(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 967 287**

(51) Int. Cl.:

H04L 9/40 (2012.01)
H04W 12/033 (2011.01)
H04W 12/37 (2011.01)
H04W 12/48 (2011.01)
H04W 12/47 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **02.12.2020 E 20211287 (6)**

(97) Fecha y número de publicación de la concesión europea: **18.10.2023 EP 4009601**

(54) Título: **Establecimiento de VPN**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.04.2024

(73) Titular/es:

MATERNA VIRTUAL SOLUTION GMBH (100.0%)
Blutenburgstraße 18
80636 München, DE

(72) Inventor/es:

MIHATSCH, OLIVER y
LEHMANN-CARPZOV, FALKO

(74) Agente/Representante:

SUGRAÑES, S.L.P.

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Establecimiento de VPN

Campo

[0001] La presente invención se refiere, en general, a la tecnología de la información. Más específicamente, la presente invención está dirigida a establecer una conexión segura entre un contenedor de dispositivo móvil y varias redes privadas virtuales (VPN, por sus siglas en inglés).

Antecedentes

[0002] Los contenedores de dispositivos móviles actúan como un espacio adicional dentro de los dispositivos móviles. Los contenedores de dispositivos móviles sirven para delimitar y proteger aplicaciones, datos y procesos dentro del contenedor de dispositivo móvil de aquellos fuera del contenedor de dispositivo móvil. Esta delaminación entre el interior y el exterior de los contenedores de dispositivo móvil también se ha cumplido al establecer una conexión VPN.

[0003] El documento EP 2 629 570 A1 se refiere a un método y dispositivo para un inicio de sesión automático de una red privada virtual en un cambio de interfaz, el método: asociar un perfil de red privada virtual con una pluralidad de interfaces de conexión, cada interfaz de conexión dentro de la pluralidad de interfaces de conexión teniendo una prioridad; monitorear la disponibilidad de la pluralidad de interfaces de conexión; si está disponible una interfaz de conexión con una prioridad más alta que la interfaz de conexión actualmente utilizada por la red privada virtual, utilizar la interfaz de conexión de mayor prioridad para la red privada virtual; y si la interfaz de conexión utilizada actualmente por la red privada virtual deja de estar disponible, transferir la red privada virtual a una interfaz de conexión disponible de máxima prioridad dentro de la pluralidad de interfaces de conexión.

[0004] El documento US 2006/212937 A1 se refiere al suministro automático de dispositivos móviles con información de VPN (red privada virtual) para que los usuarios puedan conectarse automáticamente a sus redes corporativas utilizando sus dispositivos. El estándar OMA SyncML se amplía para definir conexiones VPN y suministrarlas en los dispositivos automáticamente, ya sea de forma inalámbrica o mediante una aplicación informática proporcionada por la compañía.

[0005] El documento US 2013/297933 A1 se refiere a utilidades que permiten una autentificación multifactor en una red empresarial con una tarjeta inteligente que utiliza dispositivos móviles (por ejemplo, teléfonos inteligentes, tabletas, etc.), donde casi cualquier aplicación (app) o sitio web que acceda a los recursos de la empresa se puede lanzar o ejecutar para establecer automáticamente una conexión VPN con la red empresarial sin tener que configurar necesariamente las aplicaciones o sitios web para que se puedan utilizar con tarjetas inteligentes, lectores de tarjetas, etc. Prácticamente cualquier aplicación se puede utilizar y puede aprovechar la autentificación multifactor sin o sustancialmente sin modificaciones de la propia aplicación, como las utilidades divulgadas pueden aprovechar los clientes VPN nativos y las capacidades proporcionadas con el sistema operativo del dispositivo móvil (OS, por sus siglas en inglés) (por ejemplo, Android®, iOS). Como resultado, se puede proporcionar una solución mucho más flexible que permita el uso de aplicaciones comercializadas (por ejemplo, de una Tienda Apple) así como, por ejemplo, aplicaciones desarrolladas por empresas.

[0006] El documento US 2014/109174 A1 se refiere a proporcionar un túnel de red privada virtual (VPN) controlado por políticas por aplicación. En algunas realizaciones, las incidencias se pueden utilizar para proporcionar acceso a un recurso empresarial sin autentificación separada de la aplicación y, en algunos casos, se pueden utilizar de tal manera que proporcionen una experiencia perfecta al usuario al restablecer un túnel de VPN controlado por políticas por aplicación durante la vida útil de la incidencia. Los aspectos adicionales se refieren a una puerta de enlace de acceso que proporciona información actualizada sobre políticas e incidencias a un dispositivo móvil. Otros aspectos se refieren a borrar selectivamente las incidencias de un contenedor seguro del dispositivo móvil. Otros aspectos se refieren al funcionamiento de aplicaciones en múltiples modos, tales como un modo administrado y un modo no administrado, y a la prestación de servicios relacionados con la autentificación basados en uno o más de los aspectos anteriores.

Descripción

[0007] La invención se define por las reivindicaciones adjuntas.

[0008] La presente invención se refiere a un sistema para establecer una conexión segura entre un contenedor de dispositivo móvil y un numero de VPN. El sistema comprende un contenedor de dispositivo móvil que está configurado para aislar una parte de un dispositivo móvil de otra parte del dispositivo móvil. El sistema también comprende un número de VPN, donde cada una del número de VPN tiene un perfil de VPN. Además, el sistema comprende un token criptográfico que está configurado para proporcionar, al menos, parte del perfil de VPN de, al menos, una de un número de VPN. El sistema también comprende un enlace de comunicación que está configurado para enlazar el contenedor

de dispositivo móvil y el token criptográfico. Para establecer una conexión segura a, al menos, una VPN del número de VPN, el contenedor de dispositivo móvil está configurado para acceder, al menos, a parte del perfil de VPN de la al menos una VPN del número de VPN a través del enlace de comunicación que está configurado para enlazar el contenedor de dispositivo móvil y el token criptográfico.

[0009] Preferiblemente, se utiliza "VPN" en el presente documento para indicar una red lógica que se establece entre un cliente y un servidor y otros participantes potenciales. Otros participantes de la VPN pueden comprender puertas de enlace, otros servidores o servicios. Al establecer la red lógica entre el cliente y el servidor y otros posibles participantes, el propio cliente puede convertirse en participante de la VPN. El contenedor de dispositivo móvil puede ser un cliente de una VPN. El contenedor de dispositivo móvil puede convertirse en participante de la VPN.

[0010] Una conexión segura generalmente puede comprender una conexión que impide que terceros accedan, lean o interfieran sin autorización con la conexión o cualquier comunicación dentro de la conexión. Una conexión segura puede referirse a un canal seguro entre el contenedor de dispositivo móvil y uno de los participantes de la VPN donde cualquier actividad de seguimiento desde el exterior es imposible. Una conexión segura puede comprender un túnel de VPN.

[0011] El número de VPN puede comprender, al menos, una VPN. El número de VPN puede depender de la arquitectura de VPN a la que se conectará el contenedor de dispositivo móvil. Por ejemplo, cuando un contenedor de dispositivo móvil de un usuario se va a conectar a la VPN del departamento de la empresa del usuario, el contenedor de dispositivo móvil puede conectarse primero a la VPN general de la empresa antes de que se pueda acceder a la VPN del departamento. En este caso, el número de VPN es igual a dos. El número de VPN puede depender de la organización interna de una empresa, gobierno, institución educativa u otra entidad. El número de VPN puede modificarse en los casos en los que el contenedor de dispositivo móvil deba estar conectado de forma segura a menos o más VPN.

[0012] El número de VPN puede configurarse como cualquiera de una VPN de múltiples saltos, una VPN de doble salto, una VPN en cadena, una VPN en cascada y una VPN posterior.

[0013] Cada una del número de VPN puede comprender cualquiera de una red privada, una VPN, un *proxy*, un *proxy* de puerta de enlace, un *proxy* de túnel, un *proxy* inverso, un *proxy* de puerta de enlace, un *proxy* de puente o un conector de red. Para obtener más detalles sobre el *proxy* de puerta de enlace, se puede consultar la solicitud de patente europea EP3544252A1.

[0014] El contenedor de dispositivo móvil puede crear un espacio aislado dentro de un dispositivo móvil. El contenedor de dispositivo móvil puede permitir una división estricta entre el contenedor de dispositivo móvil y el dispositivo móvil restante. Los datos dentro del contenedor pueden almacenarse y transferirse encriptados. Las aplicaciones dentro del contenedor de dispositivo móvil, tal como calendario, correo electrónico, contactos, pueden ejecutarse completamente por separado de las que están fuera del contenedor. Por consiguiente, un contenedor de dispositivo móvil puede unir dos casos de uso separados, por ejemplo, uso privado y uso empresarial, en un dispositivo móvil. Por lo tanto, el contenedor de dispositivos móviles puede atender a empresas, gobiernos, instituciones educativas y otras entidades para trabajadores externos temporales, y políticas tal como *Bring Your Own Device* (BYOD), del inglés "trae tu propio dispositivo", o *Corporate Owned, Personally Enabled* (COPE), del inglés "propiedad de la empresa, habilitada para uso personal" y más.

