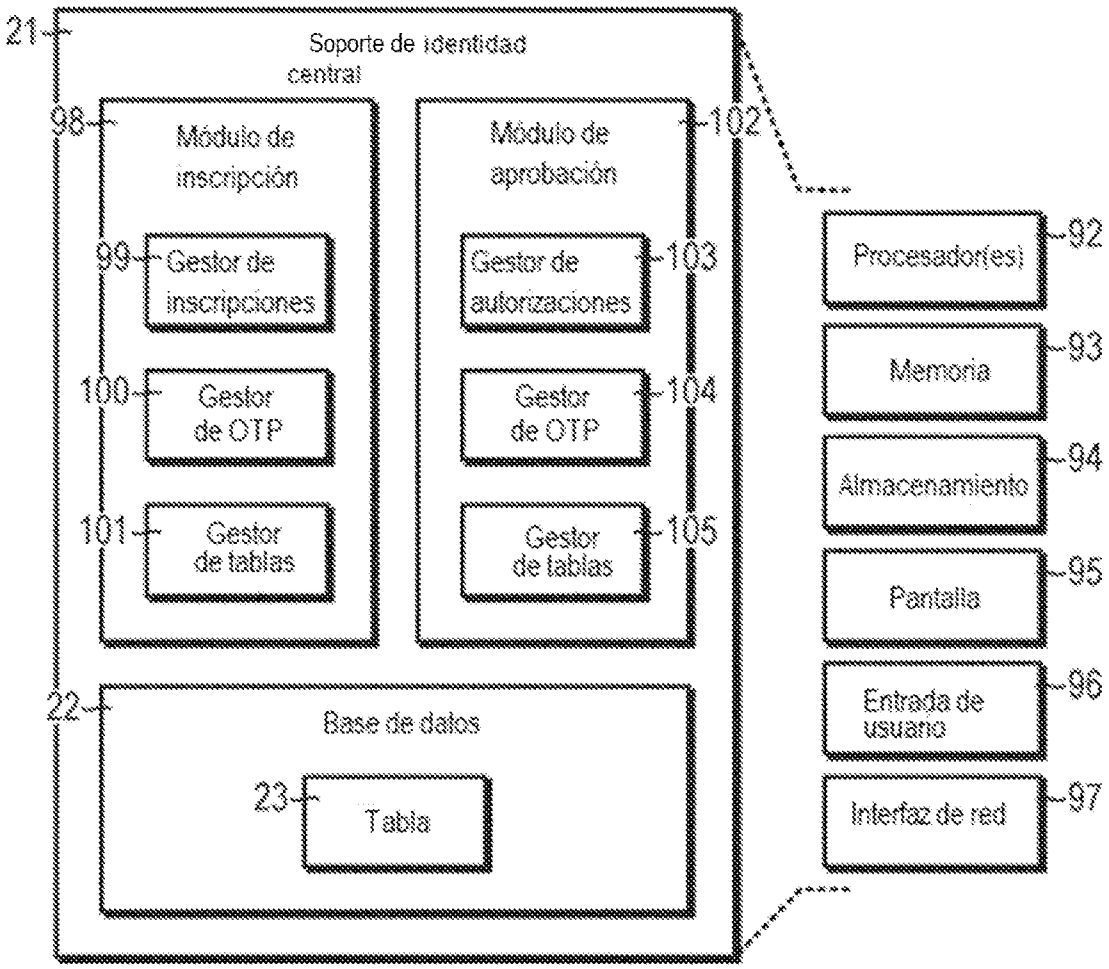

Terminal
Sistema operativo
App del proveedor de servicios
Navegador
App
K1
Datos de banda base
Aplicación SMS
Kit de herramientas de la App. SIM
Elemento seguro
EP
K3
Applet
K2
CNT
Controlador
Memoria
Pantalla
Entrada de usuario
Entrada biométrica
Dispositivo de posicionamiento
Interfaz de red
Interfaz WLAN
Primer canal
Segundo canal
HSM
K1
K2
Proveedor de servicios
Proveedor de servicios IF
Núcleo de identidad backend
Base de datos
Tabla
Pasarela de red móvil
Red móvil
Sistemas centrales de redes móviles
SMS-C
OTA
K3
HLR
MSISDN
IMSI
IMEI
Ordenador
App del proveedor de servicios
Navegador
Registrador de identidades
Procesador(es)
Memoria
Almacenamiento
Pantalla
Entrada de usuario
Interfaz de red
ID
MSISDN
IMSI
IMEI
Acc
Enlace
CNT
Tabla

Fig. 2


21
Soporte de identidad central
98
Módulo de inscripción
99
Gestor de inscripciones
100
Gestor de OTP
101
Gestor de tablas
102
Módulo de aprobación
103
Gestor de autorizaciones
104
Gestor de OTP
105
Gestor de tablas
22
Base de datos
23
Tabla
92
Procesador(es)
93
Memoria
94
Almacenamiento
95
Pantalla
96
Entrada de usuario
97
Interfaz de red

