(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 715 198**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/08 (2009.01)
H04W 4/80 (2008.01)
H04W 4/02 (2008.01)
H04W 4/021 (2008.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **15.08.2017 E 17020357 (4)**

(97) Fecha y número de publicación de la concesión europea: **12.12.2018 EP 3291503**

(54) Título: **Procedimiento y dispositivos para transmitir un paquete de datos seguro a un dispositivo de comunicación**

(30) Prioridad:

06.09.2016 WO PCT/CH2016/001149

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.06.2019

(73) Titular/es:

LEGIC IDENTSYSTEMS AG (100.0%)
Binzackerstrasse, 41
8620 Wetzikon, CH

(72) Inventor/es:

BUCK, MARTIN;
PLÜSS, PETER y
PLÜSS, MARCEL

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

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

Procedimiento y dispositivos para transmitir un paquete de datos seguro a un dispositivo de comunicación

Campo de la invención

La presente invención se refiere a un procedimiento y dispositivos para transmitir un paquete de datos seguro desde un sistema informático a un dispositivo de comunicación de corto alcance. Específicamente, la presente invención se refiere a un aparato de comunicación móvil, un dispositivo de comunicación de corto alcance y un procedimiento para transmitir un paquete de datos seguro desde un sistema informático al dispositivo de comunicación de corto alcance.

Antecedentes de la invención

Durante muchos años, los dispositivos terminales electrónicos se han instalado y usado en los sistemas de control de acceso en relación con los transpondedores de RFID pasivos (identificador de radio frecuencia). Los dispositivos terminales electrónicos se configuraron como dispositivos de comunicación de corto alcance y se incluyeron lectores de RFID para leer de manera inalámbrica los derechos de acceso o al menos los identificadores de usuario a partir de los transpondedores de RFID para controlar el acceso a un área de acceso controlado, tal como un edificio o una habitación, o para acceder a objetos controlados, tal como un automóvil o mercancías en una máquina expendedora, etc. Con la llegada de los teléfonos de radio móviles (teléfonos móviles, teléfonos inteligentes) que incluían interfaces de comunicación basadas en RFID activos, llamadas interfaces de NFC (comunicación de campo cercano), se hizo posible usar tales aparatos de comunicación móvil como portadores de derechos de acceso en lugar de los transpondedores de RFID pasivos en forma de tarjetas de RFID, mochilas o similares. Tanto los operadores como los usuarios de los sistemas de control de acceso agradecieron la provisión de aparatos de comunicación móvil con módulos de comunicación basados en radio para establecer enlaces de comunicación inalámbricos locales o directos con los dispositivos de comunicación de corto alcance, ya que ya no era necesario usar los transpondedores de RFID de fin especial en la forma de tarjetas de RFID, mochilas o similares. Además, los aparatos de comunicación móvil incluían otras interfaces de comunicación para las comunicaciones de corto alcance, tal como Bluetooth (BT) o Bluetooth de baja energía (BLE), lo que lleva a los dispositivos de comunicación de corto alcance que además están equipados con tales interfaces de comunicación adicionales a mejorar la flexibilidad y la versatilidad. No obstante, mientras que el uso de aparatos de comunicación móvil y de los dispositivos de comunicación de corto alcance de flexibilidad y versatilidad mejoradas aumentaron aún más el número de aplicaciones e instalaciones de dispositivos de comunicación de corto alcance, la gestión y el control seguro de los derechos de acceso y las credenciales para los dispositivos de comunicación de corto alcance continuaron siendo un desafío y, por lo general, requerían un cableado laborioso y costoso de los terminales a los sistemas secundarios. Además, los llamados terminales autónomos o fuera de línea sin enlaces de comunicación a los sistemas secundarios son difíciles de mantener y se mantienen actualizados con las frecuentes actualizaciones de software e innovaciones de hardware de los teléfonos móviles, en particular, y los cortos ciclos de vida del producto de costumbre en el mundo de los productos electrónicos de consumo, en general.

Sumario de la invención

Un objeto de esta invención es proporcionar un procedimiento y dispositivos para transmitir un paquete de datos seguro desde un sistema informático a un dispositivo de comunicación de corto alcance, procedimiento y dispositivos que no tengan al menos algunas de las desventajas de la técnica anterior.

De acuerdo con la presente invención, estos objetos se consiguen a través de las características de las reivindicaciones independientes. Además, otras realizaciones ventajosas se deducen de las reivindicaciones dependientes y la descripción.

Un aparato de comunicación móvil comprende un primer circuito configurado para la comunicación de datos a través de una red de radio móvil, un segundo circuito configurado para la comunicación de corto alcance con un dispositivo de comunicación de corto alcance, y un tercer circuito configurado para determinar la información de localización de aparato, indicativa de una localización actual del aparato de comunicación móvil.

