(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 799 420**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/06 (2009.01)
H04W 4/021 (2008.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **20.05.2012 PCT/US2012/038745**

(87) Fecha y número de publicación internacional: **25.04.2013 WO13058832**

(96) Fecha de presentación y número de la solicitud europea: **20.05.2012 E 12725956 (2)**

(97) Fecha y número de publicación de la concesión europea: **22.04.2020 EP 2716095**

(54) Título: **Red móvil**

(30) Prioridad:

03.06.2011 US 201113153290

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.12.2020

(73) Titular/es:

THE BOEING COMPANY (100.0%)
100 North Riverside Plaza
Chicago, IL 60606-1596, US

(72) Inventor/es:

WEN, FANG

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Red móvil

Antecedentes

El documento US2007/0143837A1 describe que un sistema de acceso remoto seguro incluye software de cliente instalado en un ordenador portátil que establece una sesión remota con un software de servidor homólogo instalado en un servidor en un DMZ de la red interna de la compañía a través de una conexión segura. El servidor de DMZ se conecta a un rúter tras un cortafuegos de segundo nivel de la compañía. El rúter enruta la sesión al ordenador de escritorio apropiado si al ordenador de escritorio se le permite un acceso remoto.

El documento EP2302865A1 describe un servidor de autenticación y un método para controlar un acceso de terminal de comunicación móvil a una red privada virtual (VPN). El servidor de autenticación comprende un primer módulo de almacenamiento configurado para almacenar una primera información característica del terminal de comunicación móvil al que se le permite el acceso; un módulo de recepción configurado para recibir un mensaje de solicitud de acceso de VPN procedente del terminal para el acceso; un módulo de evaluación configurado para evaluar el tipo del terminal para el acceso y obtener un resultado de evaluación.

El documento US2009/0100514A1 describe que se proporciona un método para una conexión de nodo móvil a una red privada virtual usando una IP móvil en un entorno móvil. Según este método, en primer lugar, el nodo móvil realiza un mensaje de solicitud de registro de IP móvil que incluye información de autenticación de usuario de VPN y transmite el mensaje a la puerta de acceso de VPN. A continuación, la puerta de acceso de VPN lee la información de autenticación de usuario de VPN procedente del mensaje y consulta una base de datos en la que la información de autenticación de usuario de VPN ya se encuentra almacenada, para verificar una autorización de acceso de VPN del nodo móvil. Si la autorización de acceso se verifica, la IP privada se graba en un mensaje de respuesta al mensaje de solicitud de registro de IP móvil, y el mensaje de respuesta se transmite al nodo móvil para asignar la IP privada.

Sumario

En un aspecto se proporciona un método tal como se define en la reivindicación adjunta 1.

En otro aspecto se proporciona un dispositivo móvil tal como se define en la reivindicación adjunta 11.

En una o más realizaciones, el identificador de dispositivo móvil se comunica con la red segura por medio de una red celular, una red Wi-Fi, y/o una red de fuera de banda. En algunas realizaciones, el método implica, además, enviar, con el gestor de dispositivo móvil, una solicitud para el identificador de dispositivo móvil. En una o más realizaciones, el identificador de dispositivo móvil es una dirección de protocolo de Internet (IP). En al menos una realización, el identificador de dispositivo móvil es un código de identificación (ID) único.

En una o más realizaciones, el método implica, además, verificar y/o validar, con el gestor de dispositivo móvil, un usuario del dispositivo móvil. En al menos una realización, el usuario del dispositivo móvil se verifica y/o valida usando biométricas del usuario. En algunas realizaciones, el usuario del dispositivo móvil y/o el propio dispositivo móvil se verifica y/o valida analizando y/o determinando la ubicación del dispositivo móvil.

En al menos una realización, el método implica, además, recibir, con el dispositivo móvil, datos seguros encriptados procedentes de la red segura. Además, el método implica desencriptar, con el dispositivo móvil, los datos seguros encriptados recibidos usando un software de seguridad de dispositivo móvil descargado previamente. En al menos una realización, el software de seguridad de dispositivo móvil descargado previamente se usa para desencriptar datos seguros encriptados y/o encriptar datos no seguros. En una o más realizaciones, el método implica, además, encriptar, con el dispositivo móvil, datos no seguros usando el software de seguridad de dispositivo móvil descargado previamente; y transmitir, con el dispositivo móvil, los datos encriptados a la red segura. En al menos una realización, el software de seguridad de dispositivo móvil comprende software de encriptación, software de desencriptación, y/o software de direccionamiento de destino fijo forzado.

En una o más realizaciones, un dispositivo móvil no seguro que funciona en una red no segura usada para establecer comunicaciones con una red segura implica un transmisor, un receptor, y un procesador. El transmisor está configurado para comunicar un identificador de dispositivo móvil a la red segura, y el receptor está configurado para recibir datos seguros encriptados procedentes de la red segura. Adicionalmente, el procesador está configurado para desencriptar los datos seguros encriptados recibidos usando el software de seguridad de dispositivo móvil descargado previamente. En al menos una realización, el procesador está configurado adicionalmente para encriptar datos no seguros usando el software de seguridad de dispositivo móvil descargado previamente, y el transmisor está configurado adicionalmente para transmitir los datos encriptados a la red segura.

En al menos una realización, un método para establecer comunicaciones con una red segura usando un dispositivo móvil no seguro que funciona en una red no segura implica comunicar un identificador de dispositivo móvil a la red segura para establecer una conexión segura entre el dispositivo móvil y la red segura. El método implica, además,

establecer una conexión segura entre el dispositivo móvil y la red segura. Asimismo, el método implica recibir, con el dispositivo móvil, datos seguros encriptados procedentes de la red segura. Adicionalmente, el método implica desencriptar, con el dispositivo móvil, los datos seguros encriptados recibidos usando el software de seguridad de dispositivo móvil descargado previamente.

En una o más realizaciones, un método para establecer comunicaciones con una red segura usando un dispositivo móvil no seguro que funciona en una red no segura implica recibir, con un receptor, una solicitud con un identificador de dispositivo móvil procedente del dispositivo móvil para establecer una conexión segura entre el dispositivo móvil y la red segura. El método implica, además, verificar y/o validar, con un gestor de dispositivo móvil en la red segura, el identificador de dispositivo móvil. Adicionalmente, el método implica establecer una conexión segura entre el dispositivo móvil y la red segura. Además, el método implica transmitir, con un transmisor, datos seguros encriptados procedentes de la red segura al dispositivo móvil. En al menos una realización, el dispositivo móvil funciona en una red celular segura o no segura y/o una red Wi-Fi segura o no segura. En algunas realizaciones, el método implica, además, recibir, con el receptor, datos encriptados transmitidos procedentes del dispositivo móvil; y desencriptar, con un procesador, los datos encriptados recibidos.

En al menos una realización, un método para permitir el establecimiento de comunicaciones con una red segura usando un dispositivo móvil no seguro que funciona en una red no segura implica comunicar una solicitud a la red segura para descargar el software de seguridad de dispositivo móvil. El método implica, además, descargar e instalar, mediante el dispositivo móvil, el software de seguridad de dispositivo móvil de la red segura. Asimismo, el método implica activar, mediante el dispositivo móvil, el software de seguridad de dispositivo móvil.