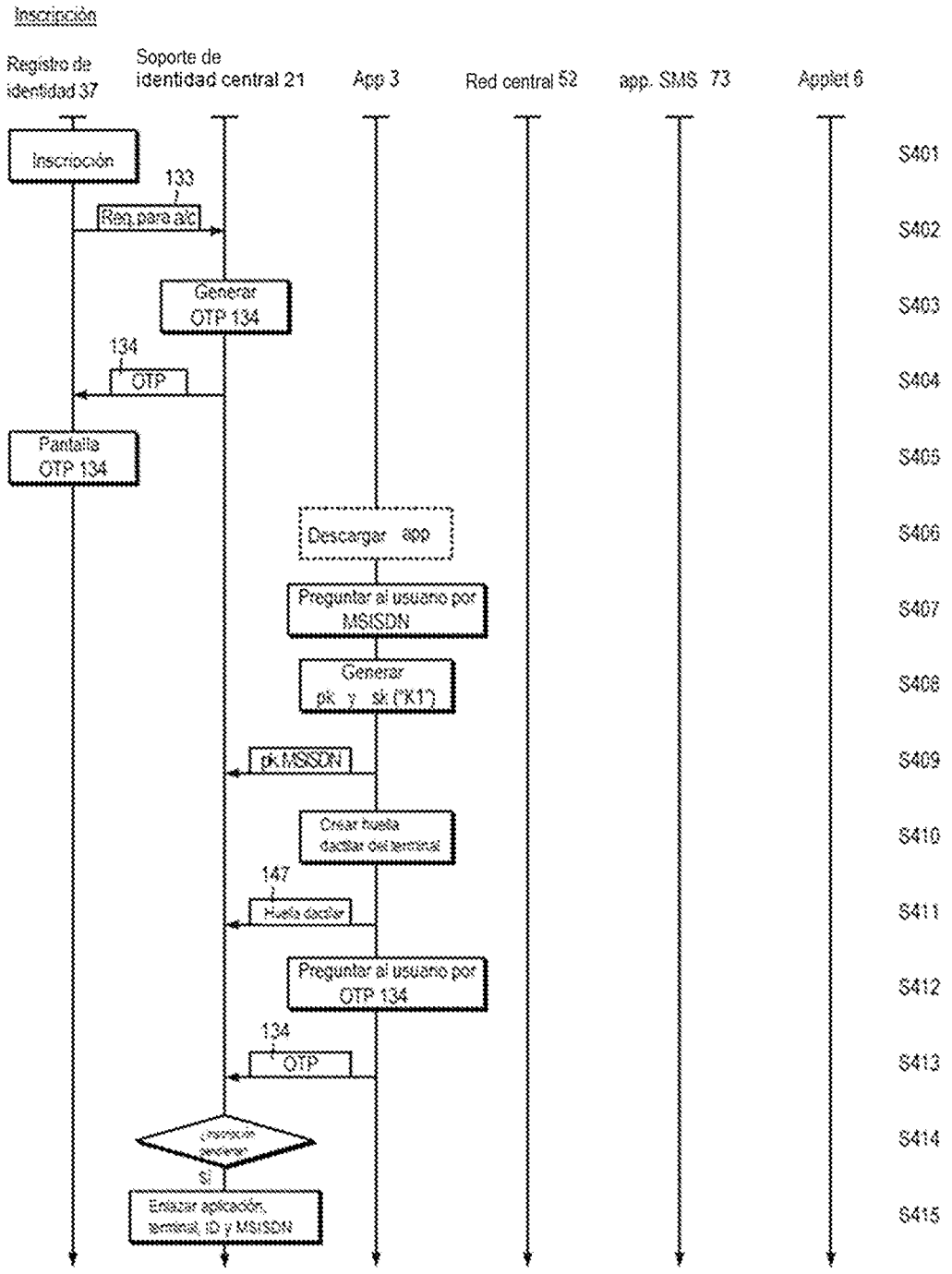

Inscripción
Registro de identidad 37
Soporte de identidad central 21
App 3
Red central 52
app. SMS 73
Applet 6
Inscripción
133
Req para a/c
Generar OTP 134
134
OTP
Pantalla OTP 134
Descargar app
Preguntar al usuario por MSISDN
Generar pk y sk ("K1")
pk MSISDN
Crear huella dactilar del terminal
147
Huella dactilar
Preguntar al usuario por OTP 134
134
OTP
¿Inscripción correcta?
Sí
Enlazar aplicación, terminal, ID y MSISDN
S401
S402
S403
S404
S405
S406
S407
S408
S409
S410
S411
S412
S413
S414
S415

Fig. 4a

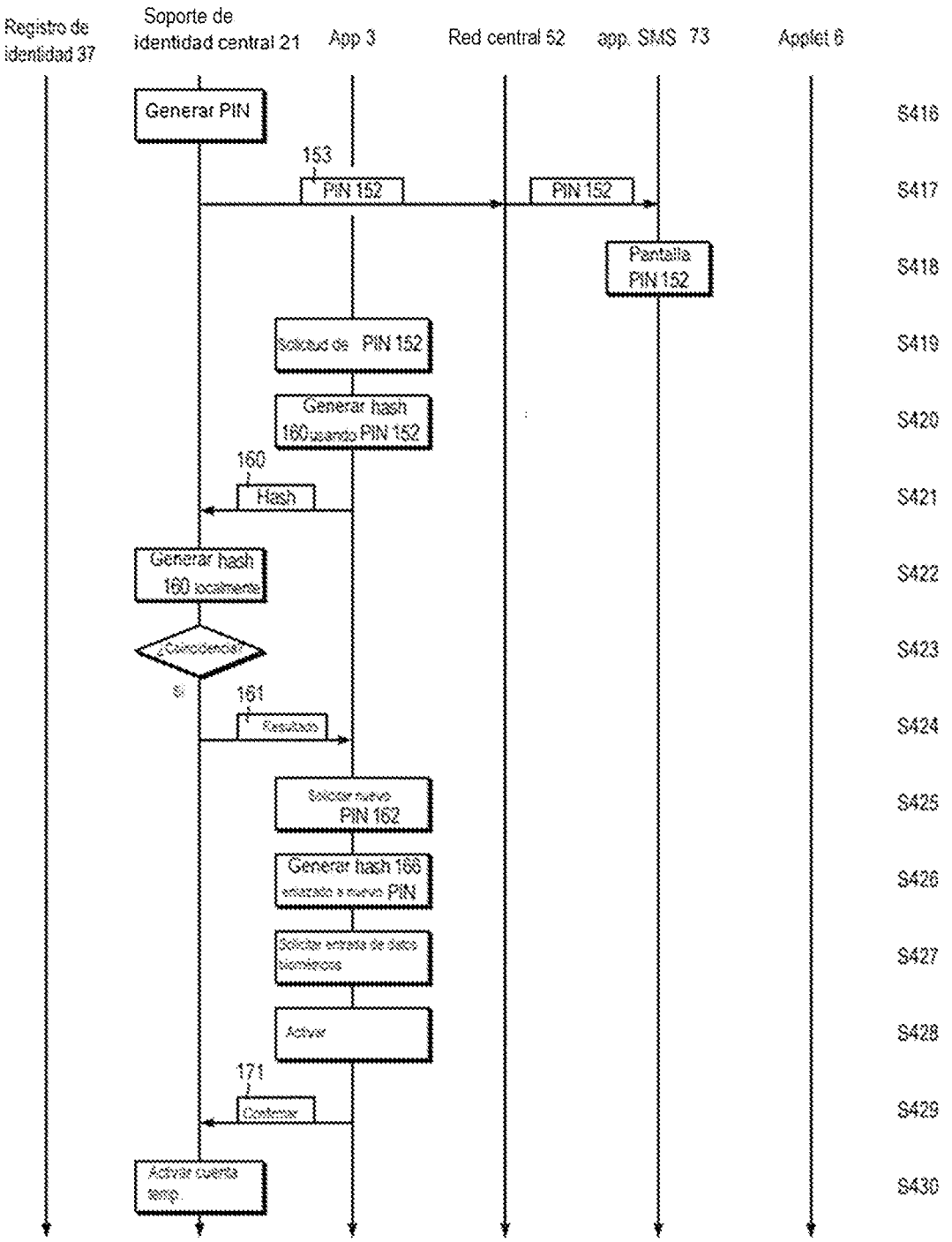

Registro de identidad 37
Soporte de identidad central 21
App 3
Red central 52
app. SMS 73
Applet 6
Generar PIN
153
PIN 152
PIN 152
Pantalla PIN 152
Solicitud de PIN 152
Generar hash 160 usando PIN 152
160
Hash
Generar hash 160 localmente
¿Coincidencia?
Sí
161
Resultado
Solicitar nuevo PIN 152
Generar hash 160 usando nuevo PIN
Solicitar entrada de datos biométricos
Activar
171
Confirmar
Activar cuenta temp.
S416
S417
S418
S419
S420
S421
S422
S423
S424
S425
S426
S427
S428
S429
S430