De acuerdo con la presente invención, los objetos mencionados anteriormente se consiguen en particular por que el aparato de comunicación móvil comprende además un procesador conectado a los circuitos primero, segundo y tercero, y configurado para recibir a través de la red de radio móvil un paquete de datos seguro desde un sistema informático, para recibir la información de localización de dispositivo desde el dispositivo de comunicación de corto alcance, para determinar la autorización de acceso basándose en verificar la correspondencia de la información de localización de dispositivo y la información de localización de aparato, determinar la autorización de acceso afirmativa en caso de correspondencia de la información de localización de dispositivo y la información de localización de aparato, y determinar la autorización de acceso negativa a falta de correspondencia de la información de localización de dispositivo y la información de localización de aparato, y para transferir el paquete de datos seguro al dispositivo de comunicación de corto alcance, en el caso de una autorización de acceso afirmativa, y para no transferir el paquete de datos seguro al dispositivo de comunicación de corto alcance, en el caso de una autorización de acceso negativa. El uso de un aparato de comunicación móvil como intermediario de comunicación

hace posible transferir un paquete de datos seguro desde un sistema informático a un dispositivo de comunicación de corto alcance, que no tiene conectividad directa con el sistema informático. El paquete de datos seguro puede transferirse al dispositivo de comunicación de corto alcance en el modo en línea, cuando el aparato de comunicación móvil tiene conectividad con el sistema informático, y en el modo fuera de línea, cuando la comunicación móvil no tiene conectividad con el sistema informático. Al verificar en el aparato de comunicación móvil la correspondencia de la localización del aparato de comunicación móvil con la información de localización de dispositivo de comunicación de corto alcance, la transferencia del paquete de datos seguro (o de cualquier otro dato confidencial o crítico para el caso) desde el aparato de comunicación móvil al dispositivo de comunicación de corto alcance puede evitarse en escenarios comprometidos donde el dispositivo de comunicación de corto alcance (no cableado) se ha movido de manera fraudulenta a otra localización o se ha instalado por error en una localización que no corresponde a la localización de dispositivo almacenada en el dispositivo de comunicación de corto alcance. Además, el paquete de datos seguro (que incluye las claves criptográficas, los datos de configuración o cualquier otro dato confidencial o crítico) puede distribuirse a dispositivos de comunicación de corto alcance a través de una multitud de tecnologías de comunicación diferentes, por ejemplo, RFID, NFC, WLAN, BT, BLE, etc.

En una realización, la información de localización de dispositivo se recibe desde el dispositivo de comunicación de corto alcance incluida en una solicitud de lectura de datos, y el procesador está configurado para rechazar la solicitud de lectura, en el caso de una autorización de acceso negativa.

En una realización, el paquete de datos seguro se recibe con la información de localización de destino, y el procesador está configurado para determinar la autorización de acceso basándose además en verificar la correspondencia de la información de localización de dispositivo y la información de localización de destino, determinar la autorización de acceso afirmativa en caso de correspondencia de la información de localización de dispositivo y la información de localización de destino, y determinar la autorización de acceso negativa a falta de correspondencia de la información de localización de dispositivo y la información de localización de destino.

En una realización adicional, el procesador está configurado para recibir además la información de tiempo de dispositivo desde el dispositivo de comunicación de corto alcance, por ejemplo, incluida en la solicitud de lectura de datos, y para determinar la autorización de acceso adicional basándose en verificar la correspondencia de la información de tiempo de dispositivo y la información de tiempo almacenada en el aparato de comunicación móvil, determinar la autorización de acceso afirmativa en caso de correspondencia de la información de tiempo de dispositivo y la información de tiempo almacenada en el aparato de comunicación móvil, y determinar la autorización de acceso negativa a falta de correspondencia de la información de tiempo de dispositivo y la información de tiempo almacenada en el aparato de comunicación móvil.

En una realización, el paquete de datos seguro incluye una o más claves de acceso secretas, uno o más derechos de acceso, los datos de configuración para el dispositivo de comunicación de corto alcance, y/o la información de tiempo, y el procesador está configurado para transferir el paquete de datos seguro que incluye la una o más claves de acceso secretas, el uno o más derechos de acceso, los datos de configuración y/o la información de tiempo, respectivamente, al dispositivo de comunicación de corto alcance, en el caso de una autorización de acceso afirmativa, y para no transferir el paquete de datos seguro al dispositivo de comunicación de corto alcance, en el caso de una autorización de acceso negativa.

En una realización, el procesador está configurado para ejecutar protocolos de autenticación y control de acceso, que rigen la autenticación y el control de acceso entre el aparato de comunicación móvil y el dispositivo de comunicación de corto alcance, para acceder al dispositivo de comunicación de corto alcance para establecer la información de localización de dispositivo en el dispositivo de comunicación de corto alcance y, en el caso de autenticación afirmativa y control de acceso, para usar la información de localización de aparato para establecer la información de localización de dispositivo en el dispositivo de comunicación de corto alcance.