[0015] El acceso al propio dispositivo móvil puede no permitir aún el acceso al contenedor de dispositivo móvil. El acceso al contenedor de dispositivo móvil puede requerir credenciales adicionales. El contenedor de dispositivo móvil puede proteger información y datos independientemente de un sistema operativo subyacente.

[0016] El contenedor de dispositivo móvil puede implementarse como una aplicación, *software* y/o *hardware* dentro de un dispositivo móvil. Un dispositivo móvil puede comprender cualquier dispositivo que sea principalmente móvil. Puede comprender ordenador, portátil, ordenador portátil, tableta, teléfonos inteligentes, relojes inteligentes y lectores de libros electrónicos.

[0017] El token criptográfico puede configurarse para proporcionar, al menos, parte del perfil de VPN de, al menos, una de un número de VPN. Como alternativa, o además de la misma, el token criptográfico puede proporcionar el perfil de VPN completo de, al menos, una de un número de VPN. Como alternativa, o además de la misma, el token criptográfico puede proporcionar, al menos, parte de cada uno de los perfiles de VPN de cada uno de los números de VPN. Como alternativa, o además de la misma, el token criptográfico puede proporcionar el perfil de VPN completo de cada uno de los números de VPN.

[0018] El token criptográfico se puede configurar para un solo uso. En este caso, acceder, al menos, a parte del perfil de VPN de la VPN también puede comprender extraer la al menos parte del perfil de VPN a la que se ha accedido al contenedor de dispositivo móvil. De este modo, la al menos parte del perfil de VPN puede ser accesible permanentemente por el contenedor de dispositivo móvil.

[0019] Al menos parte del perfil de VPN puede almacenarse en el token criptográfico cumpliendo con el estándar de sintaxis de información de token criptográfico PKCS#15. Al menos parte del perfil de VPN puede almacenarse en el token criptográfico cumpliendo con el estándar FIPS 201-2 PIV, del inglés "verificación de identidad personal". Además, o como alternativa, al menos, parte del perfil de VPN puede analizarse y almacenarse en un espacio no utilizado del token criptográfico. Además, o como alternativa, se puede analizar y almacenar una parte adicional del perfil de VPN en un espacio no utilizado del token criptográfico. El contenedor de dispositivo móvil puede comprender instrucciones sobre cómo acceder a la parte adicional del perfil de VPN que se ha analizado y almacenado previamente en un espacio no utilizado del token criptográfico.

[0020] El token criptográfico puede contener áreas de almacenamiento donde se puede almacenar, al menos, parte del perfil de VPN. Esta parte del perfil de VPN puede referirse a información, tal como material de clave secreta. En algún ejemplo, este material de clave secreta puede ser material de clave privada, material de clave pública, certificados X.509 u otros datos. Esta área de almacenamiento normalmente no puede ser procesada por el token durante el funcionamiento normal.

[0021] El perfil de VPN puede servir para la autentificación del contenedor de dispositivo móvil hacia la VPN. Se puede requerir un perfil de VPN completo para una autentificación correcta. La autentificación puede garantizarse mediante cualquiera o cualquier combinación de posesión legítima del perfil de VPN, características físicas o biométricas del usuario del contenedor de dispositivo móvil, secreto genérico entre el contenedor de dispositivo móvil y la VPN. El perfil de VPN puede comprender información clasificada.

[0022] El perfil de VPN de cada uno del número de VPN puede comprender, al menos, uno de entre: autentificación de desafío-respuesta, identificación de usuario (ID, por sus siglas en inglés), ID de dispositivo móvil, ID de contenedor de dispositivo móvil, clave criptográfica, clave encriptada, clave privada, clave pública, certificado, certificado de clave pública, secreto genérico, número de identificación personal (PIN, por sus siglas en inglés), contraseña, contraseña de un solo uso, clave de interfaz de programación de aplicaciones (API, por sus siglas en inglés), token de API, identificación biométrica, identificación de huellas dactilares, identificación de venas de la palma de la mano, identificación facial, identificación de ADN, identificación de huellas de la palma de la mano, identificación de iris, identificación de geometrías de la mano, identificación de retina, identificación ID de voz. El perfil de VPN puede ser cualquiera de entre no encriptado, asimétrico o simétricamente encriptado.

[0023] El perfil de VPN de cada una del número de VPN puede también comprender, al menos, uno de entre: información del servidor de VPN, número de puerto, nombre de servidor, dirección de red, sistema de destino, información de configuración, información de tiempo de espera, información de compresión, dirección IP, número de identificación. El perfil de VPN puede proporcionarse en texto plano y/o texto cifrado. El texto cifrado puede ser el resultado de un cifrado simétrico o asimétrico.

[0024] El token criptográfico puede estar proporcionado por, al menos, uno de entre: una tarjeta inteligente, una tarjeta de circuito integrado (ICC, por sus siglas en inglés), un medio de bus universal en serie (USB, por sus siglas en inglés), un código de respuesta rápida (QR, por sus siglas en inglés), un medio óptico, un medio de audio, un medio fotográfico, un medio holográfico, un generador de número de autentificación de transacción (TAN, por sus siglas en inglés), un reloj inteligente, un medio de comunicación de campo cercano (NFC, por sus siglas en inglés), un medio de identificación por radiofrecuencia (RFID, por sus siglas en inglés), un usuario.

[0025] El enlace de comunicación puede comprender, al menos, uno de entre: *Bluetooth*, un lector de tarjetas alámbrico, un lector de tarjetas inalámbrico, NFC, RFID, una red de área corporal (BAN, por sus siglas en inglés), un dispositivo de reconocimiento biométrico, un dispositivo de reconocimiento óptico, emparejamiento óptico, un dispositivo de reconocimiento QR, un dispositivo de reconocimiento de huellas dactilares, un dispositivo de reconocimiento de las venas de la palma de la mano, un dispositivo de reconocimiento facial, un dispositivo de reconocimiento de ADN, un dispositivo de reconocimiento de las palmas de la mano, un dispositivo de reconocimiento del iris, un dispositivo de reconocimiento de la geometría de la mano, un dispositivo de reconocimiento de la retina, un dispositivo de reconocimiento de identificación de voz.

[0026] El token criptográfico puede además comprender un mecanismo de desbloqueo para que el contenedor de dispositivo móvil lo desbloquee. El mecanismo de desbloqueo puede iniciar una interfaz gráfica de usuario que puede solicitar a un usuario del contenedor de dispositivo móvil que introduzca un PIN o escanee huellas dactilares.

[0027] La al menos parte del perfil de VPN puede ser implementada manualmente en el token criptográfico por un administrador de red. Como alternativa, o en combinación con la misma, la al menos parte del perfil de VPN se puede implementar en el token criptográfico dentro del procesamiento por lotes.

[0028] El sistema puede además comprender un token criptográfico adicional. El sistema puede configurarse para proporcionar una parte adicional del perfil de VPN para establecer una conexión segura con la VPN del número de VPN. La parte adicional del perfil de VPN puede estar proporcionada por, al menos, uno de los siguientes: contenedor de dispositivo móvil, la VPN del número de VPN, el enlace de comunicación y el token criptográfico adicional.

[0029] En caso de que el contenedor de dispositivo móvil proporcione el token criptográfico adicional, un administrador puede implementar el token adicional manualmente, implementarlo automáticamente durante la configuración del contenedor de dispositivo móvil (por ejemplo, mediante una gestión de dispositivos móviles) o puede ser parte del paquete de instalación. Como alternativa, o además de la misma, el token criptográfico adicional también puede recuperarse de un recurso de red disponible después de conectarse y unirse a una VPN anterior del número de VPN.

[0030] El token criptográfico puede configurarse para indicar al contenedor de dispositivo móvil dónde y/o cómo acceder a la parte adicional del perfil de VPN dentro del sistema. Como alternativa, o en combinación con el mismo, el contenedor de dispositivo móvil puede comprender información sobre dónde y/o cómo acceder a la al menos parte y a la parte adicional del perfil de VPN dentro del sistema.

[0031] Para establecer una conexión segura con una VPN posterior, el sistema puede además configurarse para proporcionar selectivamente, al menos, parte del perfil de VPN de la VPN posterior, solo si la conexión entre el contenedor de dispositivo móvil y la VPN se ha establecido con éxito.