Adicionalmente, el método implica transmitir, con el dispositivo móvil, una solicitud de registro de gestor de dispositivo móvil a la red segura. Asimismo, el método implica verificar y/o validar, con el gestor de dispositivo móvil, el dispositivo móvil basándose en una descripción de elemento de datos única (UDID) del dispositivo móvil, Además, el método implica transmitir, mediante el gestor de dispositivo móvil, un identificador de dispositivo móvil al dispositivo móvil. El identificador de dispositivo móvil permite que el dispositivo móvil establezca comunicaciones con la red segura.

En algunas realizaciones, el método implica, además, incluir, con el gestor de dispositivo móvil, el número de teléfono del dispositivo móvil en una lista de acceso de operador, en la que las transmisiones de datos encriptados posteriores procedentes de dispositivos móviles que tienen sus números de teléfono en la lista de acceso de operador se enrutarán de manera automática a la red segura.

Las características, funciones, y ventajas se lograrán de manera independiente en diversas realizaciones de las presentes invenciones o pueden combinarse en todavía otras realizaciones.

Breve descripción de dibujos

Estas y otras características, aspectos, y ventajas de la presente divulgación se comprenderán mejor con respecto a la siguiente descripción, reivindicaciones adjuntas, y dibujos adjuntos en los que:

La figura 1 muestra un diagrama arquitectónico de un sistema para establecer comunicaciones con una red segura usando un dispositivo móvil no seguro que funciona en una red no segura, según al menos una realización de la presente divulgación.

La figura 2 muestra un diagrama de flujo para el funcionamiento del sistema representado en la figura 1, según al menos una realización de la presente divulgación.

Las figuras 3A y 3B muestran los procedimientos para un dispositivo móvil no seguro para obtener software de seguridad de dispositivo móvil y un identificador de dispositivo móvil, según al menos una realización de la presente divulgación.

La figura 3A muestra un diagrama de un dispositivo móvil no seguro que descarga, instala, y activa software de seguridad de dispositivo móvil, según al menos una realización de la presente divulgación.

La figura 3B muestra un diagrama de un dispositivo móvil no seguro que transmite una solicitud de registro de gestor de dispositivo móvil y que recibe un identificador de dispositivo móvil, según al menos una realización de la presente divulgación.

La figura 4 muestra un diagrama de flujo para los procedimientos ilustrados en las figuras 3A y 3B, según al menos una realización de la presente divulgación.

Descripción detallada

Los métodos y el aparato dados a conocer en el presente documento proporcionan un sistema operativo para establecer comunicaciones con una red segura. Específicamente, este sistema se refiere a establecer comunicaciones con una red segura usando un dispositivo móvil no seguro que funciona en una red no segura. En particular, la presente divulgación enseña una manera por la que un dispositivo móvil no seguro, tal como un

asistente digital personal (PDA), acceda a una red segura. En la actualidad, las PDA comercialmente disponibles (por ejemplo, iPhones y iPads) no presentan una arquitectura de seguridad para proteger los datos del propietario. La presente divulgación proporciona un sistema que permite que dispositivos móviles no seguros comercialmente disponibles para la venta que funcionan en una red no segura puedan tener acceso a redes seguras. Para al menos una aplicación de la presente divulgación, soldados desplegados en el campo usan dispositivos móviles no seguros disponibles para la venta que emplean el sistema dado a conocer con el fin de transmitir y recibir datos a y de una red segura. Para algunas aplicaciones, los soldados usan dispositivos móviles no seguros disponibles para la venta que emplean el sistema dado a conocer para poder obtener unas comunicaciones seguras entre sí.

En la siguiente descripción, se exponen numerosos detalles con el fin de proporcionar una descripción más exhaustiva del sistema. Sin embargo, resultará evidente para un experto en la técnica que el sistema dado a conocer puede llevarse a la práctica sin estos detalles específicos. En los otros casos, no se han descrito en detalle características que se conocen bien para no enmascarar de manera innecesaria el sistema.

La figura 1 muestra un diagrama arquitectónico de un sistema 100 para establecer comunicaciones con una red segura usando un dispositivo 105 móvil no seguro que funciona en una red no segura, según al menos una realización de la presente divulgación. En esta figura, se descarga software de seguridad de dispositivo móvil en el dispositivo 105 móvil. El software de seguridad de dispositivo móvil puede usarse para desencriptar datos seguros encriptados y/o encriptar datos no seguros y/o hacer que datos se destinen a direcciones específicas, incluyendo las direcciones de la zona desmilitarizada (DMZ) o red segura. Los detalles del procedimiento de instalación para el software de seguridad de dispositivo móvil se presentan en las discusiones de las figuras 3A, 3B, y 4.

En la figura 1, durante el funcionamiento del sistema 100, en primer lugar, el dispositivo 105 móvil no seguro transmite un identificador de dispositivo móvil a la red segura. En al menos una realización, el dispositivo 105 móvil transmite el identificador de dispositivo móvil a la red segura usando una conexión 110 celular de datos/voz no segura (por ejemplo, una conexión celular de 3G/4G). Al hacerlo, el dispositivo 105 móvil transmite el identificador de dispositivo móvil al servidor 115 de autenticación de la red segura por medio de una torre 120 celular. Debe observarse que, para estas realizaciones, el dispositivo 105 móvil también puede realizar llamadas 122 no seguras usando la conexión 110 celular de voz por medio de una torre 120 celular.

En algunas realizaciones, el dispositivo 105 móvil transmite el identificador de dispositivo móvil a la red segura a través de una conexión 123 de Wi-Fi no segura. Para estas realizaciones, el dispositivo 105 móvil transmite el identificador de dispositivo móvil al servidor 115 de autenticación por medio de un punto 125 de acceso Wi-Fi. Debe observarse que, en otras realizaciones, el dispositivo 105 móvil puede usar diversos medios de comunicación distintos a una conexión celular o a una conexión Wi-Fi para comunicar el identificador de dispositivo móvil fuera de banda con el servidor 115 de autenticación y/o el gestor 130 de dispositivo móvil de la red segura. Un ejemplo de esto es cuando el usuario de dispositivo móvil usa un teléfono diferente para realizar una llamada a un operario de servicio técnico, autentifica él mismo o ella misma al operario de servicio técnico, le dice al operario de servicio técnico el identificador de dispositivo móvil, y hace que el operario de servicio técnico introduzca el identificador de dispositivo móvil en el gestor 130 de dispositivo móvil y/o el servidor 115 de autenticación. Alternativamente, el usuario de dispositivo móvil puede acceder a la red segura a través de un sistema remoto diferente, se autentifica a sí mismo o a sí misma en ese sistema, y entonces introduce el identificador de dispositivo móvil en el gestor 130 de dispositivo móvil y/o el servidor 115 de autenticación.

El identificador de dispositivo móvil proporciona medios para la red segura para identificar y verificar el dispositivo 105 móvil. En una o más realizaciones, el identificador de dispositivo móvil es una dirección de protocolo de Internet (IP), un código de identificación (ID) único, o una combinación de ambos, una dirección IP y un código ID único, tal como un dispositivo identificador seguro o un número de teléfono. En otras realizaciones, el identificador de dispositivo móvil es o incluye un número aleatorio que se genera mediante un algoritmo generador de número aleatorio que está contenido en el software de seguridad de dispositivo móvil descargado previamente. En algunas realizaciones, el número aleatorio cambia de manera periódica, tal como cuando el dispositivo 105 móvil se mueve, a intervalos de tiempo específicos, y/o entre llamadas telefónicas. En al menos una realización, el número aleatorio cambia de números aleatorios válidos a números aleatorios falsos con el fin de confundir cualquier posible escucha no autorizada.