Fig. 4b

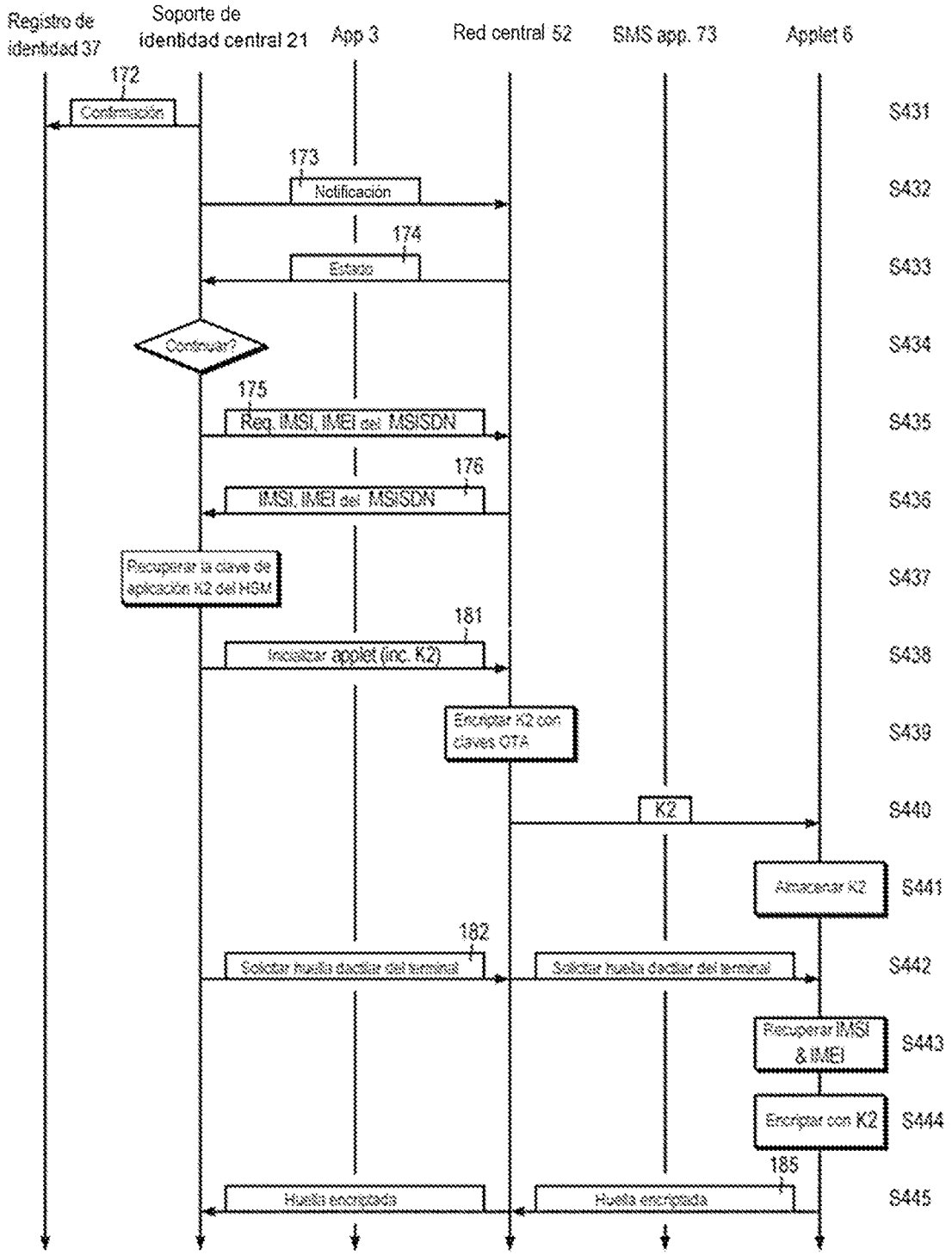

Registro de identidad 37
Soporte de identidad central 21
App 3
Red central 52
SMS app. 73
Applet 6
172
Confirmación
173
Notificación
174
Estado
Continuar?
175
Req. IMSI, IMEI del MSISDN
176
IMSI, IMEI del MSISDN
Recuperar la clave de aplicación K2 del HSM
181
Instalar applet (inc. K2)
Encriptar K2 con claves OTA
K2
Almacenar K2
182
Solicitar huella dactilar del terminal
Solicitar huella dactilar del terminal
Recuperar IMSI & IMEI
Encriptar con K2
185
Huella encriptada
Huella encriptada
S431
S432
S433
S434
S435
S436
S437
S438
S439
S440
S441
S442
S443
S444
S445