[0032] La expresión "proporcionado selectivamente" se puede utilizar en el presente documento para indicar un mecanismo que desbloquea y/o activa el perfil de VPN de la VPN posterior tras recibir retroinformación de que la conexión segura de la VPN, es decir, la VPN que precede a la VPN posterior, se ha establecido con éxito. El mecanismo puede comprender lógica, una bandera, procesos aritméticos, registros o similares. Este mecanismo puede además mejorar la seguridad del procesamiento de perfiles de VPN porque oculta, al menos, parte del perfil de VPN de la VPN posterior hasta que el contenedor de dispositivo móvil ya haya demostrado con éxito la autentificación en una VPN relacionada. Este mecanismo puede emplearse particularmente para perfiles de VPN que comprenden información clasificada. En términos figurativos, "proporcionado selectivamente" podría ilustrarse mediante una secuencia de puertas en la que, al menos, parte de la llave y/o dirección de la segunda puerta contigua solamente se proporciona después de la puerta siguiente.

[0033] Una implementación de "proporcionada selectivamente" puede utilizar diferentes conjuntos de tókenes criptográficos para acceder a la VPN posterior. Los diferentes conjuntos de tókenes criptográficos pueden ser multiuso, de un solo uso o válidos solamente durante un tiempo determinado. En un ejemplo, el contenedor móvil puede tener acceso a un token criptográfico (a) y un token criptográfico adicional (b). El contenedor de dispositivo móvil puede utilizar un token (a) para conectarse y acceder a VPN1. El contenedor móvil ahora puede conectarse y autentificarse utilizando un token criptográfico (b) a un servicio interno solamente accesible a través de VPN1 que puede proporcionar otro token criptográfico de un solo uso (c). A continuación, el contenedor móvil puede utilizar el token criptográfico de un solo uso (c) para conectarse y acceder a VPN2.

[0034] La expresión "establecido con éxito" se puede utilizar en el presente documento para indicar que el contenedor de dispositivo móvil se ha autentificado ante la VPN y se ha conectado de forma segura a la VPN. Inmediatamente después, el contenedor de dispositivo móvil y/u otros componentes del sistema pueden recibir una retroalimentación correspondiente que, a su vez, podría ser necesaria para desbloquear y/o activar el perfil de VPN de la VPN posterior.

[0035] Al menos parte del perfil de VPN de la VPN posterior puede estar proporcionado selectivamente por, al menos, uno de los siguientes: el token criptográfico, el contenedor de dispositivo móvil, la VPN del número de VPN, el enlace de comunicación y el token criptográfico adicional.

[0036] El token criptográfico adicional puede estar proporcionado por, al menos, uno de entre: una tarjeta inteligente, una tarjeta de circuito integrado (ICC), un medio de bus universal en serie (USB), un código de respuesta rápida (QR), un medio óptico, un medio de audio, un medio fotográfico, un medio holográfico, un generador de número de autentificación de transacción (TAN), un reloj inteligente, un medio de comunicación de campo cercano (NFC), un medio de identificación por radiofrecuencia (RFID), un usuario.

[0037] El enlace de comunicación adicional puede comprender, al menos, uno de entre: *Bluetooth*, un lector de tarjetas alámbrico, un lector de tarjetas inalámbrico, NFC, RFID, una red de área corporal (BAN, por sus siglas en inglés), un dispositivo de reconocimiento biométrico, un dispositivo de reconocimiento óptico, emparejamiento óptico, un dispositivo de reconocimiento QR, un dispositivo de reconocimiento de huellas dactilares, un dispositivo de reconocimiento de las venas de la palma de la mano, un dispositivo de reconocimiento facial, un dispositivo de reconocimiento de ADN, un dispositivo de reconocimiento de las palmas de la mano, un dispositivo de reconocimiento del iris, un dispositivo de reconocimiento de la geometría de la mano, un dispositivo de reconocimiento de la retina, un dispositivo de reconocimiento de identificación de voz.

[0038] El token criptográfico adicional puede además comprender un mecanismo de desbloqueo para que el contenedor de dispositivo móvil lo desbloquee. El mecanismo de desbloqueo puede iniciar una interfaz gráfica de usuario que puede solicitar a un usuario del contenedor de dispositivo móvil que introduzca un PIN o escanee huellas dactilares.

[0039] Otro aspecto de la invención se refiere a una tarjeta inteligente. La tarjeta inteligente comprende lógica criptográfica, una unidad central de procesamiento, una interfaz de comunicación que está configurada para comunicarse con un contenedor de dispositivo móvil y una memoria. La memoria puede comprender memoria volátil, tal como RAM, y/o memoria no volátil, tal como Flash, EEPROM. El contenedor de dispositivo móvil está configurado para aislar procesos y datos de un dispositivo móvil de otros procesos y datos del dispositivo móvil, y el contenedor de dispositivo móvil también está configurado para establecer una conexión segura con un número de VPN, teniendo cada VPN un perfil de VPN. La tarjeta inteligente está configurada para proporcionar, utilizando lógica criptográfica, tras solicitud del contenedor de dispositivo móvil, al menos, parte de un perfil de VPN de una VPN del número de VPN.

[0040] El perfil de VPN proporcionado por la tarjeta inteligente puede comprender, al menos, uno de los siguientes: autentificación de desafío-respuesta, identificación de usuario (ID), ID de dispositivo móvil, ID de contenedor de dispositivo móvil, clave criptográfica, clave encriptada, clave privada, clave pública, certificado, certificado de clave pública, secreto genérico, número de identificación personal (PIN), contraseña, contraseña de un solo uso, clave API, token de API, identificación biométrica, identificación de huellas dactilares, identificación de venas de la palma de la mano, identificación facial, identificación de ADN, identificación de la palma de la mano, identificación del iris, identificación de la geometría de la mano, identificación de la retina, identificación ID de voz, información del servidor de VPN, número de puerto, nombre de servidor, dirección de red, sistema de destino, información de configuración, información de tiempo de espera, información de compresión, dirección IP, número de identificación. El perfil de VPN proporcionado por la tarjeta inteligente puede proporcionarse en texto plano y/o cifrado.

[0041] La tarjeta inteligente puede además configurarse, tras una solicitud posterior del contenedor de dispositivo móvil, para proporcionar selectivamente, al menos, parte de un perfil de VPN posterior, solamente si el contenedor de dispositivo móvil estableció con éxito una conexión segura con la VPN.

[0042] La tarjeta inteligente puede además comprender un mecanismo de desbloqueo para que el contenedor de dispositivo móvil la desbloquee.

[0043] La tarjeta inteligente también puede configurarse para recibir actualizaciones de la memoria y/o la lógica criptográfica que se almacenan en el contenedor de dispositivo móvil y se reenvían a la tarjeta inteligente a través de la interfaz de comunicación.

[0044] Otro aspecto de la presente invención se refiere a un contenedor de dispositivo móvil. El contenedor de dispositivo móvil está configurado para aislar una parte del dispositivo móvil de otra parte del dispositivo móvil. El contenedor de dispositivo móvil comprende una primera interfaz que está configurada para conectarse de forma segura a un número de VPN y a una segunda interfaz que está configurada para comunicarse con una tarjeta de circuito integrado (ICC). La ICC está configurada para proporcionar, al menos, parte de un perfil de VPN de una VPN del número de VPN. Para establecer una conexión segura con la VPN del número de VPN mediante la primera interfaz, el contenedor de dispositivo móvil está configurado para acceder, al menos, a parte del perfil de VPN de la VPN del número de VPN mediante la segunda interfaz.

[0045] El contenedor de dispositivo móvil puede además configurarse para solicitar a un usuario que introduzca un código de autentificación para desbloquear la ICC.

[0046] Otro aspecto de la presente invención se refiere a un método para establecer una conexión segura entre un contenedor de dispositivo móvil y un número de VPN. El contenedor de dispositivo móvil está configurado para aislar una parte de un dispositivo móvil de otra parte del dispositivo móvil. El método comprende las etapas de

- acceder, al menos, a parte de un perfil de VPN de una VPN del número de VPN desde una tarjeta inteligente, en donde la etapa de acceder, al menos, a parte de un perfil de VPN además comprende procesos criptográficos,
- conectarse a la VPN.

[0047] El método puede además comprender las etapas de

- acceder, al menos, a parte de un perfil de VPN de una VPN posterior del número de VPN proporcionadas selectivamente tras conectarse correctamente a la VPN mediante, al menos, uno de entre
  - la tarjeta inteligente,
  - el contenedor de dispositivo móvil,
  - la VPN del número de VPN,
  - el enlace de comunicación,
  - un token criptográfico,
- conectarse a la VPN posterior.

[0048] La expresión "procesos criptográficos" se puede utilizar en el presente documento para indicar cualquiera de los procesos de descifrado o cifrado, creación de firmas digitales, mecanismos de intercambio de claves (por ejemplo, intercambio de claves Diffie-Hellman) o creación de códigos de autentificación de mensajes utilizando criptografía

simétrica o asimétrica. Dichos procesos criptográficos pueden comprender la utilización de una tarjeta inteligente.