Después de que el servidor 115 de autenticación reciba el identificador de dispositivo móvil, el servidor 115 de autenticación transmite el identificador de dispositivo móvil a un gestor 130 de dispositivo móvil en la red segura. El gestor 130 de dispositivo móvil, junto con el servidor 115 de autenticación, usa el identificador de dispositivo móvil para identificar y verificar el dispositivo 105 móvil. Debe observarse que, en algunas realizaciones, el gestor 130 de dispositivo móvil junto con el servidor 115 de autenticación también valida el usuario del dispositivo 105 móvil. Para estas realizaciones, el gestor 130 de dispositivo móvil valida el dispositivo 105 móvil usando biométricas del usuario y/o determinando si el dispositivo 105 móvil está ubicado en una ubicación válida usando señales de geolocalización, tales como señales de sistema de posicionamiento (GPS).

Después de que el gestor 130 de dispositivo móvil y el servidor 115 de autenticación identifiquen, verifiquen, y/o validen el dispositivo 105 móvil y, opcionalmente, validen al usuario del dispositivo 105 móvil, el servidor 115 de autenticación transmite esta información a un rúter 135 de acceso. Una vez que el rúter 135 de acceso recibe esta

información, la red segura establece una conexión 136, 137 segura directa entre el dispositivo 105 móvil y el rúter 135 de acceso (es decir, la conexión no se enruta a través del servidor 115 de autenticación) en donde el dispositivo 105 móvil puede transmitir y recibir datos directamente hasta y desde la red segura.

Una vez que se establece la conexión 136, 137 de datos, la red segura puede transmitir datos seguros encriptados al dispositivo 105 móvil por medio de la conexión 136, 137 de datos. Después de que el dispositivo 105 móvil reciba los datos seguros encriptados, un procesador en el dispositivo 105 móvil ejecuta el software de seguridad de dispositivo móvil para desencriptar los datos seguros encriptados. Adicionalmente, si el usuario del dispositivo 105 móvil desea transmitir datos a la red segura, un procesador en el dispositivo 105 móvil ejecutará el software de seguridad de dispositivo móvil para encriptar los datos. Después de haber encriptado los datos, el dispositivo 105 móvil transmitirá los datos encriptados a la red segura por medio de la conexión 136, 137 de datos. Debe observarse que, en algunas realizaciones, el gestor 130 de dispositivo móvil envía una solicitud al dispositivo 105 móvil para el identificador de dispositivo móvil antes de que el dispositivo 105 móvil transmita el identificador de dispositivo móvil a la red segura.

En esta figura, también se muestra que la red segura incluye almacenamiento 140 de datos seguros, sistemas 145 de acceso de escritorio remotos, sistemas 150 de aplicación web móvil, un sistema 155 de inscripción único web, y/o sistemas 172 de bases de datos de aplicación. En esta figura, se muestra que el almacenamiento 140 de datos seguros incluye un sistema 160 de puerta de acceso de escritorio remoto, un sistema 165 de puerta de acceso de aplicación web móvil, y un sistema 170 de puerta de acceso de bases de datos de aplicación móvil.

Después de que la red segura establezca una conexión 136, 137 no segura directa entre el dispositivo 105 móvil y el rúter 135 de acceso, el dispositivo 105 móvil todavía podrá acceder al Internet 175 público. Si el usuario del dispositivo 105 móvil desea acceder a Internet 175, el rúter 135 de acceso enrutará la conexión al Internet 175 público por medio de un sistema 180 traductor de direcciones de red (NAT) y un sistema 185 proxi de web. Un servidor 190 de sistema de denominación de dominio (DNS) se usa para traducir los nombres de dominio introducidos por el usuario en sus direcciones IP numéricas correspondientes.

En una o más realizaciones de la presente divulgación, un usuario de un dispositivo 105 móvil no seguro que funciona en una red no segura puede comunicar datos seguros a y de otro usuario de otro dispositivo 105 móvil no seguro que funciona en una red no segura mediante la comunicación por medio de una red segura. Estos datos pueden ser diversos tipos de datos que incluyen, pero no se limitan a, datos de voz, datos de vídeo, y datos de texto. En estas realizaciones, un primer usuario de un primer dispositivo 105 móvil y un segundo usuario de un segundo dispositivo móvil (no mostrado) ya tienen una conexión 136, 137 directa establecida a la red segura de manera que ambos dispositivos 105 móviles pueden transmitir y recibir directamente datos hasta y desde la red segura.

Para estas realizaciones, si el primer usuario del primer dispositivo 105 móvil desea transmitir datos seguros al segundo usuario del segundo dispositivo móvil, un procesador en el primer dispositivo 105 móvil ejecutará el software seguro de dispositivo móvil para encriptar los datos. Una vez están encriptados los datos, el primer dispositivo 105 móvil transmitirá los datos encriptados al rúter 135 de acceso en la red segura por medio de conexión 136, 137 de datos. A continuación, el rúter 135 de acceso transmitirá los datos encriptados por medio de una conexión de datos directa al segundo dispositivo móvil. Después de que el segundo dispositivo móvil reciba los datos encriptados, un procesador en el segundo dispositivo móvil ejecutará el software de seguridad de móvil para desencriptar los datos encriptados de modo que el segundo usuario puede comprender los datos.

Debe observarse que, si el primer dispositivo 105 móvil tiene, inicialmente, una conexión 136, 137 directa establecida a la red segura, pero el segundo dispositivo móvil no la tiene, el primer dispositivo 105 móvil puede seguir comunicando datos seguros al segundo dispositivo móvil por medio de la red segura. Para estos casos, si el primer usuario del primer dispositivo 105 móvil desea transmitir datos seguros al segundo usuario del segundo dispositivo móvil, un procesador en el primer dispositivo 105 móvil ejecutará el software seguro de dispositivo móvil para encriptar los datos. Una vez están encriptados los datos, el primer dispositivo 105 móvil transmitirá los datos encriptados al rúter 135 de acceso en la red segura por medio de conexión 136, 137 de datos.

Después de que el rúter 135 de acceso recibe los datos encriptados, el rúter 135 de acceso determina si el segundo dispositivo móvil ya tiene una conexión directa establecida a la red. Después de que el rúter 135 de acceso determine que el segundo dispositivo móvil ya no tiene una conexión directa establecida a la red, a continuación, el rúter 135 de acceso transmitirá una solicitud al segundo dispositivo móvil para enviar su identificador de dispositivo móvil a la red segura para su verificación. Después de que el segundo dispositivo móvil reciba la solicitud, el segundo dispositivo móvil envía su identificador de dispositivo móvil al servidor 115 de autenticación. A continuación, la red segura realiza el procedimiento anteriormente descrito para establecer una conexión segura directa desde el segundo dispositivo móvil hasta la red segura. Una vez se establece una conexión segura directa desde el segundo dispositivo móvil hasta la red segura, el rúter 135 de acceso transmite los datos encriptados al segundo dispositivo móvil. Después de que el segundo dispositivo móvil reciba los datos encriptados, un procesador en el segundo dispositivo móvil ejecutará el software de seguridad de móvil para desencriptar los datos encriptados.