En una realización adicional, el procesador está configurado para ejecutar protocolos de autenticación y control de acceso, que rigen la autenticación y el control de acceso entre el aparato de comunicación móvil y el dispositivo de comunicación de corto alcance, para acceder al aparato de comunicación móvil, usando una o más claves de acceso secretas y/o derechos de acceso, para realizar al menos una de: una lectura de datos en un almacén de datos seguro del aparato de comunicación móvil, una escritura de datos en el almacén de datos seguro e interactuar con una aplicación segura del aparato de comunicación móvil.

Además del aparato de comunicación móvil, la presente invención también se refiere a un dispositivo de comunicación de corto alcance, que comprende un circuito configurado para la comunicación de corto alcance con un aparato de comunicación móvil y un procesador conectado al circuito. El procesador está configurado para recibir un paquete de datos desde el aparato de comunicación móvil. El paquete de datos incluye información de localización de aparato, indicativa de una localización actual del aparato de comunicación móvil. El procesador está configurado además para determinar la autorización de acceso basándose en verificar la correspondencia de la información de localización de dispositivo almacenada en el dispositivo de comunicación de corto alcance y la información de localización de aparato recibida desde el aparato de comunicación móvil, determinar la autorización de acceso afirmativa en caso de correspondencia de la información de localización de dispositivo y la información de localización de aparato, y determinar la autorización de acceso negativa a falta de correspondencia de la información

de localización de dispositivo y la información de localización de aparato. El procesador está configurado además para determinar y almacenar en el dispositivo de comunicación de corto alcance un contenido del paquete de datos recibido desde el aparato de comunicación móvil, en el caso de una autorización de acceso afirmativo, y rechazar el paquete de datos, en el caso de una autorización de acceso negativa. Al verificar en el dispositivo de comunicación de corto alcance la correspondencia de la localización del aparato de comunicación móvil con la información de localización de dispositivo de comunicación de corto alcance, puede evitarse la aceptación del paquete de datos del aparato de comunicación móvil en escenarios comprometidos donde el aparato de comunicación móvil se localiza en una localización diferente a la especificada y se almacena en el dispositivo de comunicación de corto alcance, por ejemplo, debido a un ataque remoto de interfaz extendida, o debido a una instalación del dispositivo de comunicación de corto alcance en una localización errónea.

En una realización, el procesador está configurado para recibir, a partir de la información de tiempo de aparato de comunicación móvil, y para determinar la autorización de acceso adicional basándose en verificar la correspondencia de información de tiempo de dispositivo almacenada en el dispositivo de comunicación de corto alcance y la información de tiempo recibida desde el aparato de comunicación móvil, determinar la autorización de acceso afirmativa en caso de correspondencia de la información de tiempo de dispositivo y la información de tiempo recibida desde el aparato de comunicación móvil, y determinar la autorización de acceso negativa a falta de correspondencia de la información de tiempo de dispositivo y la información de tiempo recibida desde el aparato de comunicación móvil.

En una realización adicional, el procesador está configurado para extraer del paquete de datos seguro una o más claves de acceso secretas, uno o más derechos de acceso, los datos de configuración para el dispositivo de comunicación de corto alcance, y/o la información de tiempo; y almacenar en un almacén de datos seguro del dispositivo de comunicación de corto alcance la una o más claves de acceso secretas, el uno o más derechos de acceso, los datos de configuración y/o la información de tiempo, respectivamente.

En una realización, el procesador está configurado para ejecutar protocolos de autenticación y control de acceso, que rigen la autenticación y el control de acceso entre el dispositivo de comunicación de corto alcance y el aparato de comunicación móvil, para acceder al dispositivo de comunicación de corto alcance para establecer la información de localización de dispositivo en el dispositivo de comunicación de corto alcance y, en el caso de autenticación afirmativa y control de acceso, para recibir desde el aparato de comunicación móvil la información de localización de aparato, y establecer la información de localización de dispositivo en el dispositivo de comunicación de corto alcance usando la información de localización de dispositivo.

En una realización adicional, el procesador está configurado para ejecutar protocolos de autenticación y control de acceso, que rigen la autenticación y el control de acceso entre el dispositivo de comunicación de corto alcance y el aparato de comunicación móvil, para acceder al aparato de comunicación móvil, usando una o más claves de acceso secretas y/o derechos de acceso, para realizar la lectura de datos de un almacén de datos seguro del aparato de comunicación móvil, la escritura de datos en el almacén de datos seguro y/o una interactuación con una aplicación segura del aparato de comunicación móvil.