[0049] La etapa de acceder, al menos, a parte de un perfil de VPN también puede comprender extraer, al menos, parte del perfil de VPN. Después de la extracción, la al menos parte del perfil de VPN puede almacenarse dentro del contenedor de dispositivo móvil y, de este modo, hacerse accesible permanentemente. Este puede ser el caso, por ejemplo, de las tarjetas inteligentes configuradas para un solo uso.

Breve descripción de los dibujos

[0050] Las características de los ejemplos se describirán, a modo de ejemplo, en la siguiente descripción detallada con referencia a los dibujos adjuntos, en los que los números de referencia similares corresponden a componentes similares, aunque quizás no idénticos. Por razones de brevedad, los números de referencia o las características que tienen una función descrita anteriormente pueden o no describirse en conexión con otros dibujos en los que aparecen.

[0051] A continuación, se describirán algunos ejemplos no limitativos con referencia a los dibujos adjuntos, en los que:

la Figura 1 muestra una ilustración esquemática de un sistema ilustrativo para establecer una conexión segura entre un contenedor de dispositivo móvil y un número de VPN.

la Figura 2 muestra una ilustración esquemática de un sistema ilustrativo para establecer una conexión segura entre un contenedor de dispositivo móvil y una VPN que incluye dos tókenes criptográficos.

las Figuras 3a - 3c muestran ilustraciones esquemáticas de configuraciones ilustrativas de un número de VPN.

la Figura 4 muestra una interfaz gráfica de usuario simplificada de un mecanismo de desbloqueo ilustrativo de un token criptográfico.

la Figura 5 muestra una ilustración esquemática de una tarjeta inteligente ilustrativa.

la Figura 6 muestra una ilustración esquemática de un contenedor de dispositivo móvil ilustrativo que comprende dos interfaces.

la Figura 7 y Figura 8 se refieren a métodos ilustrativos para establecer una conexión segura entre un contenedor de dispositivo móvil y un número de VPN.

Descripción detallada

[0052] La Figura 1 muestra una ilustración esquemática simplificada de un sistema 2 para establecer una conexión segura 12 entre un contenedor de dispositivo móvil 6 que está implementado en un dispositivo móvil 4 y un número de VPN 8. En la Figura 1, el número de VPN 8 es igual a una VPN. El sistema 2 comprende un token criptográfico 10. El token criptográfico se proporciona en una tarjeta inteligente 16. El token criptográfico 10 proporciona un perfil de VPN 18, 20. El perfil de VPN incluye información 18 del servidor de VPN que, por ejemplo, indica una dirección de red de destino. El perfil de VPN incluye además una clave de autentificación 20 para la autentificación del contenedor de dispositivo móvil 6 hacia la VPN 8. El token criptográfico 10 y el contenedor de dispositivo móvil 6 están enlazados por un enlace de comunicación 14. Para establecer una conexión segura 12 con la VPN, el contenedor de dispositivo móvil 6 accede a la información 18 del servidor de VPN y a la clave de autentificación 20 desde el token criptográfico 10 a través del enlace de comunicación 14. El contenedor de dispositivo móvil 6 extrae y almacena la información 18 del servidor de VPN y la clave de autentificación 20 para accesibilidad permanente.

[0053] La Figura 2 muestra otro ejemplo esquemático del sistema 2 para establecer una conexión segura entre un contenedor de dispositivo móvil 6 y un número de VPN 8 que comprende dos tókenes criptográficos 10, 22. En el presente documento, el número de VPN 8 también es igual a uno. La tarjeta inteligente 16 proporciona un token criptográfico 10 e incluye información 18 del servidor de VPN. El contenedor de dispositivo móvil 6 y el token criptográfico 10 están enlazados por el enlace de comunicación 14. Un medio de comunicación de campo cercano 24 proporciona otro token criptográfico 22 e incluye la clave de autentificación 20. El contenedor de dispositivo móvil 6 y el token criptográfico 22 están enlazados por el enlace de comunicación 26. Para conectarse de forma segura a la VPN del número de VPN 8, el contenedor de dispositivo móvil 6 accede a la información 18 del servidor de VPN desde el token criptográfico 10 a través del enlace de comunicación 14, y a la clave de autentificación 20 desde el token criptográfico 22 a través del enlace de comunicación 26. Cualquiera de los tókenes criptográficos 10, 22 o el contenedor de dispositivo móvil 6 indica dónde encontrar las diferentes partes del perfil de VPN (no se muestra).

[0054] Las Figuras 3a a 3c ilustran configuraciones ilustrativas del número de VPN 8. En la Figura 3a, el número de VPN comprende una VPN 28. Por consiguiente, es necesario un perfil de VPN para establecer una conexión segura con esta VPN 28.

[0055] La Figura 3b muestra una configuración de VPN de múltiples saltos con tres VPN posteriores 28a, 28b, 28c. Por ejemplo, las tres VPN posteriores 28a, 28b, 28c corresponden a diferentes VPN dentro de una empresa, gobierno, institución educativa u otra entidad. La VPN 28a corresponde a la VPN principal de la entidad, la VPN 28b corresponde a una VPN de departamento de la entidad, mientras que la 28c corresponde a una VPN de equipo. Partes del perfil de VPN de la respectiva VPN posterior son proporcionadas por la VPN anterior después de que el contenedor de dispositivo móvil se conecte correctamente a la VPN anterior (no se muestra). Por ejemplo, la información del servidor de VPN de la VPN 28b la proporciona la VPN 28a una vez que se ha establecido una conexión segura con la VPN 28a.

[0056] La Figura 3c muestra una configuración de VPN en cascada del número de VPN 8. En el presente documento, la VPN 28 específica se ramifica en más de una VPN posterior.

[0057] La Figura 4 ilustra una interfaz gráfica de usuario simplificada e ilustrativa de un mecanismo de desbloqueo 30 de la tarjeta inteligente 16. La interfaz gráfica de usuario 30 solicita a un usuario del contenedor de dispositivo móvil 6 que introduzca un PIN para desbloquear la tarjeta inteligente. Una vez introducido el PIN correctamente, el contenedor de dispositivo móvil 6 puede acceder al token criptográfico 10 proporcionado por la tarjeta inteligente 16 a través del enlace de comunicación 14.

[0058] La Figura 5 muestra una ilustración esquemática de un ejemplo de una tarjeta inteligente 16. La tarjeta inteligente 16 comprende memoria 32, lógica criptográfica 34, una unidad central de procesamiento 36 y una interfaz de comunicación 38. La interfaz de comunicación 38 está configurada para comunicarse por cable o inalámbricamente a través del enlace de comunicación 14 con un contenedor de dispositivo móvil 6 de un dispositivo móvil 4. La tarjeta inteligente 16 proporciona, tras la solicitud del contenedor de dispositivo móvil 6, al menos, parte de un perfil de VPN de la memoria 32.

[0059] La Figura 6 muestra una ilustración esquemática de un contenedor de dispositivo móvil 6 ilustrativo con dos interfaces 40, 42. El contenedor de dispositivo móvil 6 se implementa dentro de un dispositivo móvil 4. La primera interfaz 40 está configurada para conectarse a través de una conexión segura 12 a un número de VPN 8. La segunda interfaz 42 está configurada para comunicarse con una ICC. El contenedor de dispositivo móvil 4 accede, al menos, a parte de un perfil de VPN de una VPN del número de VPN 8 desde la ICC 44 a través de la segunda interfaz 42. A partir de entonces, el contenedor de dispositivo móvil 6 se conecta a la VPN del número de VPN 8 a través de la primera interfaz 40.

[0060] Las Figuras 7 y 8 se refieren a métodos ilustrativos 700, 800 para establecer una conexión segura entre un contenedor de dispositivo móvil y un número de VPN. En la Figura 7, el método 700 comprende la etapa 710 de acceder, al menos, a parte de un perfil de VPN de una VPN del número de VPN desde una tarjeta inteligente. El método 700 además comprende la etapa 710 de conectarse a la VPN. A partir de entonces, en la etapa 720, se accede, al menos, a parte de un perfil de VPN de una VPN posterior del número de VPN que se proporciona selectivamente tras conectarse correctamente a la VPN mediante, al menos, uno de entre la tarjeta inteligente, el contenedor de dispositivo móvil, la VPN del número de VPN, el enlace de comunicación, un token criptográfico. El método además comprende conectarse a la VPN posterior en la etapa 730.

[0061] La Figura 8 muestra otro método 800 que comprende el método 700. Además de la misma, la primera etapa 810, que se refiere al acceso, al menos, a parte de un perfil de VPN de una VPN del número de VPN desde una tarjeta inteligente, también comprende procesos criptográficos.