La figura 2 muestra un diagrama 200 de flujo para el funcionamiento del sistema representado en la figura 1, según al menos una realización de la presente divulgación. Al comienzo 205 del procedimiento, un dispositivo móvil

transmite su identificador de dispositivo móvil a un servidor de autenticación en la red 210 de seguridad. Opcionalmente, el dispositivo móvil transmite información de geolocalización y/o biométrica relacionada con el usuario al servidor de autenticación en la red 215 segura. A continuación, el servidor de autenticación transmite el identificador de dispositivo móvil a un gestor 220 de dispositivo móvil. A continuación, el servidor de autenticación verifica y valida el identificador de dispositivo móvil con el gestor 225 de dispositivo móvil.

Opcionalmente, el servidor de autenticación transmite la información de geolocalización y/o biométrica relacionada con el usuario al gestor 230 de dispositivo móvil. A continuación, el servidor de autenticación verifica y valida, opcionalmente, la información de geolocalización y/o biométrica relacionada con el usuario con el gestor 235 de dispositivo móvil.

A continuación, se establece una conexión segura entre el dispositivo móvil y la red 240 segura. A continuación, el dispositivo móvil recibe datos seguros encriptados procedentes de la red segura 245 por medio de la conexión establecida. Después, el dispositivo móvil recibe los datos seguros encriptados, el dispositivo móvil desencripta los datos seguros encriptados recibidos usando el software 250 de seguridad de dispositivo móvil descargado previamente. A continuación, el dispositivo móvil encripta los datos no seguros que transmitirá a la red segura, usando el software 255 de seguridad de dispositivo móvil descargado previamente. Después de que el dispositivo móvil encripte los datos no seguros, el dispositivo móvil transmite los datos encriptados a la red 260 segura. El dispositivo móvil continuará transmitiendo y recibiendo datos encriptados hasta y desde la red segura 265, por consiguiente. A continuación, el procedimiento finaliza 270.

Las figuras 3A y 3B muestran los procedimientos para que un dispositivo móvil no seguro obtenga software de seguridad de dispositivo móvil y un identificador de dispositivo móvil, según al menos una realización de la presente divulgación. En particular, la figura 3A muestra un diagrama 300 de un dispositivo 310 móvil no seguro para descargar e instalar software de seguridad de dispositivo móvil, así como para activar el software de seguridad de dispositivo móvil en el dispositivo 310 móvil, según al menos una realización de la presente divulgación. En esta figura, en primer lugar, un dispositivo 310 móvil envía una solicitud a la red 320 segura, opcionalmente, por medio de un ordenador 330 de escritorio de usuario, para descargar e instalar el software de seguridad de dispositivo móvil. Debe observarse que, alternativamente, esta solicitud puede realizarse a la red 320 segura de una manera fuera de banda, tal como mediante un operador de red segura que ha obtenido la información necesaria para autorizar y permitir al dispositivo 310 móvil. Después de que la red 320 segura reciba la solicitud, la red 320 segura permite que el dispositivo 310 móvil descargue e instale el software de seguridad de dispositivo móvil. Después de que el dispositivo 310 móvil descargue e instale el software de seguridad de dispositivo móvil, opcionalmente, por medio del ordenador 330 de escritorio de usuario, el dispositivo 310 móvil activa el software de seguridad de dispositivo móvil en el dispositivo 310 móvil.

La figura 3B muestra un diagrama 360 de un dispositivo 310 móvil no seguro que transmite una solicitud de registro de gestor de dispositivo móvil y que recibe un identificador de dispositivo móvil, según al menos una realización de la presente divulgación. En esta figura, en primer lugar, el dispositivo 310 móvil transmite una solicitud de registro de dispositivo móvil a la red segura. Opcionalmente, se usa una puerta 370 de acceso de servicio a la web para trasladar la solicitud de registro de gestor de dispositivo móvil para el gestor 380 de dispositivo móvil en la red segura. Después de que el gestor 380 de dispositivo móvil reciba la solicitud, el gestor 380 de dispositivo móvil valida el dispositivo 310 móvil basándose en la descripción de elemento de datos única (UDID) del dispositivo 310 móvil. Después de que el gestor 380 de dispositivo móvil haya validado el dispositivo 310 móvil, el gestor 380 de dispositivo móvil transmite un identificador de dispositivo móvil al dispositivo 310 móvil, opcionalmente, por medio de la puerta 370 de acceso de servicio a la web.

En algunas realizaciones, una vez que el gestor 380 de dispositivo móvil ha validado el dispositivo 310 móvil, el gestor 380 de dispositivo móvil incluye el número de teléfono del dispositivo móvil en una lista de acceso de operador. Los dispositivos 310 móviles que tienen sus números de teléfono en la lista de acceso de operador tendrán comunicaciones con la red segura por medio de una conexión segura directa.

La figura 4 muestra un diagrama 400 de flujo para los procedimientos ilustrados en las figuras 3A y 3B, según al menos una realización de la presente divulgación. Al comienzo 405 del procedimiento, se realiza una comunicación con la red segura para descargar el software 410 de seguridad de dispositivo móvil. Opcionalmente, si existe una conexión de red celular, el número de teléfono del dispositivo móvil se incluye en una lista 415 de acceso de operador. A continuación, el dispositivo móvil descarga es instala el software de seguridad de dispositivo móvil de la red 420 segura. Después de que el dispositivo móvil descargue e instale el software de seguridad de dispositivo móvil, el dispositivo móvil activa el software 425 de seguridad.

A continuación, se establece una conexión segura entre el dispositivo móvil y el gestor 430 de dispositivo móvil. A continuación, el dispositivo móvil transmite una solicitud de registro de dispositivo móvil a la red 435 segura. El gestor de dispositivo móvil valida el dispositivo móvil basándose en la UDID del dispositivo 440 móvil. Opcionalmente, el dispositivo móvil valida el dispositivo móvil basándose en información 445 de geolocalización y/o biométrica relacionada con el usuario. Después de que el gestor de dispositivo móvil valide el dispositivo móvil, el gestor de dispositivo móvil transmite un identificador de dispositivo móvil al dispositivo 450 móvil. Después de que el gestor de dispositivo móvil transmita el identificador de dispositivo móvil, el procedimiento finaliza 455.

Un aspecto de la presente divulgación se refiere a un método para establecer comunicaciones con una red 320 segura usando un dispositivo 105, 310 móvil no seguro que funciona en una red no segura. En un ejemplo, el método incluye comunicar un identificador de dispositivo móvil con la red 320 segura; validar, con un gestor 130, 380 de dispositivo móvil en la red 320 segura, el identificador de dispositivo móvil; y establecer una conexión 136, 137 segura entre el dispositivo 105, 310 móvil y la red 320 segura. En una variante, el identificador de dispositivo móvil se comunica con la red 320 segura por medio de al menos una de una red celular, una red Wi-Fi, y una red de fuera de banda. En otro ejemplo, el método también incluye enviar, con el gestor 130, 380 de dispositivo móvil, una solicitud para el identificador de dispositivo móvil. En otra alternativa, el identificador de dispositivo móvil es una dirección de protocolo de Internet (IP). En todavía otro ejemplo, el identificador de dispositivo móvil es un código de identificación (ID) único. En otra variante, el método también incluye validar, con un gestor 130, 380 de dispositivo móvil, un usuario del dispositivo 105, 310 móvil. En otra alternativa, el usuario del dispositivo 105, 310 móvil se valida usando biométricas del usuario. En otro ejemplo, el dispositivo 105, 310 móvil se valida determinando una ubicación del dispositivo 105, 310 móvil. En todavía otra variante, el método también incluye recibir, con el dispositivo 105, 310 móvil, datos seguros encriptados procedentes de la red 320 segura; y desencriptar, con el dispositivo 105, 310 móvil, los datos seguros encriptados recibidos usando el software de seguridad de dispositivo móvil. En otro ejemplo, el método también incluye encriptar, con el dispositivo 105, 310 móvil, datos no seguros usando el software de seguridad de dispositivo móvil; y transmitir, con el dispositivo 105, 310 móvil, los datos encriptados a la red 320 segura.