Además del aparato de comunicación móvil y el dispositivo de comunicación de corto alcance, la presente invención también se refiere a un procedimiento para transmitir un paquete de datos seguro desde un sistema informático a un dispositivo de comunicación de corto alcance. El procedimiento comprende: transmitir el paquete de datos seguro desde el sistema informático a través de una red de radio móvil a un aparato de comunicación móvil; colocar el aparato de comunicación móvil en un intervalo de comunicación del dispositivo de comunicación de corto alcance; determinar una autorización de acceso basándose en verificar la correspondencia de la información de localización de aparato, indicativa de una localización actual del aparato de comunicación móvil, y la información de localización de dispositivo almacenada en el dispositivo de comunicación de corto alcance, determinar la autorización de acceso afirmativa en caso de correspondencia de la información de localización de aparato y la información de localización de dispositivo, y determinar la autorización de acceso negativa a falta de correspondencia de la información de localización de aparato y la información de localización de dispositivo; y, en el caso de una autorización de acceso afirmativa, transferir el paquete de datos seguro al dispositivo de comunicación de corto alcance y determinar y almacenar en el dispositivo de comunicación de corto alcance un contenido del paquete de datos recibido desde el aparato de comunicación móvil.

En una realización, el procedimiento comprende además: recibir en el aparato de comunicación móvil una solicitud de lectura de datos desde el dispositivo de comunicación de corto alcance, incluyendo la solicitud de lectura de datos la información de localización de dispositivo; determinar en el aparato de comunicación móvil la información de localización de aparato; determinar en el aparato de comunicación móvil una primera autorización de acceso basándose en la información de localización de dispositivo recibida desde el dispositivo de comunicación de corto alcance y la información de localización de aparato; y transferir el paquete de datos seguro desde el aparato de comunicación móvil al dispositivo de comunicación de corto alcance, en el caso de una primera autorización de acceso afirmativa, o rechazar la solicitud de lectura, en el caso de una primera autorización de acceso negativa.

En una realización adicional, el procedimiento comprende además: recibir en el dispositivo de comunicación de corto alcance la información de localización de aparato desde el aparato de comunicación móvil; determinar en el

dispositivo de comunicación de corto alcance una segunda autorización de acceso basándose en la información de localización de dispositivo almacenada en el dispositivo de comunicación de corto alcance y la información de localización de aparato recibida desde el aparato de comunicación móvil; y determinar y almacenar en el dispositivo de comunicación de corto alcance el contenido del paquete de datos seguro recibido desde el aparato de comunicación móvil, en el caso de una segunda autorización de acceso afirmativa, o rechazar el paquete de datos, en el caso de una segunda autorización de acceso negativa.

La presente invención también se refiere a un procedimiento para transmitir un paquete de datos seguro desde un sistema informático a un dispositivo de comunicación de corto alcance, en el que el procedimiento comprende: transmitir el paquete de datos seguro desde el sistema informático a través de una red de radio móvil a un aparato de comunicación móvil; colocar el aparato de comunicación móvil en un intervalo de comunicación del dispositivo de comunicación de corto alcance; recibir en el dispositivo de comunicación móvil la información de localización de dispositivo de comunicación de corto alcance, por ejemplo, incluida en una solicitud de lectura de datos desde el dispositivo de comunicación de corto alcance; determinar en el aparato de comunicación móvil la información de localización de aparato indicativa de una localización actual del aparato de comunicación móvil; determinar en el aparato de comunicación móvil una primera autorización de acceso basándose en la información de localización de dispositivo recibida desde el dispositivo de comunicación de corto alcance y la información de localización de aparato, determinar la primera autorización afirmativa de acceso en caso de correspondencia de la información de localización de aparato y la información de localización de dispositivo, y determinar la primera autorización negativa del acceso a falta de correspondencia de la información de localización de aparato y la información de localización de dispositivo; transferir el paquete de datos seguro desde el aparato de comunicación móvil al dispositivo de comunicación de corto alcance, en el caso de una primera autorización afirmativa del acceso, o rechazar la solicitud de lectura, en el caso de una primera autorización negativa del acceso; recibir en el dispositivo de comunicación de corto alcance la información de localización de aparato desde el aparato de comunicación móvil; determinar en el dispositivo de comunicación de corto alcance una segunda autorización del acceso basándose en la información de localización de dispositivo almacenada en el dispositivo de comunicación de corto alcance y la información de localización de aparato recibida desde el aparato de comunicación móvil, determinar la segunda autorización afirmativa del acceso en caso de correspondencia de la información de localización de aparato y la información de localización de dispositivo, y determinar una segunda autorización negativa del acceso a falta de correspondencia de la información de localización de aparato y la información de localización de dispositivo; y determinar y almacenar en el dispositivo de comunicación de corto alcance el contenido del paquete de datos seguro recibido desde el aparato de comunicación móvil, en el caso de una segunda autorización afirmativa del acceso, o rechazar el paquete de datos, en el caso de una segunda autorización negativa del acceso.

Breve descripción de los dibujos

La presente invención se explicará con más detalle, a modo de ejemplo, haciendo referencia a los dibujos en los que:

La figura 1: muestra un diagrama de bloques que ilustra esquemáticamente un aparato de comunicación móvil configurado para transferir un paquete de datos seguro desde un sistema informático a un dispositivo de comunicación de corto alcance.