Lista de símbolos de referencia	
2	sistema para establecer una conexión segura entre un contenedor de dispositivo móvil y una VPN
4	dispositivo móvil
6	contenedor de dispositivo móvil
8	un número de VPN
10	token criptográfico
12	conexión segura
14	enlace de comunicación
16	tarjeta inteligente
18	información del servidor de VPN
20	clave de autentificación
22	token criptográfico adicional
24	chip NFC
26	enlace de comunicación adicional
28	VPN
28a, 28b, 28c	VPN posterior
30	interfaz gráfica de usuario del mecanismo de desbloqueo
32	memoria

(continuación)

Lista de símbolos de referencia	
34	lógica criptográfica
36	unidades de procesamiento central
38	interfaz de comunicación
40	primera interfaz
42	segunda interfaz
44	tarjeta de circuito integrado

REIVINDICACIONES

1. Un sistema (2) para establecer una conexión segura (12) entre un contenedor de dispositivo móvil (6) y un número de redes privadas virtuales, VPN, (8) que comprende:

- un contenedor de dispositivo móvil (6), configurado para aislar una parte de un dispositivo móvil (4) de otra parte del dispositivo móvil (4);
- un número de VPN (8), teniendo cada una del número de VPN (8) un perfil de VPN (18, 20);
- un token criptográfico (10), configurado para proporcionar, al menos, parte del perfil de VPN (18, 20) de, al menos, una del número de VPN (8);
- un enlace de comunicación (14), configurado para enlazar el contenedor de dispositivo móvil (6) y el token criptográfico (10);

en donde, para establecer una conexión segura con, al menos, una primera VPN del número de VPN (8), el contenedor de dispositivo móvil (6) está configurado para acceder, al menos, a parte del perfil de VPN (18, 20) de la al menos una primera VPN del número de VPN (8) a través del enlace de comunicación (14) configurado para enlazar el contenedor de dispositivo móvil (6) y el token criptográfico (10); **caracterizado por que** para establecer una conexión segura con una VPN posterior del número de VPN (8), el sistema (2) está además configurado para proporcionar selectivamente, al menos, parte del perfil de VPN de la VPN posterior, solamente si la conexión entre el contenedor de dispositivo móvil (6) y la al menos una primera VPN se ha establecido correctamente.

2. El sistema (2) de acuerdo con la reivindicación 1, en donde el número de VPN (8) está configurado para cualquiera de

- una VPN de múltiples saltos,
- una VPN de doble salto,
- una VPN encadenada,
- una VPN en cascada,
- VPN posterior.

3. El sistema (2) de acuerdo con cualquiera de las reivindicaciones anteriores, en donde el sistema (2) está configurado para proporcionar una parte adicional del perfil de VPN (18, 20) de la al menos una primera VPN del número de VPN para establecer la conexión segura con la al menos una primera VPN del número de VPN (8), en donde al menos uno de entre

- el contenedor de dispositivo móvil (6),
- la VPN del número de VPN (8),
- el enlace de comunicación (14),
- un token criptográfico adicional (22),

está configurado para proporcionar la parte adicional del perfil de VPN (18, 20).

4. El sistema (2) de acuerdo con la reivindicación 3, que además comprende

- un enlace de comunicación adicional (26), configurado para enlazar el contenedor de dispositivo móvil (6) y el token criptográfico adicional (22);
- en donde, para establecer la conexión segura con la al menos una primera VPN del número de VPN (8), el contenedor de dispositivo móvil (6) está configurado para acceder a la parte adicional del perfil de VPN de la al menos una primera VPN del número de VPN (8).

5. El sistema (2) de acuerdo con la reivindicación 1, en donde, al menos, parte del perfil de VPN de la VPN posterior está proporcionado selectivamente por, al menos, uno de entre

- el token criptográfico (10),
- el contenedor de dispositivo móvil (6),
- la VPN del número de VPN (8),
- el enlace de comunicación (14),
- el token criptográfico adicional (22),
- el enlace de comunicación adicional (26).

6. El sistema (2) de acuerdo con cualquiera de las reivindicaciones anteriores, en donde el perfil de VPN de cada una del número de VPN comprende, al menos, uno de entre:

- una autentificación de desafío-respuesta,
- una identificación de usuario, ID,
- un ID de dispositivo móvil,

- una ID del contenedor de dispositivo móvil,
- una clave criptográfica,
- una clave encriptada,
- una clave privada,
- una clave pública,
- un certificado,
- un certificado de clave pública,
- un secreto genérico,
- un número de identificación personal, PIN,
- una contraseña,
- una contraseña de un solo uso,
- una clave de interfaz de programación de aplicaciones, API,
- un token de API,
- una identificación biométrica,
- una identificación de huellas dactilares,
- una identificación de las venas de la palma de la mano,
- una identificación facial,
- una identificación de ADN,
- una identificación de la palma de la mano,
- una identificación del iris,
- una identificación de la geometría de la mano,
- una identificación de la retina,
- una identificación ID de voz,
- información del servidor de VPN,
- un número de puerto,
- un nombre de servidor,
- una dirección de red,
- un sistema de destino,
- información de configuración,
- información de tiempo de espera,
- información de compresión,
- una dirección IP,
- un número de identificación

en, al menos, uno de entre

- texto plano
- texto cifrado.

7. El sistema (2) de acuerdo con cualquiera de las reivindicaciones anteriores, en donde el token criptográfico (10, 22) está proporcionado por, al menos, uno de entre:

- una tarjeta inteligente,
- una tarjeta de circuito integrado, ICC,
- un medio de bus universal en serie, USB,
- un código de respuesta rápida, QR,
- un medio óptico,
- un medio de audio,
- un medio fotográfico,
- un medio holográfico,
- un generador de número de autentificación de transacción, TAN,
- un reloj inteligente,
- un medio de comunicación de campo cercano, NFC,
- un medio de identificación por radiofrecuencia, RFID,
- un usuario.

y en donde el enlace de comunicación comprende, al menos, uno de entre

- *Bluetooth*,
- un lector de tarjetas con cable,
- un lector de tarjetas inalámbrico,
- NFC,
- RFID,
- una red de área corporal, BAN,
- un dispositivo de reconocimiento biométrico,
- un dispositivo de reconocimiento óptico,
- un dispositivo de reconocimiento QR,
- un dispositivo de reconocimiento de huellas dactilares,

- un dispositivo de reconocimiento de las venas de la palma de la mano,
- un dispositivo de reconocimiento facial,
- un dispositivo de reconocimiento de ADN,
- un dispositivo de reconocimiento de la palma de la mano,
- un dispositivo de reconocimiento del iris,
- un dispositivo de reconocimiento de la geometría de la mano,
- un dispositivo de reconocimiento de la retina,
- un dispositivo de reconocimiento de identificación de voz.

8. Una tarjeta inteligente (16), que comprende:

- una memoria (32),
- una lógica criptográfica (34),
- una unidad de procesamiento central (36),
- una interfaz de comunicación (38) configurada para comunicarse con un contenedor de dispositivo móvil (6), en donde el contenedor de dispositivo móvil (6) está configurado para establecer una conexión segura con, al menos, una primera VPN de un número de redes privadas virtuales, VPN (8), teniendo cada VPN un perfil de VPN,
en donde la tarjeta inteligente (16) está configurada para proporcionar, utilizando la lógica criptográfica (34), tras una solicitud del contenedor de dispositivo móvil (6), al menos, parte de un perfil de VPN de la al menos una primera VPN del número de VPN (8); **caracterizada por que**
la tarjeta inteligente (16) está además configurada, tras una solicitud posterior del contenedor de dispositivo móvil (6), para proporcionar selectivamente, al menos, parte de un perfil de VPN de una VPN posterior del número de VPN (8), solamente si el contenedor de dispositivo móvil (6) ha establecido correctamente la conexión segura con la al menos una primera VPN.

9. La tarjeta inteligente (16) de acuerdo con la reivindicación 8, en donde el perfil de VPN (18, 20) comprende, al menos, uno de los siguientes:

- una autentificación de desafío-respuesta,
- una identificación de usuario, ID,
- un ID de dispositivo móvil,
- una ID del contenedor de dispositivo móvil,
- una clave criptográfica,
- una clave encriptada,
- una clave privada,
- una clave pública,
- un certificado,
- un certificado de clave pública,
- un secreto genérico,
- un número de identificación personal, PIN,
- una contraseña,
- una contraseña de un solo uso,
- una clave API,
- un token de API,
- una identificación biométrica,
- una identificación de huellas dactilares,
- una identificación de las venas de la palma de la mano,
- una identificación facial,
- una identificación de ADN,
- una identificación de la palma de la mano,
- una identificación del iris,
- una identificación de la geometría de la mano,
- una identificación de la retina,
- una identificación ID de voz
- información del servidor de VPN,
- un número de puerto,
- un nombre de servidor,
- una dirección de red,
- un sistema de destino,
- información de configuración,
- información de tiempo de espera,
- información de compresión,
- una dirección IP,
- un número de identificación,

en, al menos, uno de entre

- texto plano

- texto cifrado.