Otro aspecto de la divulgación se refiere a un dispositivo 105, 310 móvil no seguro, que funciona en una red no segura usada para establecer comunicaciones con una red 320 segura. En una variante, el dispositivo 105, 310 móvil incluye un transmisor, configurado para comunicar un identificador de dispositivo móvil con la red 320 segura; un receptor, configurado para recibir datos seguros encriptados procedentes de la red 320 segura; y un procesador; configurado para desencriptar los datos seguros encriptados recibidos usando el software de seguridad de dispositivo móvil. En un ejemplo, el software de seguridad de dispositivo móvil incluye al menos uno de software de encriptación, software de desencriptación, y software de direccionamiento de destino fijo forzado. En todavía otra variante, el transmisor comunica el identificador de dispositivo móvil con la red 320 segura por medio de al menos una de una red celular, una red Wi-Fi, y una red de fuera de banda. En otro ejemplo, el identificador de dispositivo móvil es una dirección de protocolo de Internet (IP). En otra alternativa, el identificador de dispositivo móvil es un código de identificación (ID) único. En todavía otra variante, el procesador también está configurado para encriptar datos no seguros usando el software de seguridad de dispositivo móvil descargado previamente y el transmisor también está configurado para transmitir los datos encriptados a la red 320 segura. Todavía otro aspecto de la divulgación se refiere a un método para establecer comunicaciones con una red 320 segura usando un dispositivo 105, 310 móvil no seguro que funciona en una red no segura. En una variante, el método incluye comunicar un identificador de dispositivo móvil con la red 320 segura para establecer una conexión 136, 137 segura entre el dispositivo 105, 310 móvil y la red 320 segura; y establecer una conexión 136, 137 segura entre el dispositivo 105, 310 móvil y la red 320 segura.

Otro aspecto adicional de la divulgación se refiere a un método para establecer comunicaciones con una red 320 segura usando un dispositivo 105, 310 móvil no seguro que funciona en una red no segura. En un ejemplo, el método incluye recibir una solicitud con un identificador de dispositivo móvil para establecer una conexión 136, 137 segura entre el dispositivo 105, 310 móvil y la red 320 segura; validar, con un gestor 130, 380 de dispositivo móvil en la red 320 segura, el identificador de dispositivo móvil; y establecer una conexión 136, 137 segura entre el dispositivo 105, 310 móvil y la red 320 segura. En otra variante, el dispositivo 105, 310 móvil funciona en al menos una de una red celular y una red Wi-Fi. En una alternativa, el método también incluye enviar, con el gestor 130, 380 de dispositivo móvil, una solicitud para el identificador de dispositivo móvil. En todavía otro ejemplo, el identificador de dispositivo móvil es una dirección de protocolo de Internet (IP). En otra variante adicional, el identificador de dispositivo móvil es un código de identificación (ID) único. En otra alternativa, el método también incluye validar, con el gestor 130, 380 de dispositivo móvil, un usuario del dispositivo 105, 310 móvil. En otro ejemplo, el método también incluye transmitir, con un transmisor, datos seguros encriptados procedentes de la red 320 segura al dispositivo 105, 310 móvil. En otra variante adicional, el método también incluye recibir, con el receptor, datos encriptados transmitidos procedentes del dispositivo 105, 310 móvil; y desencriptar, con un procesador, los datos encriptados recibidos. En un ejemplo, el usuario del dispositivo 105, 310 móvil se valida usando biométricas del usuario. En otra alternativa, el dispositivo 105, 310 móvil se valida determinando una ubicación del dispositivo 105, 310 móvil.

Otro aspecto de la divulgación se refiere a un método para permitir el establecimiento de comunicaciones con una red 320 segura usando un dispositivo 105, 310 móvil no seguro que funciona en una red no segura. En una variante, el método incluye comunicar una solicitud a la red 320 segura para descargar el software de seguridad de dispositivo móvil; descargar e instalar, mediante el dispositivo 105, 310 móvil, el software de seguridad de dispositivo móvil de la red 320 segura; activar, mediante el dispositivo 105, 310 móvil, el software de seguridad de dispositivo móvil; transmitir, con el dispositivo 105, 310 móvil, una solicitud de registro de gestor de dispositivo móvil a la red 320 segura; validar, con el gestor 130, 380 de dispositivo móvil, el dispositivo 105, 310 móvil basándose en una descripción de elemento de datos única (UDID) del dispositivo 105, 310 móvil; y transmitir, mediante el gestor 130, 380 de dispositivo móvil, un identificador de dispositivo móvil al dispositivo 105, 310 móvil, en donde el identificador de dispositivo móvil permite que el dispositivo 105, 310 móvil establezca comunicaciones con la red 320 segura. En otro ejemplo, el método también alberga incluir, con el gestor 130, 380 de dispositivo móvil, un número de teléfono

del dispositivo 105, 310 móvil en una lista de acceso de operador, en donde las transmisiones de datos encriptados posteriores procedentes de los dispositivos 105, 310 móviles que tienen sus números de teléfono en la lista de acceso de operador se enrutarán de manera automática a la red 320 segura.

Aunque en el presente documento se han dado a conocer determinadas realizaciones y métodos ilustrativos, para los expertos en la técnica puede resultar evidente a partir de la divulgación anterior que pueden realizarse variaciones y modificaciones de tales realizaciones y métodos sin alejarse del alcance de la técnica dada a conocer. Existen muchos ejemplos adicionales de la técnica dada a conocer, diferenciándose unos con respecto a otros simplemente en cuestiones de detalles. Por consiguiente, se prevé que la técnica dada a conocer solamente se vea limitada en el grado requerido por las reivindicaciones adjuntas y las normas y principios de la ley aplicable.

REIVINDICACIONES

1. Método para establecer comunicaciones con una red (320) segura usando un dispositivo (105, 310) móvil no seguro que funciona en una red no segura, comprendiendo el método:

un servidor (115) de autenticación en la red segura que recibe un identificador de dispositivo móvil procedente del dispositivo móvil, en el que el identificador de dispositivo móvil incluye un número aleatorio generado por un algoritmo generador de número aleatorio que está contenido en el software de seguridad de dispositivo móvil descargado, cambiando el número aleatorio de manera periódica de números aleatorios válidos a números aleatorios falsos;

transmitiendo el servidor de autenticación el identificador de dispositivo móvil a un gestor (130, 380) de dispositivo móvil en la red segura;

usando el gestor de dispositivo móvil junto con el servidor de autenticación el identificador de dispositivo móvil para identificar y verificar el dispositivo móvil;

transmitiendo el servidor de autenticación a un rúter (135) de acceso en la red segura que el dispositivo móvil se ha identificado y verificado; y

en respuesta a esto, estableciendo la red segura una conexión (136, 137) segura directa entre el rúter de acceso y el dispositivo móvil que no se enruta a través del servidor de autenticación, de manera que el dispositivo móvil puede transmitir y recibir datos directamente hasta y desde la red segura.