La figura 2: muestra un diagrama de flujo que ilustra una secuencia a modo de ejemplo de las etapas para transmitir un paquete de datos seguro desde un sistema informático a un dispositivo de comunicación de corto alcance.

La figura 3: muestra un diagrama de flujo que ilustra una secuencia a modo de ejemplo de las etapas para que un aparato de comunicación móvil configure la información de localización en un dispositivo de comunicación de corto alcance.

La figura 4: muestra un diagrama de flujo que ilustra una secuencia a modo de ejemplo de las etapas para el acceso controlado de un dispositivo de comunicación de corto alcance a un aparato de comunicación móvil.

La figura 5: muestra un diagrama de flujo que ilustra una secuencia a modo de ejemplo de las etapas para verificar en un dispositivo de comunicación de corto alcance la autorización de acceso de un aparato de comunicación móvil basándose en la información de localización recibida desde el aparato de comunicación móvil.

Descripción detallada de las realizaciones preferidas

En las figuras 1-5, el número de referencia 1 se refiere a un aparato de comunicación móvil que se implementa como un teléfono de radio móvil (teléfono inteligente, reloj inteligente) o un ordenador móvil tal como un ordenador de tableta, una PDA (asistente de datos personal) o un ordenador personal portátil.

Como se ilustra en la figura 1, el aparato 1 de comunicación móvil comprende un circuito configurado para la comunicación 11 de red de radio móvil, un circuito configurado para la comunicación 13 de corto alcance con un

dispositivo 2 de comunicación de corto alcance, y un circuito configurado para determinar la información 12 de localización de aparato indicativa de la localización actual del aparato 1 de comunicación móvil. Un experto en la materia entenderá que dos o más de estos circuitos pueden implementarse como un circuito común o pueden implementarse como circuitos separados.

El circuito 13 de comunicación de corto alcance está configurado para la comunicación de datos bidireccional de corto alcance con un dispositivo 2 de comunicación de corto alcance. El circuito 13 de comunicación de corto alcance comprende un transceptor de RFID (identificador de radio frecuencia), un transceptor de NFC (comunicación de campo cercano), un transceptor de BLE (Bluetooth de baja energía) y/o un transceptor de WLAN (Wi-Fi). Por ejemplo, el circuito 13 de comunicación de corto alcance está configurado para interactuar con un dispositivo sin contacto de acuerdo con un protocolo de RFID estandarizado tal como se define en estándares tales como ISO 18092, ISO 15693 o ISO 14443, o de acuerdo con una transmisión de datos patentada o un protocolo de RFID. Por ejemplo, el circuito 13 de comunicación de corto alcance está configurado para operar a una frecuencia portadora en el intervalo de 100 KHz a 2,5GHz; en particular, la frecuencia de portadora se establece a la frecuencia de trabajo de un sistema de RFID, por ejemplo, 6,78 MHz, 13,56 MHz o 27,12 MHz (u otro múltiplo de 13,56 MHz).

El circuito 11 de comunicación de red de radio móvil está configurado para la comunicación de datos con un sistema 4 informático remoto a través de una red 3 de radio móvil. El circuito 11 de comunicación de red de radio móvil está configurado para BT (Bluetooth), BLE (Bluetooth de baja energía), WLAN (red de área local inalámbrica), GSM (sistema global para comunicaciones móviles), UMTS (sistema de telecomunicaciones móviles universal) y/u otros servicios de comunicación de datos de radio móviles. En consecuencia, la red 3 de radio móvil comprende una WLAN, una red GSM, una red UMTS, otra red de comunicación de datos de radio móvil y/o Internet.

El circuito 12 de determinación de localización de aparatos está configurado para determinar la localización actual del aparato 1 de comunicación móvil. El circuito 12 de determinación de localización de aparatos comprende un receptor para la navegación basada en satélites, por ejemplo un receptor de GPS (sistema de posicionamiento global). Como alternativa o además, el circuito 12 de determinación de localización de aparatos está configurado para determinar la localización del aparato 1 de comunicación móvil usando datos de red a partir de la red 3 de radio móvil.

Como se ilustra en la figura 1, el aparato 1 de comunicación móvil comprende además un procesador 14, un almacén 15 de datos seguro y una pantalla 16. El procesador 14 está conectado al circuito 11 de comunicación de red de radio móvil, al circuito 12 de determinación de localización de aparatos, al circuito 13 de comunicación de corto alcance, al almacén 15 de datos seguro y a la pantalla 16.

En una realización, el procesador 14 está configurado (programado) para implementar una tarjeta 141 virtual. Específicamente, la tarjeta 141 virtual se implementa como un módulo de software programado que comprende un código de programa informático que se almacena en un medio legible por ordenador no transitorio y configurado para controlar el procesador 14 directamente, por medio de instrucciones específicas de procesador, o por medio de instrucciones interpretables a través de una capa de abstracción de hardware (intermedia), por ejemplo, una plataforma de máquina virtual como la máquina virtual Java (JVM) o una plataforma abierta de tarjeta java (JCOP) de acuerdo con lo especificado por la asociación GlobalPlatform. En una realización alternativa, la tarjeta 141 virtual se implementa por medio de un lenguaje de descripción de hardware VHDL (lenguaje de descripción de hardware de circuito integrado de muy alta velocidad) o VHSIC que se ejecuta en un Simulador de VHDL, que se implementa en el procesador 14.