10. Un contenedor de dispositivo móvil (6), configurado para aislar una parte del dispositivo móvil (4) de otra parte del dispositivo móvil (4), que comprende

- una primera interfaz (40), configurada para conectarse de forma segura a un número de redes privadas virtuales, VPN (8),

- una segunda interfaz (42), configurada para comunicarse con una tarjeta inteligente (16), en donde la tarjeta inteligente (16) está configurada para proporcionar, al menos, parte de un perfil de VPN (18, 20) de, al menos, una primera VPN del número de VPN (8) y, al menos, parte de un perfil de VPN de una VPN posterior del número de VPN (8),
en donde, para establecer una conexión segura con la al menos una primera VPN del número de VPN (8) a través de la primera interfaz (40), el contenedor de dispositivo móvil (6) está configurado para, tras una solicitud a la tarjeta inteligente (16), acceder, al menos, a parte del perfil de VPN (18, 20) de la al menos una primera VPN del número de VPN (8) a través de la segunda interfaz (42), y
en donde, para establecer una conexión segura con una VPN posterior del número de VPN (8), el contenedor de dispositivo móvil (6) está configurado para, tras una solicitud posterior a la tarjeta inteligente (16), recibir selectivamente, al menos, la parte del perfil de VPN de la VPN posterior, solamente si el contenedor de dispositivo móvil (6) ha establecido correctamente la conexión segura con la al menos una primera VPN.

11. El contenedor de dispositivo móvil (6) de acuerdo con la reivindicación 10, en donde el perfil de VPN (18, 20) comprende, al menos, uno de los siguientes:

- una autentificación de desafío-respuesta,
- una identificación de usuario, ID,
- un ID de dispositivo móvil,
- una ID del contenedor de dispositivo móvil,
- una clave criptográfica,
- una clave encriptada,
- una clave privada,
- una clave pública,
- un certificado,
- un certificado de clave pública,
- un secreto genérico,
- un número de identificación personal, PIN,
- una contraseña,
- una contraseña de un solo uso,
- una clave API,
- un token de API,
- una identificación biométrica,
- una identificación de huellas dactilares,
- una identificación de las venas de la palma de la mano,
- una identificación facial,
- una identificación de ADN,
- una identificación de la palma de la mano,
- una identificación del iris,
- una identificación de la geometría de la mano,
- una identificación de la retina,
- una identificación ID de voz
- información del servidor de VPN,
- un número de puerto,
- un nombre de servidor,
- una dirección de red,
- un sistema de destino,
- información de configuración,
- información de tiempo de espera,
- información de compresión,
- una dirección IP,
- un número de identificación,

en, al menos, uno de entre
- texto plano
- texto cifrado.

12. Un método (700; 800) para establecer una conexión segura entre un contenedor de dispositivo móvil (6), configurado para aislar una parte de un dispositivo móvil (4) de otra parte del dispositivo móvil (4), y un número de

redes privadas virtuales, VPN, (8), que comprende las etapas de:

- acceder (710), al menos, a parte de un perfil de VPN (18, 20) de, al menos, una primera VPN del número de VPN (8) desde una tarjeta inteligente (16), en donde la etapa de acceder (710), al menos, a parte de un perfil de VPN además comprende procesos criptográficos (810);
- conectarse (720) a la al menos una primera VPN; **caracterizado por**
- acceder (730), al menos, a parte de un perfil de VPN (18, 20) de una VPN posterior del número de VPN proporcionadas selectivamente tras conectarse correctamente a la al menos una primera VPN mediante, al menos, uno de entre

  - la tarjeta inteligente (16),
  - el contenedor de dispositivo móvil (6),
  - la VPN del número de VPN (8),
  - el enlace de comunicación (14),
  - un token criptográfico (10, 22); y

- conectarse (730) a la VPN posterior.