Fig. 4c

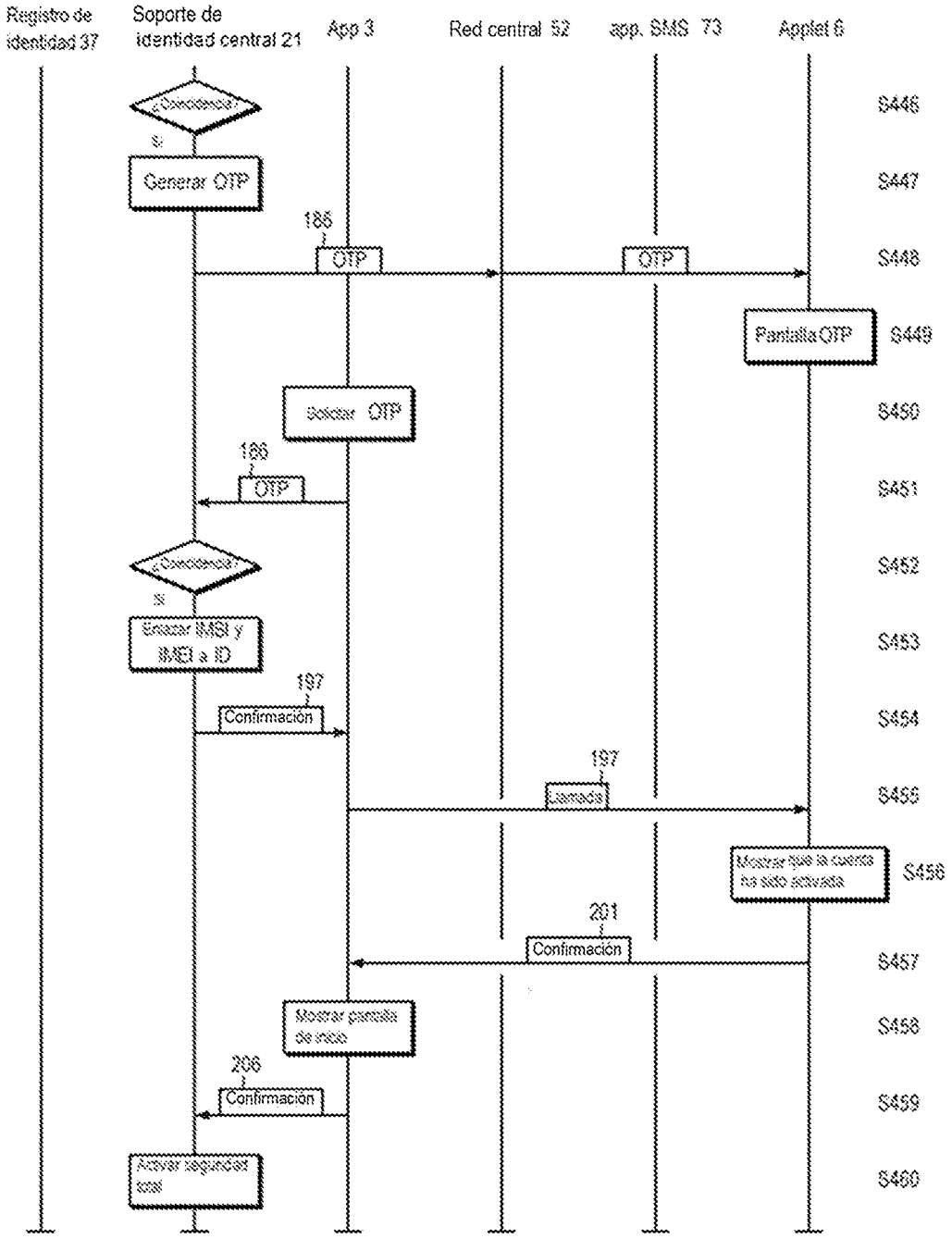

Registro de identidad 37
Soporte de identidad central 21
App 3
Red central 52
app. SMS 73
Applet 6
¿Coincidencia?
Si
Generar OTP
186
OTP
OTP
Pantalla OTP
Solicitar OTP
186
OTP
¿Coincidencia?
Si
Enviar IMSI y IMEI a ID
197
Confirmación
197
Confirmación
Mostrar que la cuenta ha sido activada
201
Confirmación
Mostrar pantalla de inicio
206
Confirmación
Activar seguridad total
S446
S447
S448
S449
S450
S451
S452
S453
S454
S455
S456
S457
S458
S459
S460

Fig. 4d

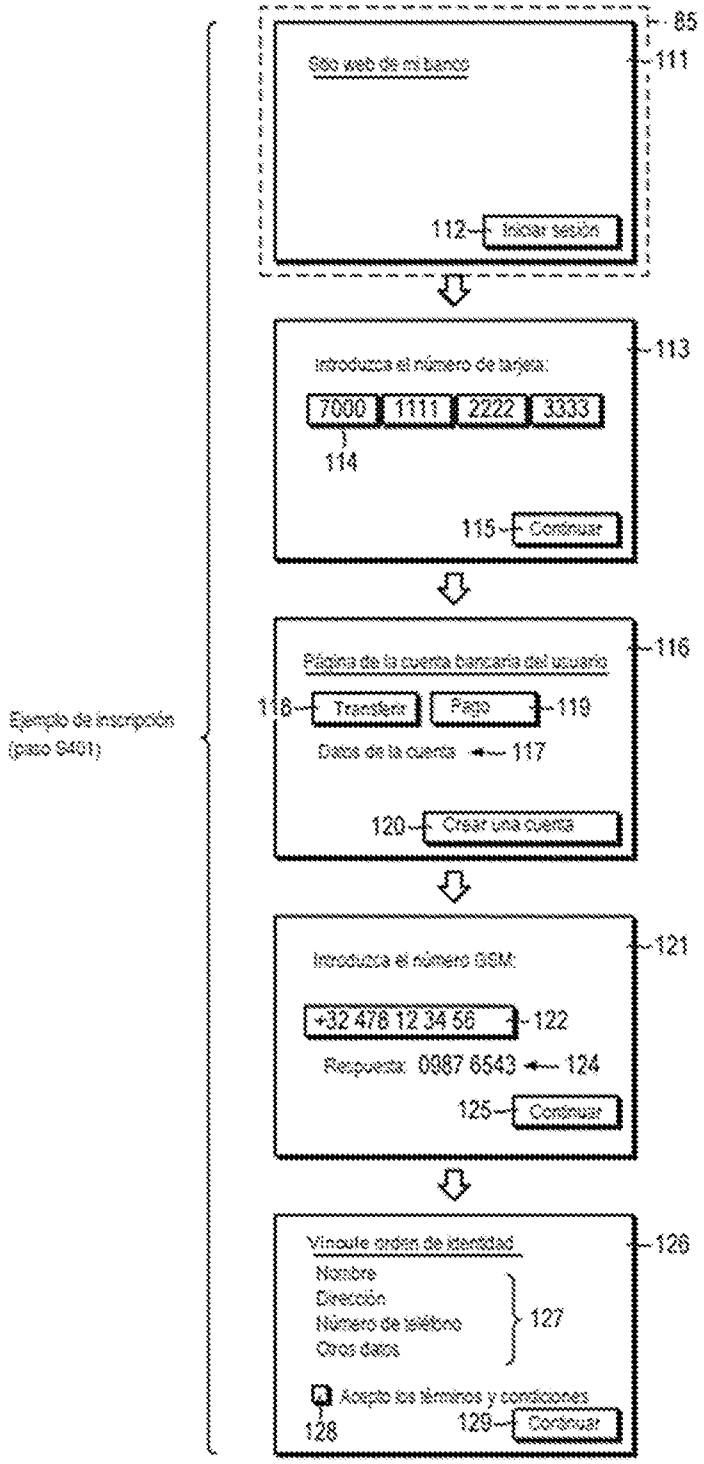

85
Sitio web de mi banco
111
112
Iniciar sesión
Introduzca el número de tarjeta:
7000
1111
2222
3333
113
114
115
Continuar
Página de la cuenta bancaria del usuario
116
118
Transferir
Pago
119
Datos de la cuenta
117
120
Crear una cuenta
Introduzca el número SIM:
121
+32 478 12 34 56
122
Respuesta: 0987 6543
124
125
Continuar
Vincule datos de identidad
126
Nombre
Dirección
Número de teléfono
Otros datos
127
Acepto los términos y condiciones
128
129
Continuar
Ejemplo de inscripción
(paso S401)

Fig. 5

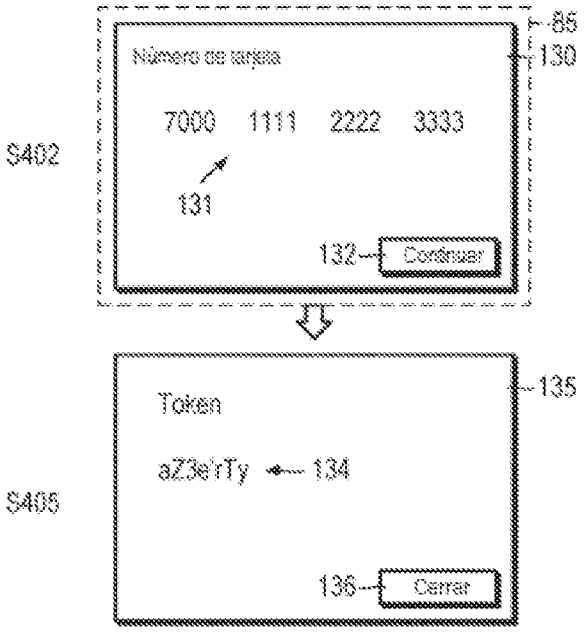

85
130
Número de tarjeta
7000 1111 2222 3333
131
132
Continuar
S402
135
Token
aZ3e'rTy
134
S405
136
Cerrar