2. Método según la reivindicación 1, en el que el identificador de dispositivo móvil se comunica con la red (320) segura por medio de al menos una de una red celular, una red Wi-Fi, y una red de fuera de banda.

3. Método según cualquiera de las reivindicaciones 1-2, en el que el método comprende, además, enviar, con el gestor (130, 380) de dispositivo móvil, una solicitud para el identificador de dispositivo móvil.

4. Método según cualquiera de las reivindicaciones 1-3, en el que el identificador de dispositivo móvil incluye una dirección de protocolo de Internet, IP.

5. Método según cualquiera de las reivindicaciones 1-4, en el que el identificador de dispositivo móvil incluye un código de identificación único, ID.

6. Método según cualquiera de las reivindicaciones 1-5, en el que el método comprende, además, validar, con el gestor (130, 380) de dispositivo móvil, un usuario del dispositivo (105, 310) móvil.

7. Método según la reivindicación 6, en el que el usuario del dispositivo (105, 310) móvil se valida usando biométricas del usuario.

8. Método según cualquiera de las reivindicaciones 1-7, en el que el dispositivo (105, 310) móvil se valida determinando una ubicación del dispositivo (105, 310) móvil.

9. Método según cualquiera de las reivindicaciones 1-8, en el que el método comprende, además:

recibir, con el dispositivo (105, 310) móvil, datos seguros encriptados procedentes de la red (320) segura; y

desencriptar, con el dispositivo (105, 310) móvil, los datos seguros encriptados recibidos usando un software de seguridad de dispositivo móvil.

10. Método según cualquiera de las reivindicaciones 1-8 en el que el método comprende, además:

encriptar, con el dispositivo (105, 310) móvil, datos no seguros usando un software de seguridad de dispositivo móvil; y

transmitir, con el dispositivo (105, 310) móvil, los datos encriptados a la red (320) segura.

11. Dispositivo (105, 310) móvil no seguro que funciona en una red no segura usado para establecer comunicaciones con una red (320) segura, comprendiendo el dispositivo (105, 310) móvil:

un transmisor, en el que el transmisor está configurado para comunicar un identificador de dispositivo móvil a la red (320) segura;

un receptor, en el que el receptor está configurado para recibir datos seguros encriptados procedentes de la red (320) segura; y

un procesador, en el que el procesador está configurado para desencriptar los datos seguros encriptados recibidos usando un software de seguridad de dispositivo móvil, estando el dispositivo móvil dispuesto para hacer funcionar un

método definido en cualquiera de las reivindicaciones 1 a la reivindicación 10.

12. Dispositivo (105, 310) móvil según la reivindicación 11, en el que el software de seguridad de dispositivo móvil comprende al menos uno de software de encriptación, software de desencriptación, y software de direccionamiento de destino fijo forzado.

13. Dispositivo (105, 310) móvil según cualquiera de las reivindicaciones 11-12, en el que el identificador de dispositivo móvil es una dirección de protocolo de Internet, IP.

14. Dispositivo (105, 310) móvil según cualquiera de las reivindicaciones 11-13, en el que el identificador de dispositivo móvil es un código de identificación único, ID.

15. Dispositivo (105, 310) móvil según cualquiera de las reivindicaciones 11-14, en el que el procesador está configurado, además, para encriptar datos no seguros usando el software de seguridad de dispositivo móvil, y en el que el transmisor está configurado, además, para transmitir los datos encriptados a la red (320) segura.

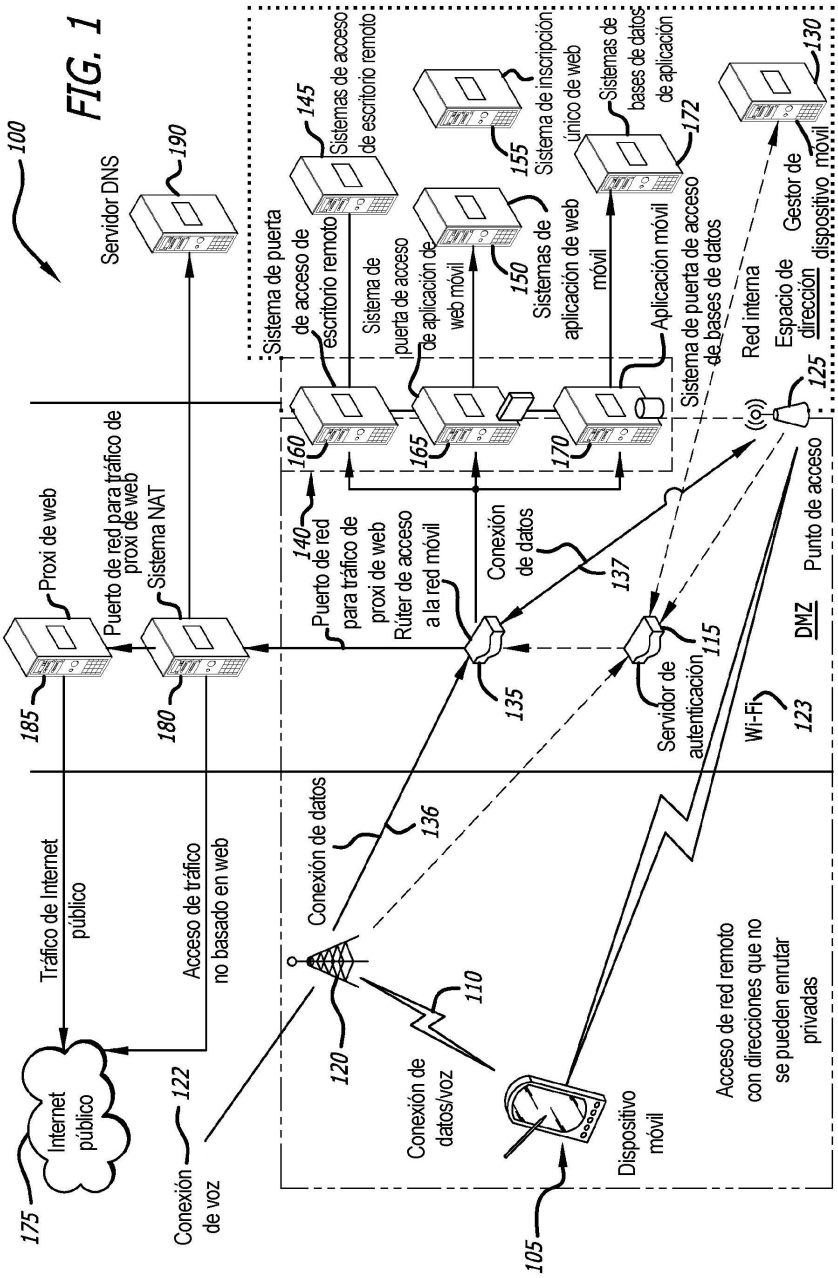


FIG. 1
100
Servidor DNS
190
Sistema de puerta de acceso de escritorio remoto
145
Sistemas de acceso de escritorio remoto
Sistema de puerta de acceso de aplicación de web móvil
155
Sistema de inscripción único de web
Sistemas de bases de datos de aplicación
172
130
150
Sistemas de aplicación de web móvil
Aplicación móvil
Sistema de puerta de acceso de bases de datos
Red interna
Espacio de dirección
Gestor de dispositivo móvil
125
160
165
170
Proxi de web
Puerto de red para tráfico de proxi de web
Sistema NAT
140
Puerto de red para tráfico de proxi de web
Rúter de acceso a la red móvil
Conexión de datos
137
185
180
135
Servidor de autenticación
115
DMZ
Punto de acceso
Wi-Fi
123
Tráfico de Internet público
Acceso de tráfico no basado en web
Conexión de datos
136
120
110
Conexión de datos/voz
Dispositivo móvil
Acceso de red remoto con direcciones que no se pueden enrutar privadas
Internet público
175
122
Conexión de voz
105