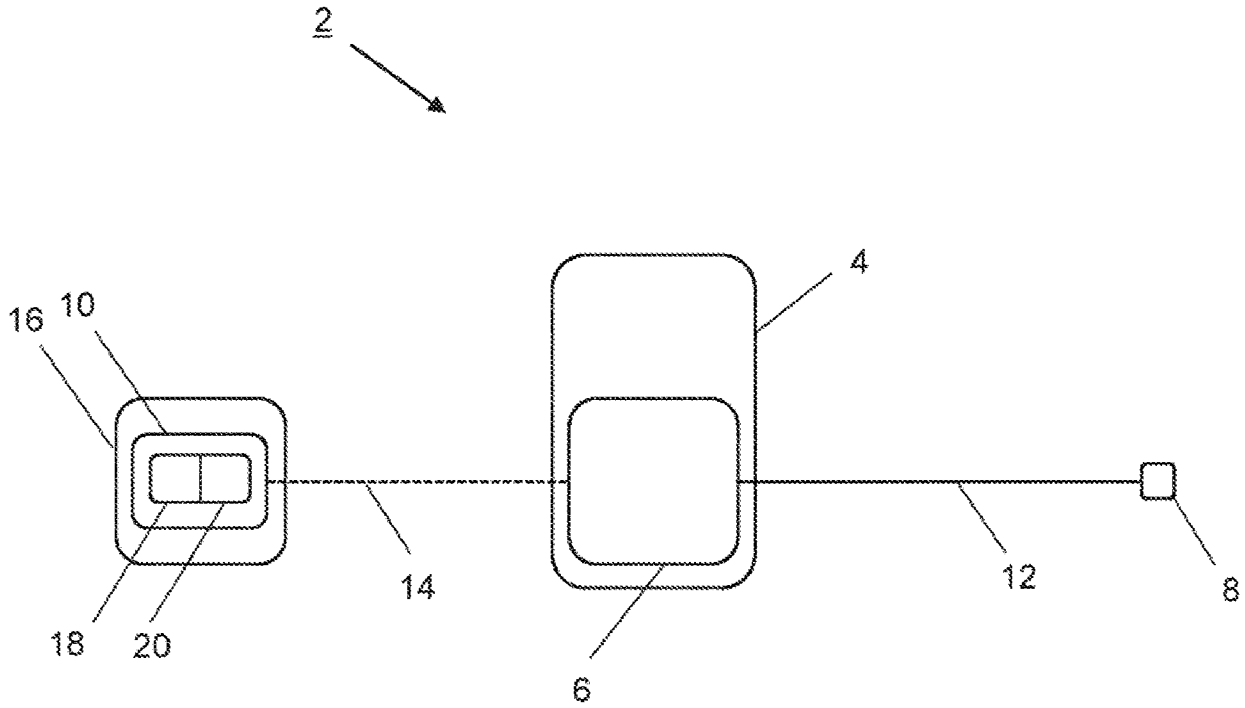

Fig. 1

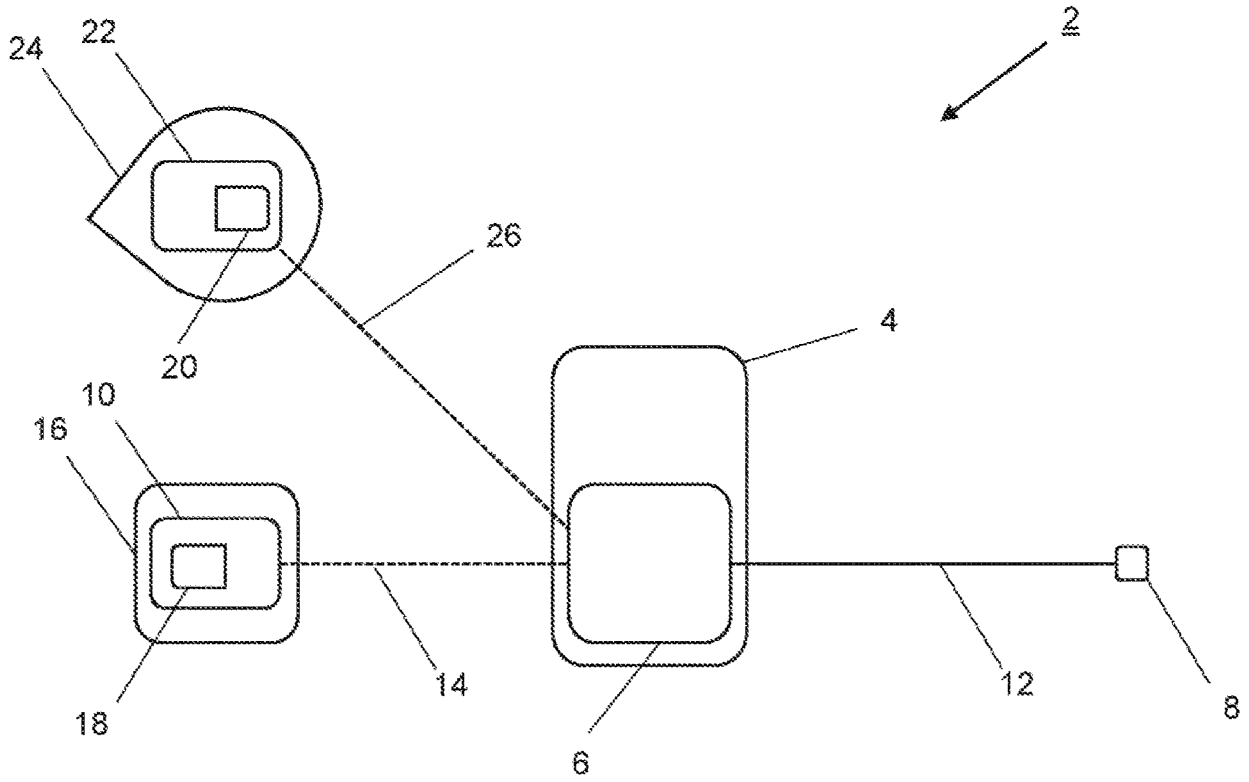

Fig. 2

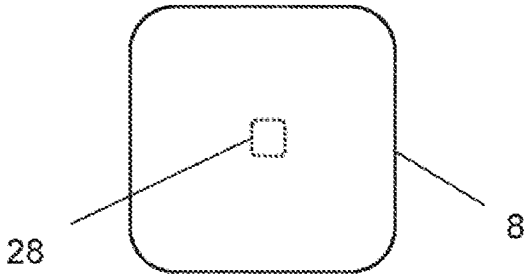

Fig. 3a

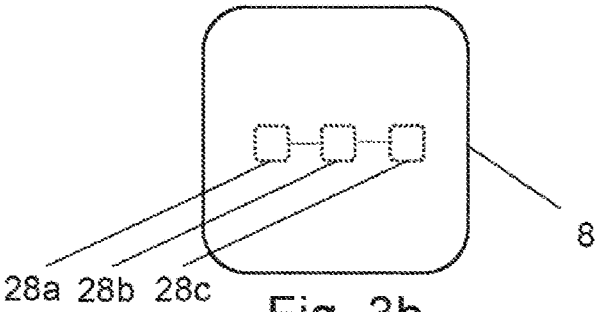

Fig. 3b

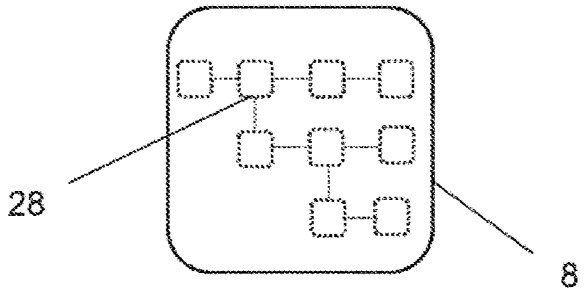

Fig. 3c

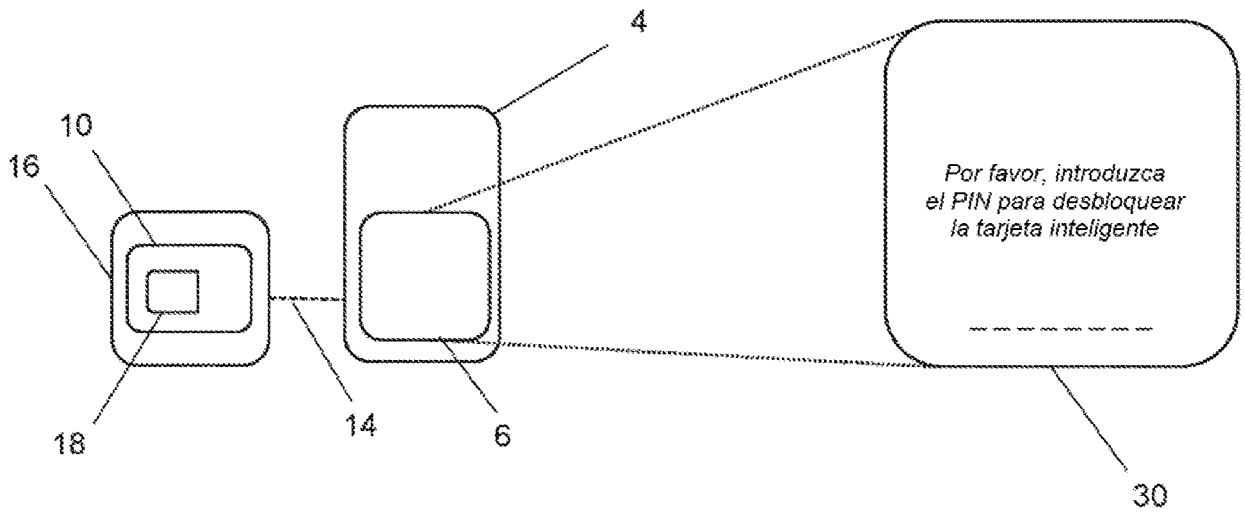
4
10
16
Por favor, introduzca
el PIN para desbloquear
la tarjeta inteligente
18
14
6
30