Fig. 6

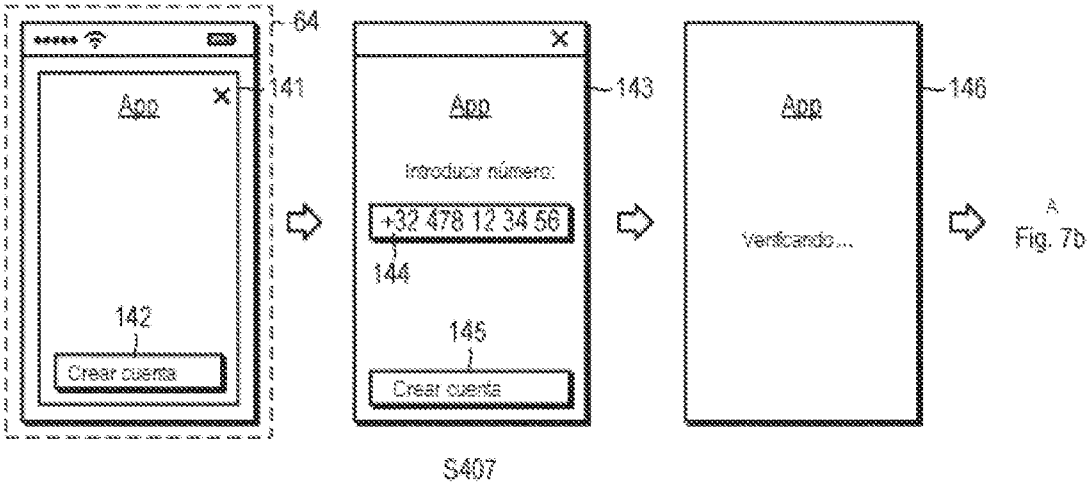

64
141
App
142
Crear cuenta
143
App
Introducir número:
+32 478 12 34 56
144
145
Crear cuenta
146
App
Verificando...
A
Fig. 7b
S407

Fig. 7a

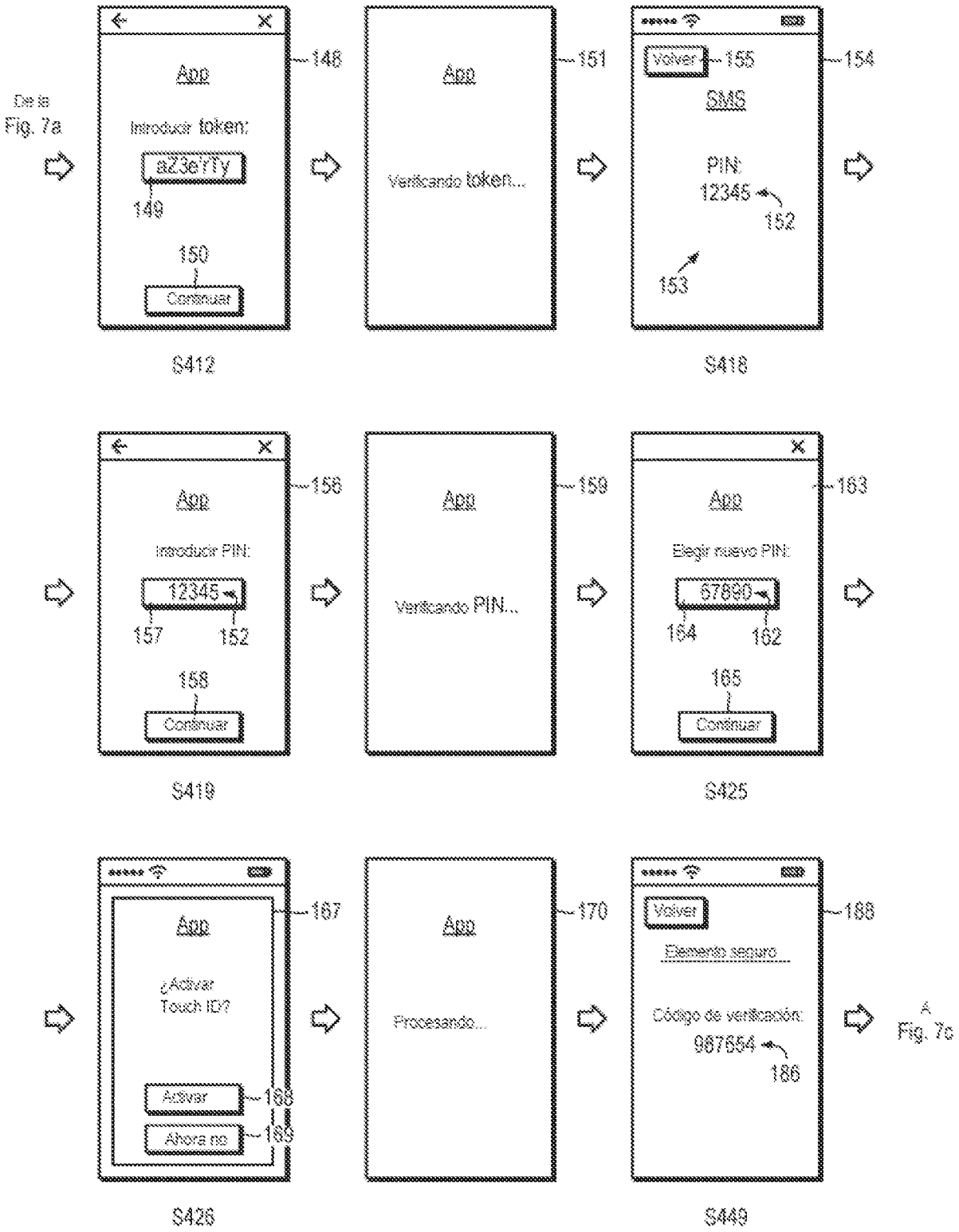

De la Fig. 7a
App
Introducir token:
aZ3eY1y
149
150
Continuar
148
S412
App
Verificando token...
151
App
Volver
155
154
SMS
PIN:
12345
152
153
S418
App
Introducir PIN:
12345
157
152
158
Continuar
156
S419
App
Verificando PIN...
159
App
Elegir nuevo PIN:
67890
164
162
165
Continuar
163
S425
App
¿Activar Touch ID?
Activar
Ahora no
168
169
167
S426
App
Procesando...
170
Volver
Elemento seguro
Código de verificación:
987654
186
188
S449
A
Fig. 7c