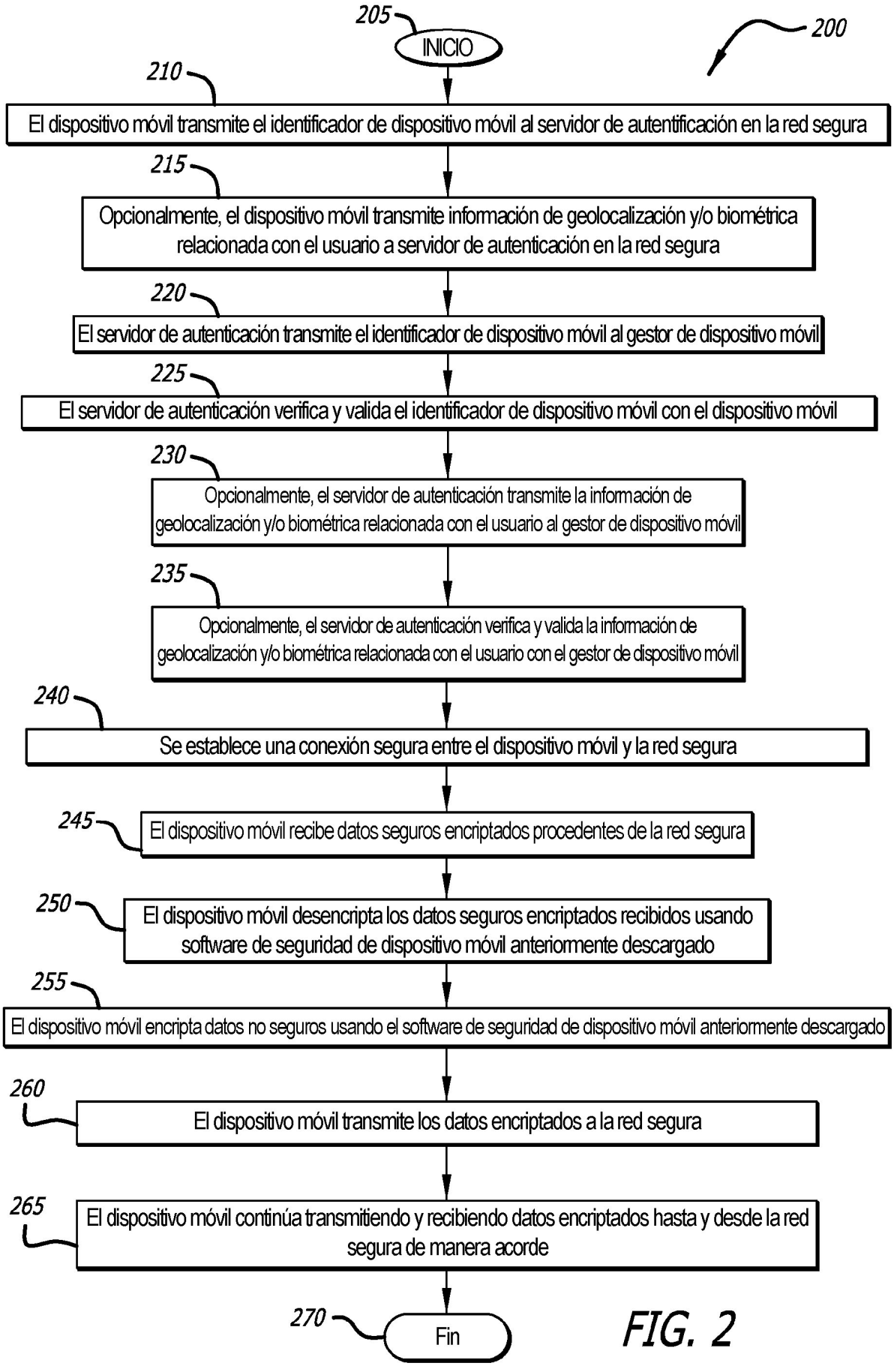

205
INICIO
200
210
El dispositivo móvil transmite el identificador de dispositivo móvil al servidor de autentificación en la red segura
215
Opcionalmente, el dispositivo móvil transmite información de geolocalización y/o biométrica relacionada con el usuario a servidor de autenticación en la red segura
220
El servidor de autenticación transmite el identificador de dispositivo móvil al gestor de dispositivo móvil
225
El servidor de autenticación verifica y valida el identificador de dispositivo móvil con el dispositivo móvil
230
Opcionalmente, el servidor de autenticación transmite la información de geolocalización y/o biométrica relacionada con el usuario al gestor de dispositivo móvil
235
Opcionalmente, el servidor de autenticación verifica y valida la información de geolocalización y/o biométrica relacionada con el usuario con el gestor de dispositivo móvil
240
Se establece una conexión segura entre el dispositivo móvil y la red segura
245
El dispositivo móvil recibe datos seguros encriptados procedentes de la red segura
250
El dispositivo móvil desencripta los datos seguros encriptados recibidos usando software de seguridad de dispositivo móvil anteriormente descargado
255
El dispositivo móvil encripta datos no seguros usando el software de seguridad de dispositivo móvil anteriormente descargado
260
El dispositivo móvil transmite los datos encriptados a la red segura
265
El dispositivo móvil continúa transmitiendo y recibiendo datos encriptados hasta y desde la red segura de manera acorde
270
Fin