La tarjeta 141 virtual está configurada para emular las funciones de una tarjeta inteligente implementada por hardware, es decir, una tarjeta de chip o una tarjeta de circuito integrado que comprende un procesador y una memoria (RAM, ROM), por ejemplo una tarjeta de RFID para interactuar con un lector de tarjetas de acuerdo con un protocolo de RFID estandarizado como se define en estándares tales como ISO 18092, ISO 21481, ISO 1 5693 o ISO 14443, o de acuerdo con un protocolo de transmisión de datos o RFID patentado.

En la figura 1, el número de referencia 142 se refiere a diferentes aplicaciones APP_A, APP_B. En una realización, las aplicaciones APP_A, APP_B se implementan como aplicaciones APP_A, APP_B de tarjeta de la tarjeta 141 virtual. Las aplicaciones 142 se implementan como módulos de software programados que comprenden un código de programa informático, que se almacena en un medio legible por ordenador no transitorio y se configura para controlar el procesador 12 directamente, por medio de instrucciones específicas de procesador o por medio de instrucciones interpretables a través de la capa de abstracción de hardware.

El procesador 14 o la tarjeta 141 virtual, respectivamente, están configurados para controlar el acceso y la ejecución de las aplicaciones 142 (tarjeta), por ejemplo, en adhesión a los estándares y las especificaciones respectivas para los módulos de tarjeta inteligente no virtuales (reales). Por ejemplo, el acceso y la ejecución de las aplicaciones 142 (tarjeta) se controlan de acuerdo con las especificaciones definidas por la asociación GlobalPlatform para la gestión de aplicaciones, el estándar de seguridad MULTOS (multi sistema operativo) para tarjetas inteligentes definido por el Consorcio MULTOS, TCOS (Sistema operativo de tarjeta de chip TeleSec) definido por T-Systems International GmbH de Deutsche Telekom AG, el estándar EMV definido por Europay Internacional (ahora MasterCard Europe), MasterCard y VISA, o MTSC (control de sistema maestro-testigo) definido por LEGIC Identsystems AG.

El número de referencia 151 se refiere a los datos de aplicación para las diferentes aplicaciones APP_A, APP_B, que se almacenan en el almacén 15 de datos seguro y es accesible solo a las aplicaciones APP_A, APP_B respectivas, por ejemplo, los datos son datos de tarjeta para diferentes aplicaciones de tarjeta del procesador 14 o de la tarjeta 141 virtual.

Como se ilustra en la figura 1, el dispositivo 2 de comunicación de corto alcance comprende un circuito 23 de comunicación de corto alcance configurado para el intercambio de datos de corto alcance con el aparato 1 de comunicación móvil, por ejemplo, un intervalo de varios centímetros o varios metros. Por consiguiente, el circuito 23 de comunicación de corto alcance comprende un transceptor de RFID, un transceptor de NFC, un transceptor de BLE y/o un transceptor de WLAN (Wi-Fi) compatible con el circuito de comunicación 13 de corto alcance del aparato 1 de comunicación móvil. El dispositivo 2 de comunicación de corto alcance comprende además un almacén 21 de datos seguro y un procesador 22 conectado al circuito 23 de comunicación de corto alcance y al almacén 21 de datos seguro. El almacén 21 de datos seguro es accesible solo para el procesador 22 del dispositivo 2 de comunicación de corto alcance.

En una realización, el dispositivo 2 de comunicación de corto alcance está configurado como un circuito integrado, es decir, un chip. En una realización, el dispositivo 2 de comunicación de corto alcance se implementa como un lector de tarjetas, por ejemplo, un lector de tarjetas para interactuar con un dispositivo de acuerdo con un protocolo de RFID estandarizado como se define en estándares tales como ISO 18092, ISO 21481, ISO 15693 o ISO 14443, o de acuerdo con un protocolo de transmisión de datos o RFID patentado.

El sistema 4 informático comprende uno o más ordenadores con uno o más procesadores configurados para comunicarse con el aparato 1 de comunicación móvil a través de la red 3 de radio móvil. El sistema 4 informático es una entidad de confianza y, en función de la realización y/o el escenario, el sistema 4 informático se implementa como un centro informático, un ordenador fijo, un aparato de comunicación móvil (como se ha descrito anteriormente en el contexto del aparato 1 de comunicación móvil), o un dispositivo de comunicación de corto alcance (como se ha descrito anteriormente en el contexto del dispositivo 2 de comunicación de corto alcance). En un escenario, el sistema 4 informático se usa (temporalmente, de manera extraíble o fija) junto con una tarjeta inteligente que tiene almacenados datos seguros en la misma para su distribución por parte del sistema 4 informático.