Fig. 7b

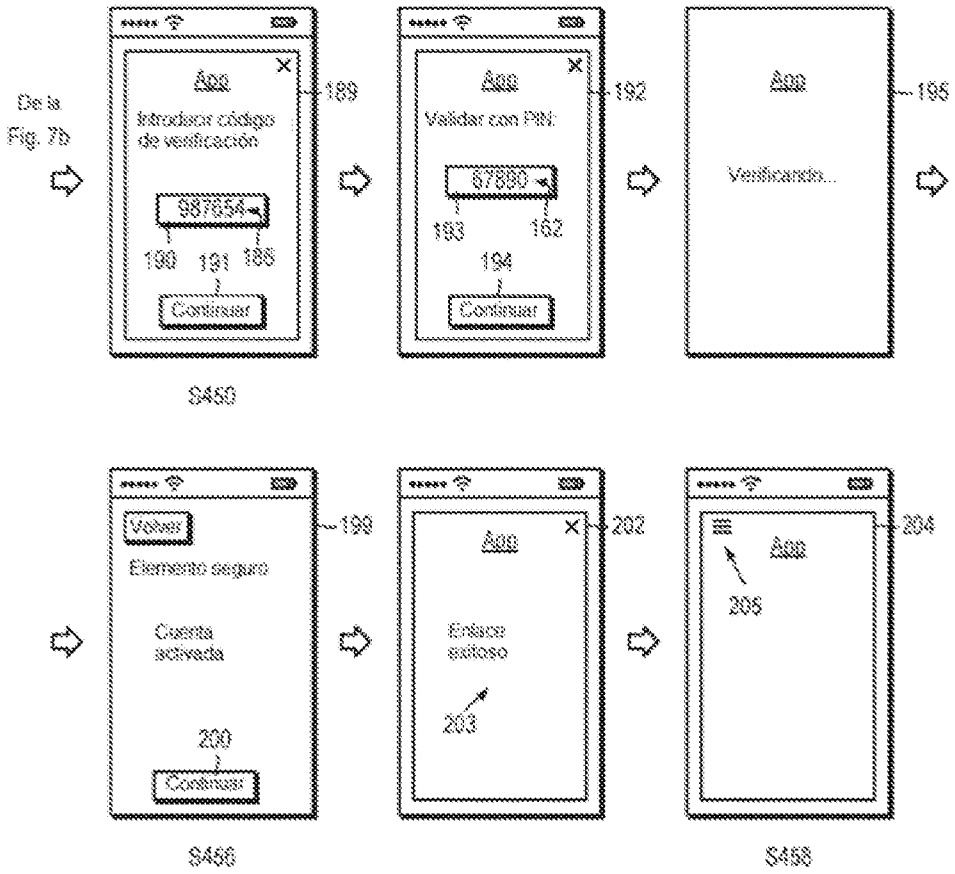

De la Fig. 7b
App
Introducir código de verificación
987654
190
191
186
Continuar
189
S450
App
Validar con PIN:
67890
193
192
194
Continuar
App
Verificando...
195
Volver
Elemento seguro
Cuenta activada
200
Continuar
199
S456
App
Enlace exitoso
203
202
App
205
204
S458

Fig. 7c

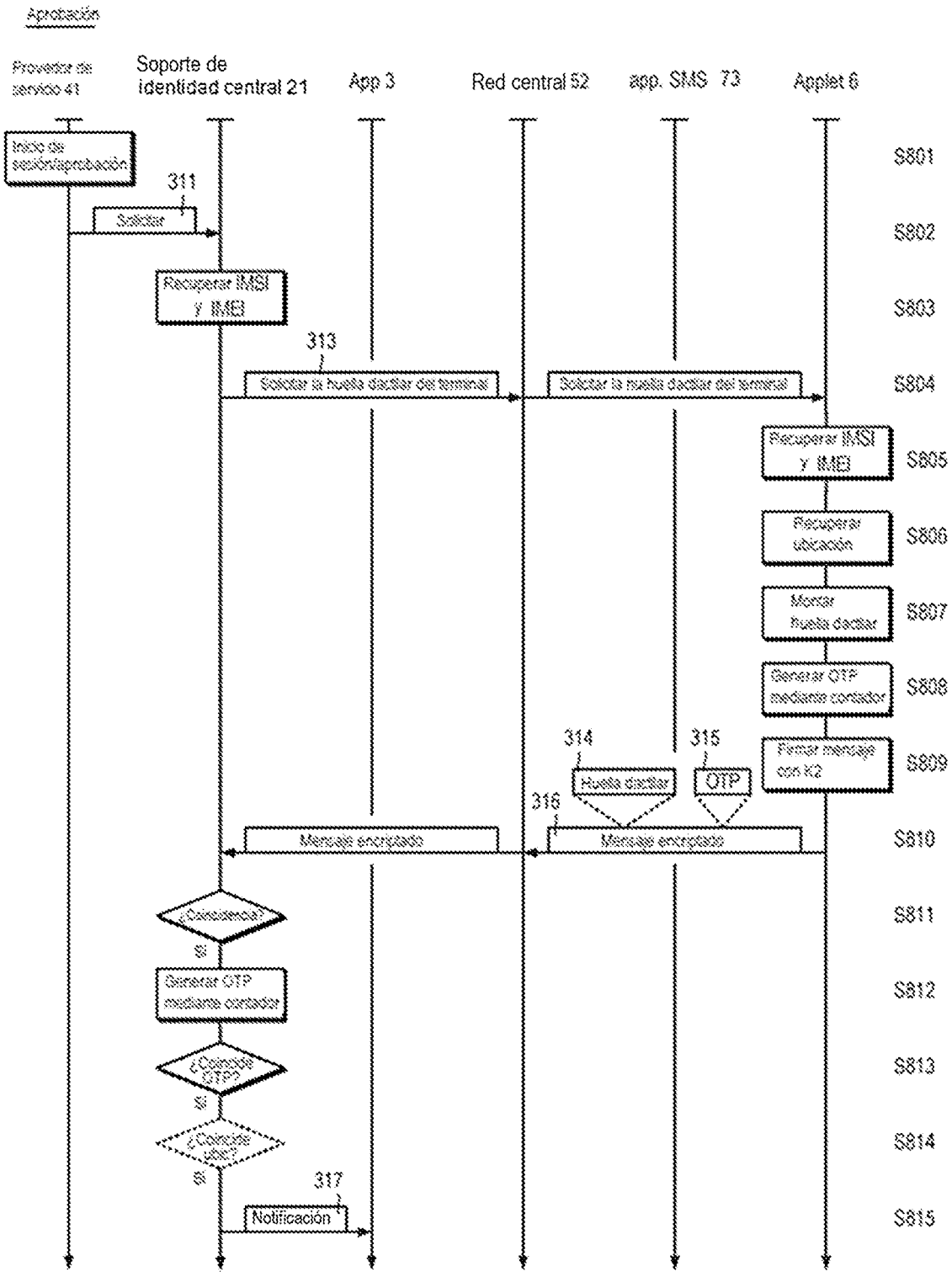

Aprobación
Proveedor de servicio 41
Soporte de identidad central 21
App 3
Red central 52
app. SMS 73
Applet 6
Inicio de sesión/aprobación
311
Solicitar
Recuperar IMSI y IMEI
313
Solicitar la huella dactilar del terminal
Solicitar la huella dactilar del terminal
Recuperar IMSI y IMEI
Recuperar ubicación
Mostrar huella dactilar
Generar OTP mediante contador
Formar mensaje con K2
314
Huella dactilar
315
OTP
316
Mensaje encriptado
Mensaje encriptado
¿Coincide?
SI
Generar OTP mediante contador
¿Coincide OTP?
SI
¿Coincide IMEI?
SI
317
Notificación
S801
S802
S803
S804
S805
S806
S807
S808
S809
S810
S811
S812
S813
S814
S815