FIG. 2

FIG. 3A

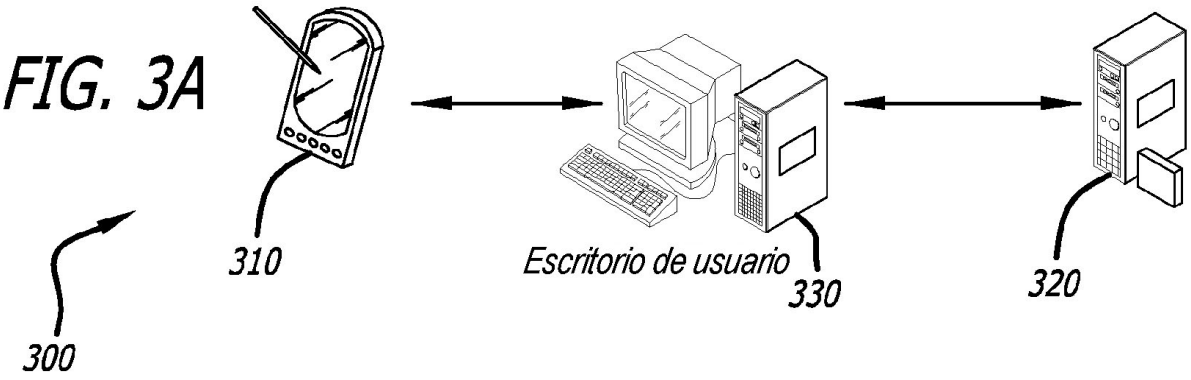
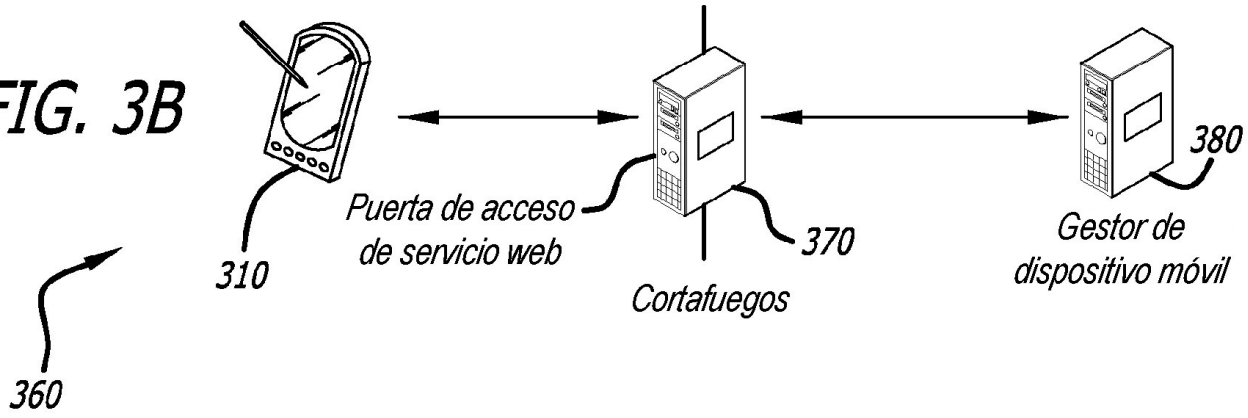

310
Escritorio de usuario
330
320
300

FIG. 3B


310
Puerta de acceso
de servicio web
370
Cortafuegos
380
Gestor de
dispositivo móvil
360

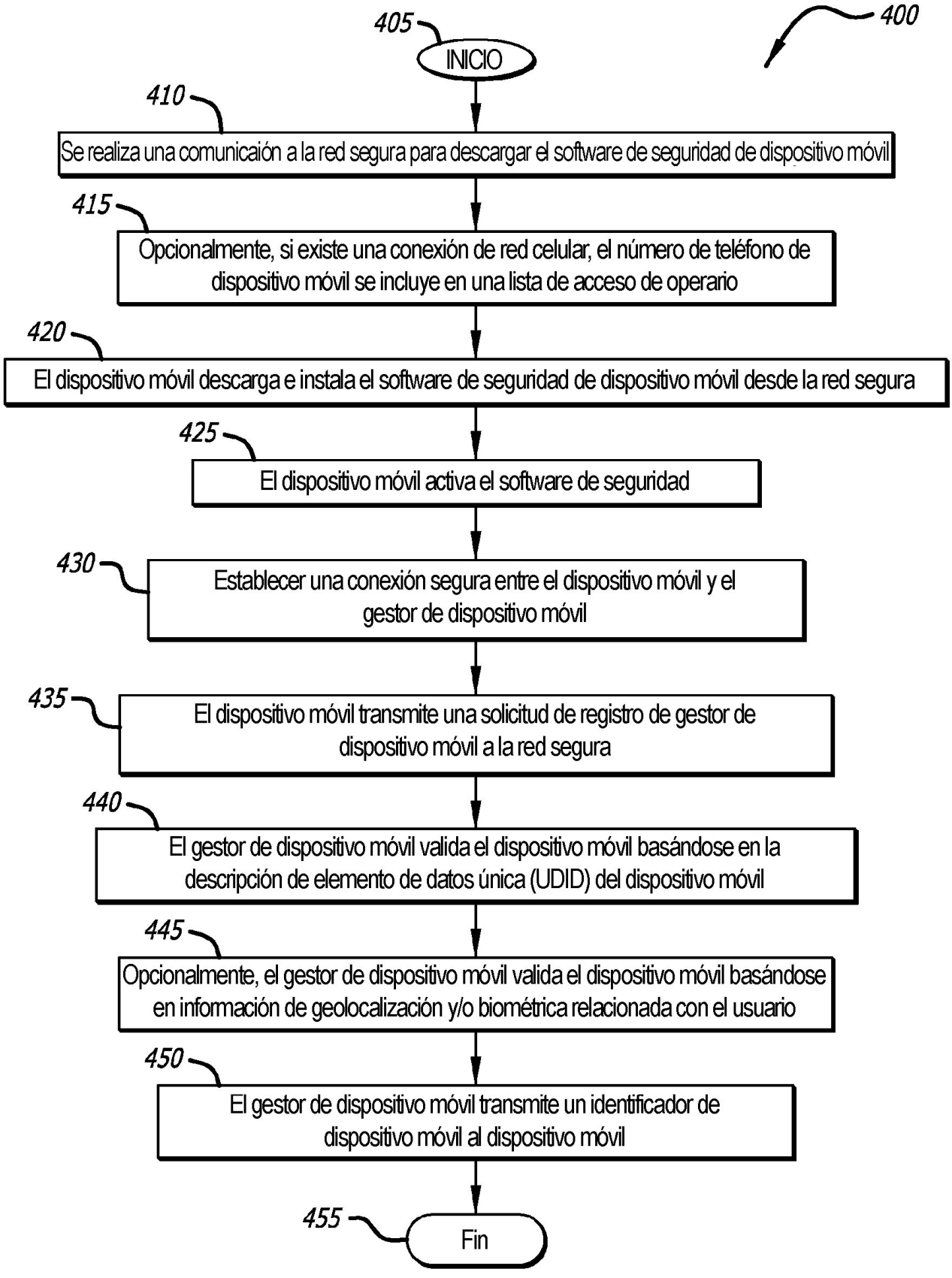

400
405
INICIO
410
Se realiza una comunicaión a la red segura para descargar el software de seguridad de dispositivo móvil
415
Opcionalmente, si existe una conexión de red celular, el número de teléfono de dispositivo móvil se incluye en una lista de acceso de operario
420
El dispositivo móvil descarga e instala el software de seguridad de dispositivo móvil desde la red segura
425
El dispositivo móvil activa el software de seguridad
430
Establecer una conexión segura entre el dispositivo móvil y el gestor de dispositivo móvil
435
El dispositivo móvil transmite una solicitud de registro de gestor de dispositivo móvil a la red segura
440
El gestor de dispositivo móvil valida el dispositivo móvil basándose en la descripción de elemento de datos única (UDID) del dispositivo móvil
445
Opcionalmente, el gestor de dispositivo móvil valida el dispositivo móvil basándose en información de geolocalización y/o biométrica relacionada con el usuario
450
El gestor de dispositivo móvil transmite un identificador de dispositivo móvil al dispositivo móvil
455
Fin

FIG. 4