El sistema 4 informático está configurado como una autoridad de derechos de acceso informatizada. El sistema 4 informático o la autoridad de derechos de acceso informatizada, respectivamente, están configurados para almacenar y gestionar claves criptográficas y/o derechos de acceso para acceder a tarjetas (inteligentes), incluidas las tarjetas inteligentes implementadas por el procesador 14, por ejemplo, tal como las tarjetas 141 virtuales. Las claves criptográficas y/o los derechos de acceso definen para una tarjeta inteligente identificada, los derechos para leer datos de la tarjeta inteligente, escribir datos en la tarjeta inteligente e interactuar con una aplicación específica de la tarjeta inteligente.

En los siguientes párrafos se describen, haciendo referencia a las figuras 2 a 5, las secuencias a modo de ejemplo de las etapas realizadas por el sistema 4 informático, el aparato 1 de comunicación móvil, y el dispositivo 2 de comunicación de corto alcance.

La figura 2 ilustra una secuencia a modo de ejemplo de las etapas para transmitir un paquete de datos seguro desde el sistema 4 informático al dispositivo 2 de comunicación de corto alcance. Como se describirá a continuación con más detalle, el paquete de datos seguro se transmite desde el sistema 4 informático a través del aparato 1 de comunicación móvil al dispositivo 2 de comunicación de corto alcance. En función de la selección del usuario, el escenario de aplicación y/o los ajustes de configuración, el paquete de datos seguro se transmite en el modo en línea o en el modo fuera de línea. En el modo en línea, el aparato 1 de comunicación móvil tiene conectividad a través de la red 3 de radio móvil al sistema 4 informático y opera como una entidad intermediaria o de retransmisión para el sistema 4 informático para transferir el paquete de datos seguro al dispositivo 2 de comunicación de corto alcance, mientras que el aparato 1 de comunicación móvil está conectado a través de la red 3 de radio móvil al sistema 4 informático, es decir, en línea. En el modo fuera de línea, el aparato 1 de comunicación móvil opera como una entidad de almacenamiento y retransmisión, recibiendo y almacenando el paquete de datos seguro desde el sistema 4 informático mientras haya conectividad a través de la red 3 de radio móvil al sistema 4 informático, y posteriormente, en un punto posterior en el tiempo, transfiriendo el paquete de datos seguro almacenado al dispositivo 2 de comunicación de corto alcance, sin tener el requisito de conectividad a través de la red 3 de radio móvil al sistema 4 informático, es decir, fuera de línea.

Como se ilustra en la figura 2, en las etapas del bloque B, el paquete de datos seguro se transmite desde el sistema 4 informático a través de la red 3 de radio móvil al aparato 1 de comunicación móvil.

En la etapa S0 preparatoria opcional, se transmite una solicitud de configuración desde el aparato 1 de comunicación móvil o su procesador 14, respectivamente, al sistema 4 informático. Por ejemplo, la solicitud de configuración se presenta por una persona de servicio autorizada que planea preparar y configurar uno o más dispositivos 2 de comunicación de corto alcance especificados para interactuar con una o más aplicaciones (tarjeta) específicas implementadas por el procesador 14 o instaladas en tarjetas inteligentes o implementaciones virtuales de tarjetas inteligentes.

En la etapa S1, que responde a la solicitud de configuración del aparato 1 de comunicación móvil, o de otra unidad autorizada o usuario, o por su propia iniciativa, el sistema 4 informático genera un paquete de datos seguro. El paquete de datos está protegido porque al menos algunos de sus contenidos están cifrados. Los contenidos cifrados del paquete de datos seguro solo pueden descifrarse por un destinatario con los medios de descifrado apropiados, que incluye el algoritmo de descifrado y la clave de descifrado secreta. El contenido o la carga útil del paquete de datos seguro comprenden claves de acceso criptográficas, derechos de acceso, datos de configuración, información de tiempo y/o información de localización. Los datos de configuración incluyen valores de parámetros de configuración y/o código de programa ejecutable. En una realización, el paquete de datos seguro tiene una estructura jerárquica y/o anidada, es decir, el contenido de un primer paquete de datos seguro, accesible por medio de una primera clave de descifrado, puede incluir otro segundo paquete de datos seguro, accesible por medio de una segunda clave de descifrado. En una realización, el paquete de datos seguro incluye además (no cifrado) o está vinculado al destino o a la información de destinatario, que incluye la información de direccionamiento, que identifica el destinatario(s) previsto, por ejemplo, las direcciones de red o los identificadores de dispositivos de uno específico o un grupo de dispositivos de comunicación de corto alcance, y la información de localización de destino, que especifica una posición geográfica o zona del destinatario(s) prevista, por ejemplo, unas coordenadas, una dirección postal y/o información descriptiva, que incluye el número de piso, el número o nombre de la habitación, el número o nombre de dispositivo, etc. En una realización, el sistema 4 informático lee el paquete de datos seguro o su contenido de una tarjeta inteligente a través de una interfaz de RFID o NFC o a través de una interfaz basada en contacto.