Fig. 8a

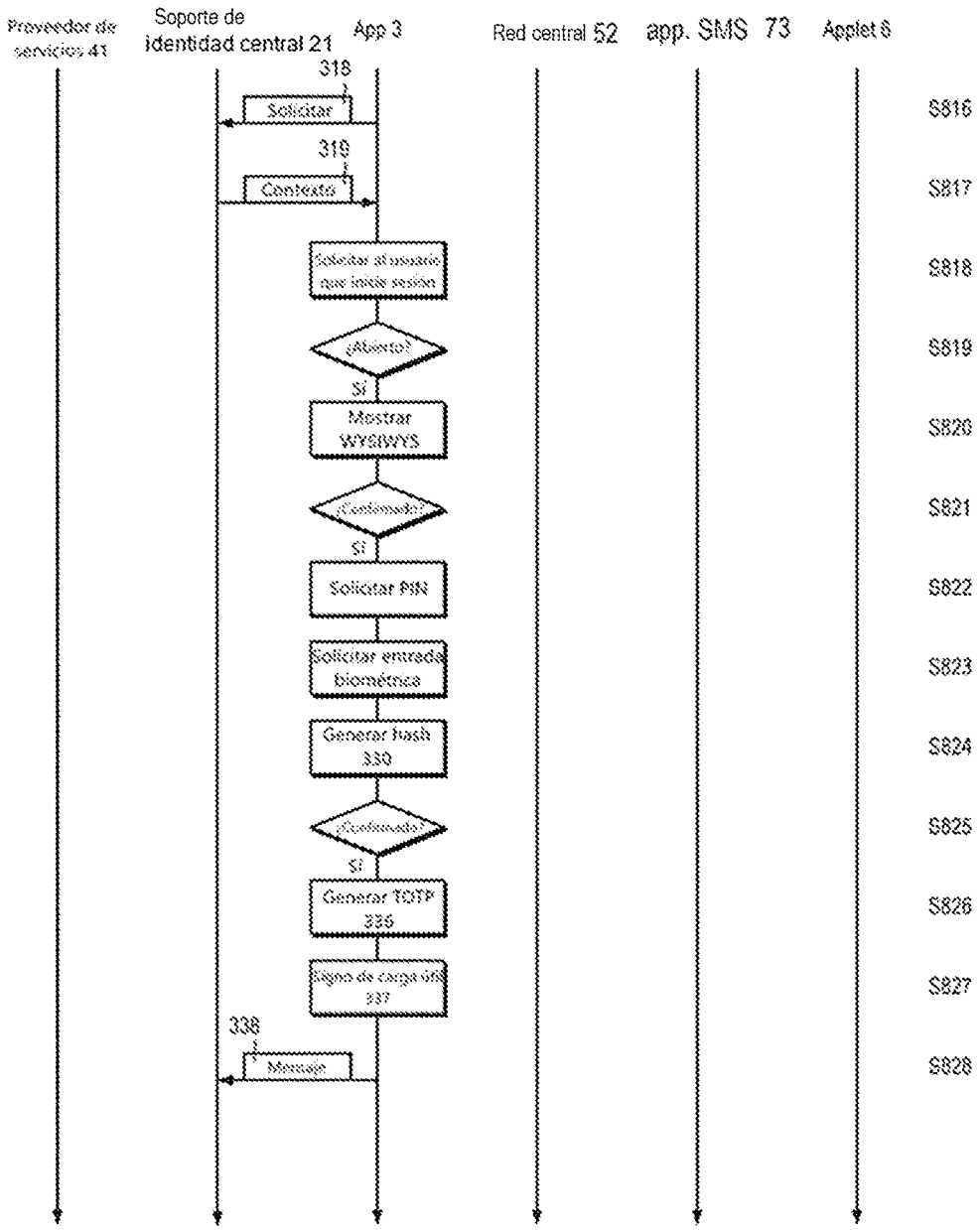

Proveedor de servicios 41
Soporte de identidad central 21
App 3
Red central 52
app. SMS 73
Applet 8
318
Solicitar
319
Contexto
Solicitar al usuario que inicie sesión
¿Abierto?
Sí
Mostrar WYSIWYS
¿Confirmado?
Sí
Solicitar PIN
Solicitar entrada biométrica
Generar hash 330
¿Confirmado?
Sí
Generar TOTP 335
Signo de carga útil 337
338
Mensaje
S816
S817
S818
S819
S820
S821
S822
S823
S824
S825
S826
S827
S828

Fig. 8b

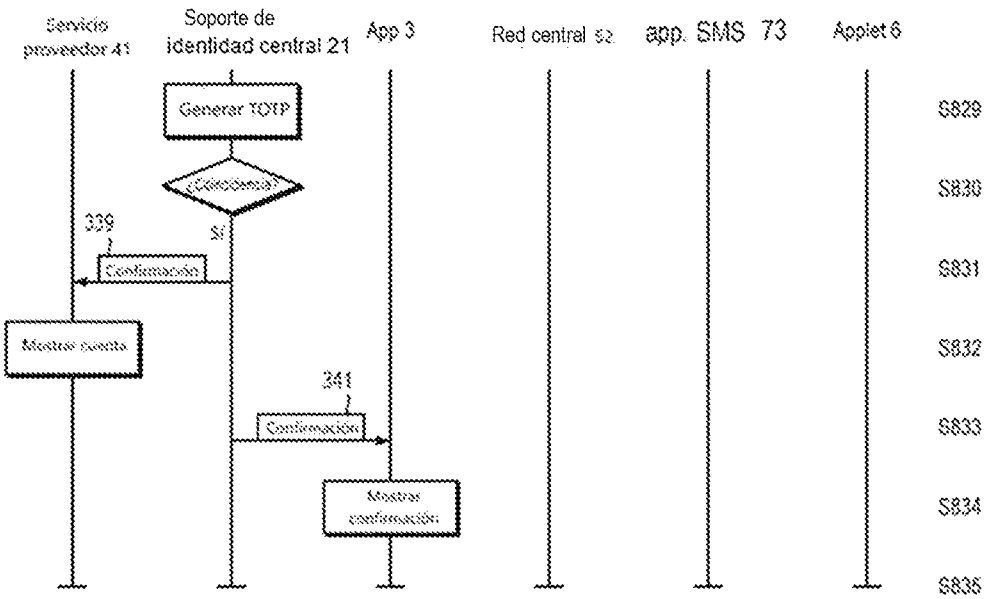

Servicio proveedor 41
Soporte de identidad central 21
App 3
Red central 52
app. SMS 73
Applet 6
Generar TOTP
¿Coincidencia?
339
SI
Confirmación
Mostrar cuenta
341
Confirmación
Mostrar confirmación
S829
S830
S831
S832
S833
S834
S835