Fig. 4

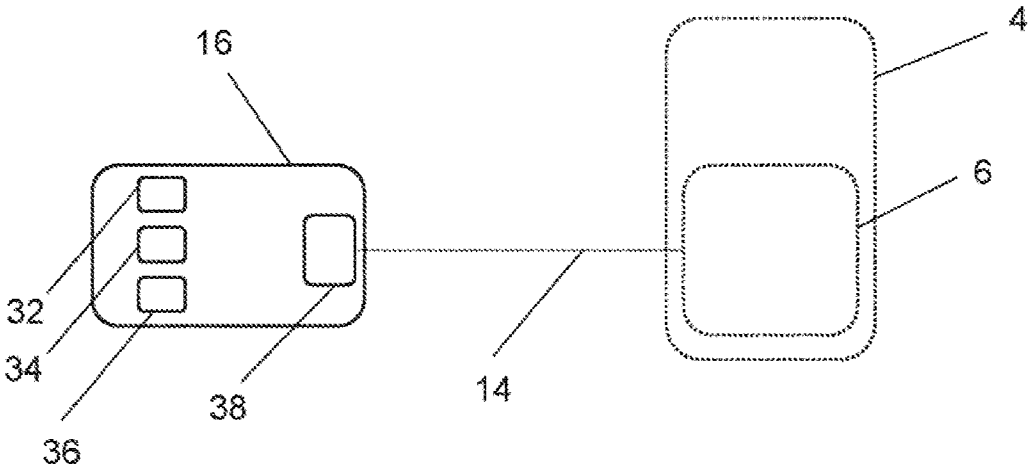

Fig. 5

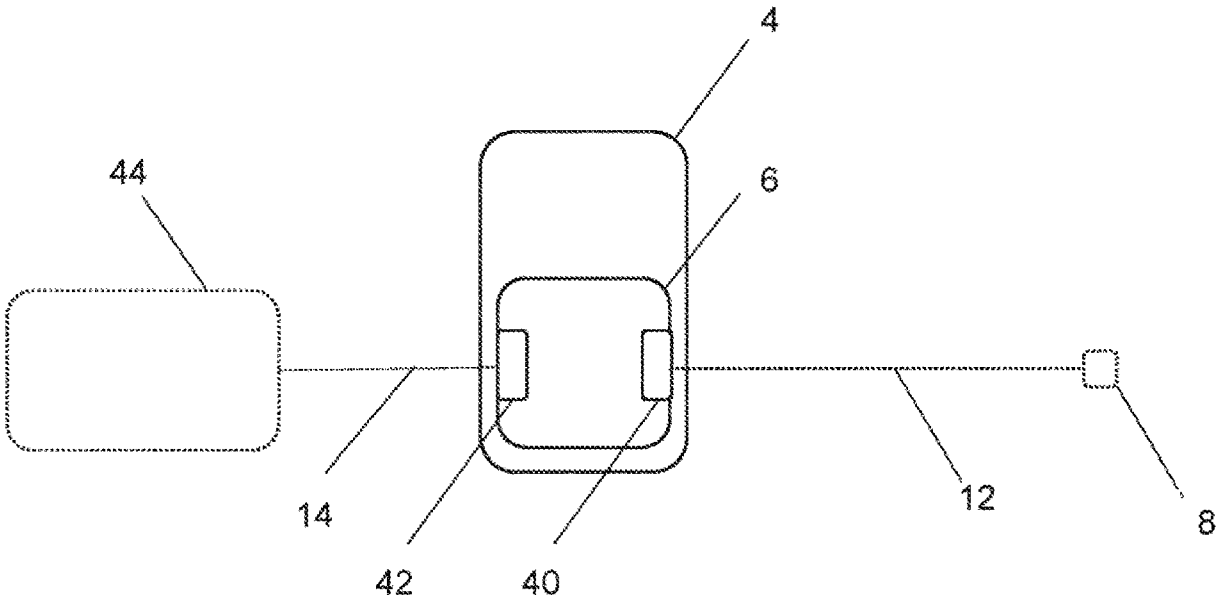

Fig. 6

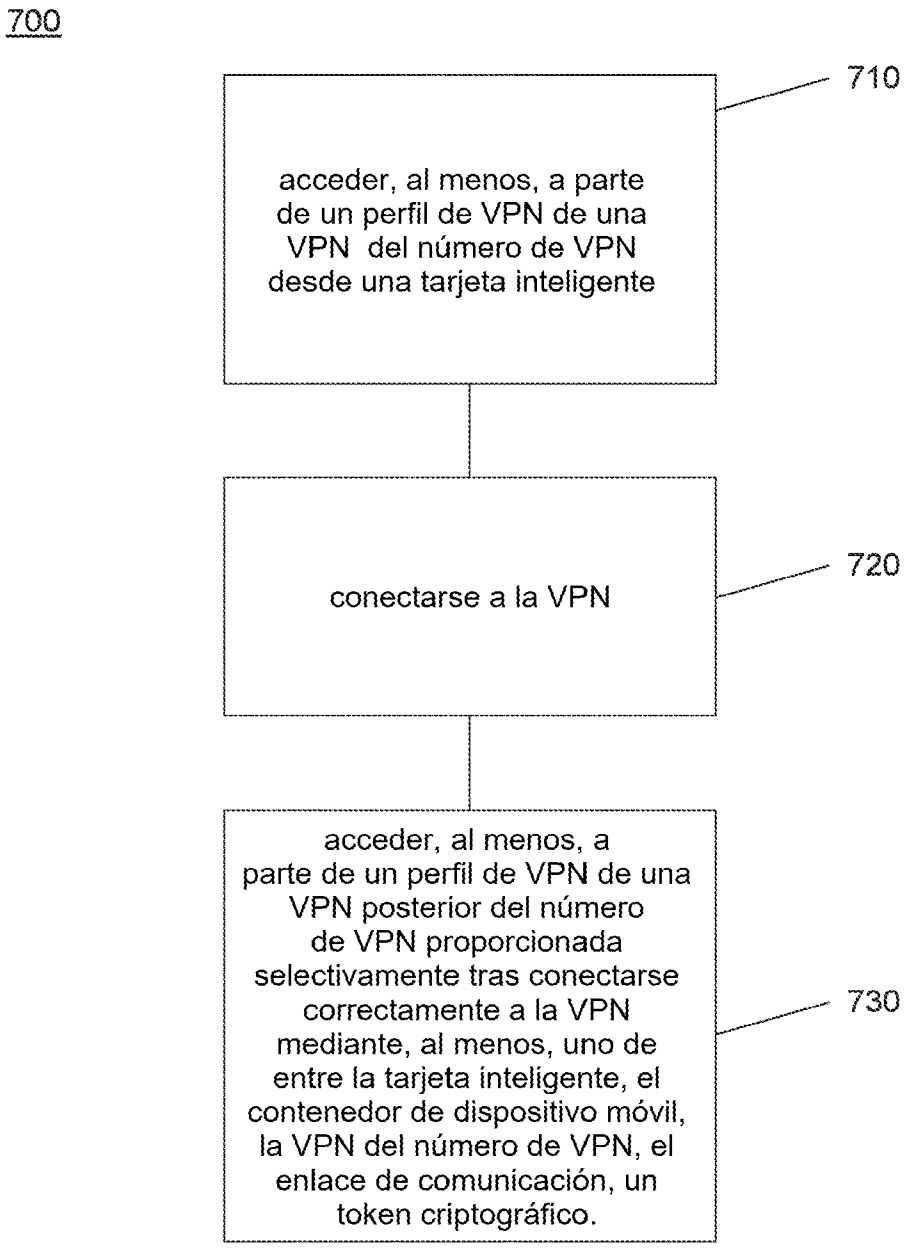
700
710
acceder, al menos, a parte de un perfil de VPN de una VPN del número de VPN desde una tarjeta inteligente
720
conectarse a la VPN
730
acceder, al menos, a parte de un perfil de VPN de una VPN posterior del número de VPN proporcionada selectivamente tras conectarse correctamente a la VPN mediante, al menos, uno de entre la tarjeta inteligente, el contenedor de dispositivo móvil, la VPN del número de VPN, el enlace de comunicación, un token criptográfico.

Fig. 7

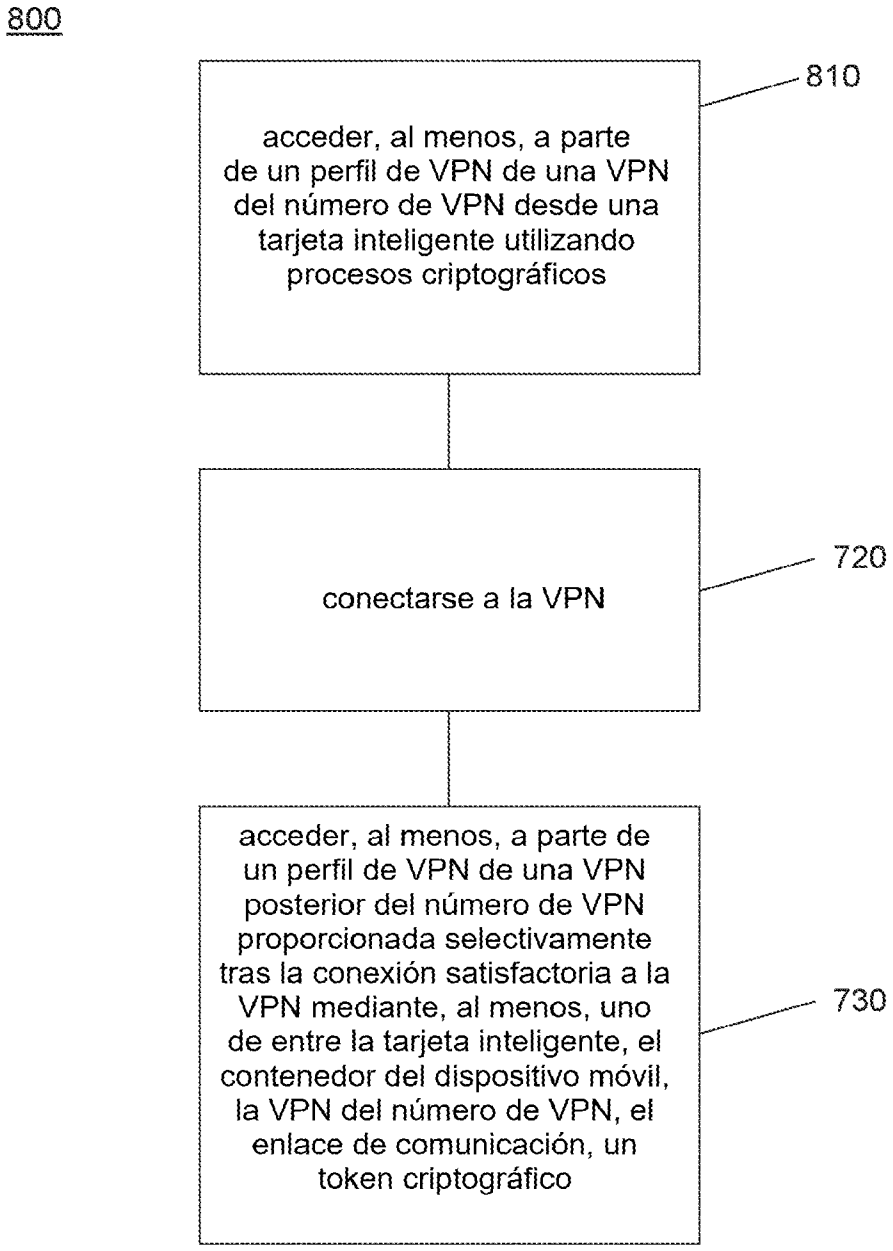
800
acceder, al menos, a parte de un perfil de VPN de una VPN del número de VPN desde una tarjeta inteligente utilizando procesos criptográficos
810
conectarse a la VPN
720
acceder, al menos, a parte de un perfil de VPN de una VPN posterior del número de VPN proporcionada selectivamente tras la conexión satisfactoria a la VPN mediante, al menos, uno de entre la tarjeta inteligente, el contenedor del dispositivo móvil, la VPN del número de VPN, el enlace de comunicación, un token criptográfico
730

Fig. 8