Fig. 8c

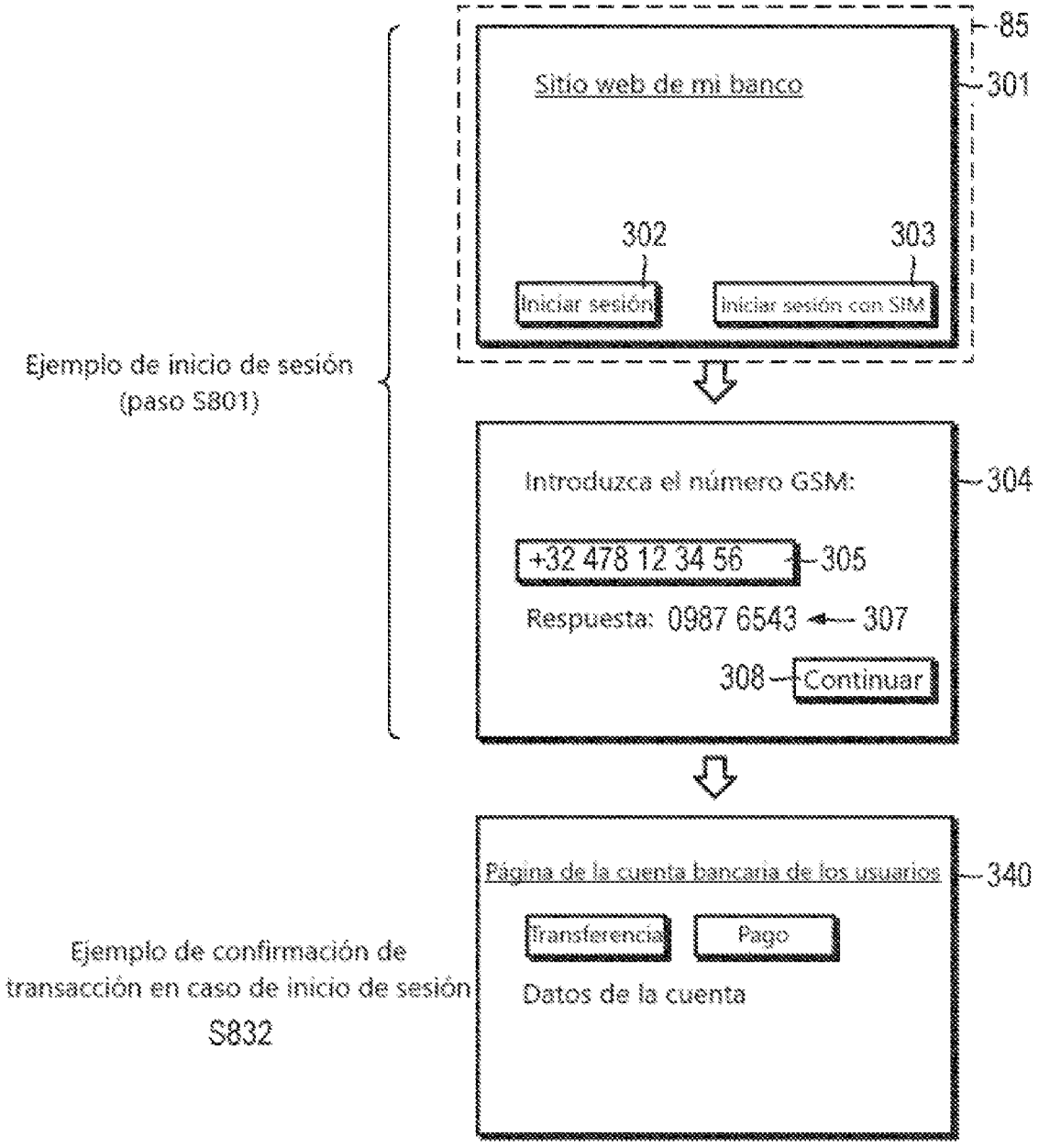

Ejemplo de inicio de sesión
(paso S801)
85
301
Sitio web de mi banco
302
303
Iniciar sesión
Iniciar sesión con SIM
Introduzca el número GSM:
304
+32 478 12 34 56
305
Respuesta: 0987 6543
307
308
Continuar
Ejemplo de confirmación de
transacción en caso de inicio de sesión
S832
Página de la cuenta bancaria de los usuarios
340
Transferencia
Pago
Datos de la cuenta

Fig. 9

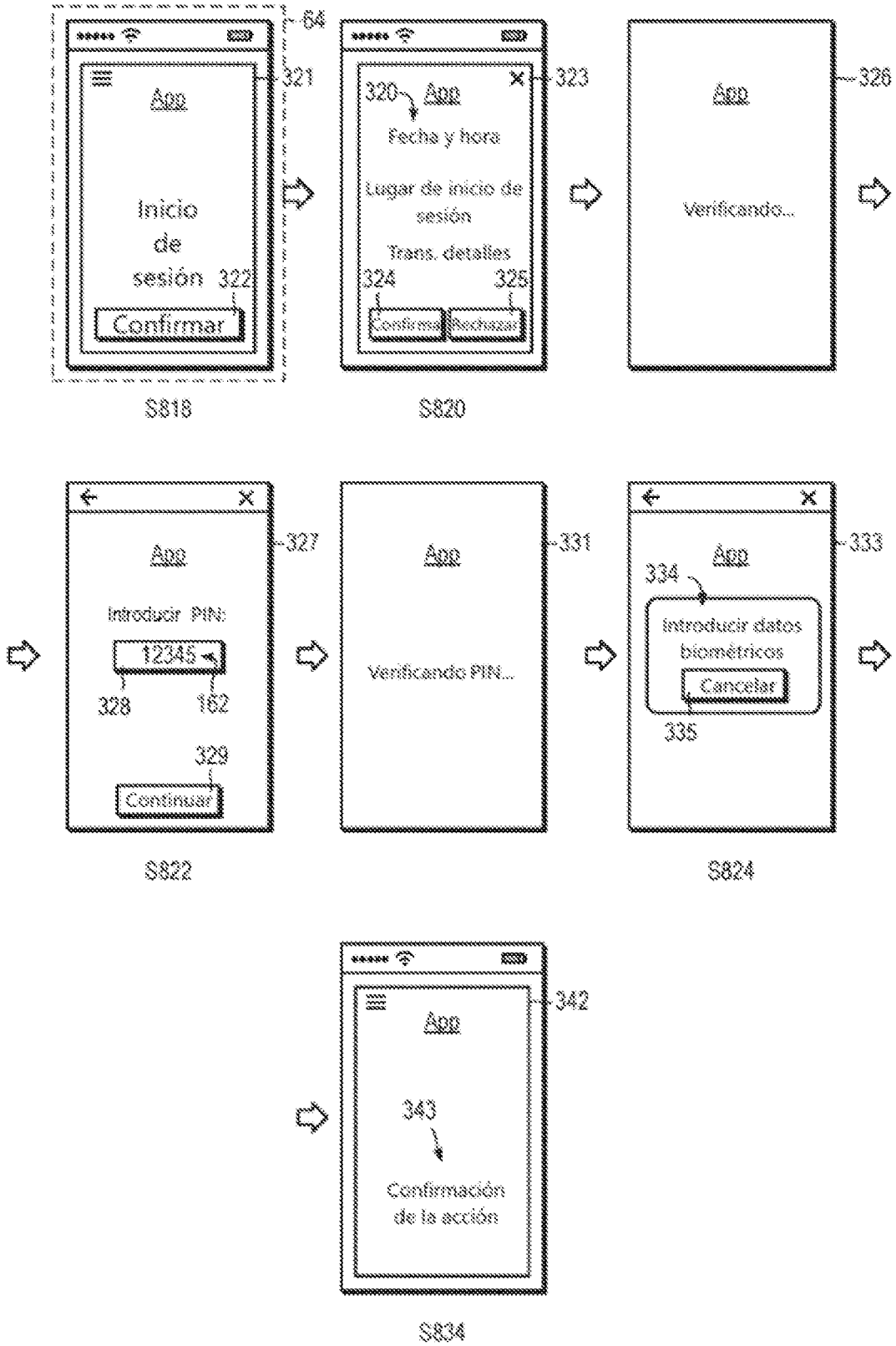

64
App
321
Inicio de sesión
322
Confirmar
S818
320
App
323
Fecha y hora
Lugar de inicio de sesión
Trans. detalles
324
325
Confirmar
Rechazar
S820
App
326
Verificando...
App
327
Introducir PIN:
12345
328
162
329
Continuar
S822
App
331
Verificando PIN...
App
333
334
Introducir datos biométricos
Cancelar
335
S824
App
342
343
Confirmación de la acción
S834

Fig. 10