En la etapa S2, el paquete de datos seguro se transmite desde el sistema 4 informático a través de la red 3 de radio móvil al aparato 1 de comunicación móvil.

En la etapa S3, se recibe el paquete de datos seguro por el aparato 1 de comunicación móvil o su procesador 14, respectivamente.

En la etapa S4, el aparato 1 de comunicación móvil entra en el alcance de comunicación del dispositivo 2 de comunicación de corto alcance. El dispositivo 2 de comunicación de corto alcance detecta la presencia del aparato 1 de comunicación móvil o su procesador 14 o la tarjeta 141 virtual, respectivamente, y la autenticación y el control de acceso se ejecutan entre el dispositivo 2 de comunicación de corto alcance y el procesador 14 o la tarjeta 141 virtual del aparato 1 de comunicación móvil a través de los circuitos 13, 23 de comunicación de corto alcance. Un experto en la materia entenderá que pueden usarse diversos algoritmos criptográficos estandarizados o patentados para realizar los protocolos de autenticación y control de acceso entre el dispositivo 2 de comunicación de corto alcance y el aparato 1 de comunicación móvil o su procesador 14 o la tarjeta 141 virtual. El dispositivo 2 de comunicación de corto alcance o su procesador 22, respectivamente, y el aparato 1 de comunicación móvil o su procesador 14 o la tarjeta 141 virtual, respectivamente, están configurados para realizar los protocolos de autenticación y control de acceso, por ejemplo, en cumplimiento de los estándares y especificaciones respectivas para módulos de tarjetas inteligentes no virtuales (reales), tales como ISO 7816 y/o ISO 9798, como se describe por la asociación GlobalPlatform.

En la etapa S5, tras la autenticación y la autorización con éxito, el dispositivo 2 de comunicación de corto alcance o su procesador 22, respectivamente, genera una solicitud de lectura de datos. La solicitud de lectura de datos incluye la información 211 de localización de dispositivo que está almacenada en el dispositivo 2 de comunicación de corto alcance, que indica la localización (configurada/programada) del dispositivo 2 de comunicación de corto alcance específico. La información 211 de localización de dispositivo se almacena en el almacén 21 de datos seguro del dispositivo 2 de comunicación de corto alcance. En función del escenario o la realización, la información 211 de localización de dispositivo se almacena en el almacén 21 de datos seguro antes de que se instale el dispositivo 2 de comunicación de corto alcance, por ejemplo, durante el procedimiento de fabricación o configuración, o a través de la configuración en el sitio autenticada cuando ya está instalado, tal como se explicará más adelante con más detalle. Normalmente, el dispositivo 2 de comunicación de corto alcance se instala como un dispositivo 2 de comunicación de corto alcance estacionario y la información 211 de localización de dispositivo indica la localización estacionaria configurada del dispositivo 2 de comunicación de corto alcance. Sin embargo, en función de la aplicación, por ejemplo, en la conexión con un automóvil, el dispositivo 2 de comunicación de corto alcance puede ser móvil y la información 211 de localización de dispositivo indica la localización estacionaria configurada del dispositivo 2 de comunicación de corto alcance donde se le permite recibir paquetes de datos seguros desde un aparato de comunicación móvil autorizado 2, por ejemplo, en una estación o zona de servicio.

En la etapa S6, la solicitud de lectura de datos se transmite desde el dispositivo 2 de comunicación de corto alcance al aparato 1 de comunicación móvil a través de los circuitos 13, 23 de comunicación de corto alcance.

En la etapa S7, al usar el circuito 12 de determinación de localización de aparatos, el procesador 14 del aparato 1 de comunicación móvil determina su localización actual (en el caso de un punto muerto, se usa la última localización disponible determinada). En una realización, el procesador 14 del aparato 1 de comunicación móvil comprueba si ha almacenado un paquete de datos seguro con una localización de destino que coincida con la localización actual del aparato 1 de comunicación móvil. Si no hay un paquete de datos seguro con la localización de destino coincidente, el procesador 14 genera un mensaje de alerta, que informa al usuario del aparato 1 de comunicación móvil que no hay un paquete de datos seguro disponible para la localización actual; de lo contrario, el procesador 14 continúa en

la etapa S8.

En la etapa S8, el procesador 14 del aparato 1 de comunicación móvil verifica además la autorización de acceso del dispositivo 2 de comunicación de corto alcance mediante la comprobación de si la información de localización de dispositivo recibida desde el dispositivo 2 de comunicación de corto alcance corresponde a la localización de aparato determinada para el aparato 1 de comunicación móvil. Específicamente, el procesador 14 comprueba si la localización de dispositivo está dentro de una zona o área definida alrededor de la localización de aparato, por ejemplo, una zona o área con un radio de cinco, diez, veinte, cincuenta o cien metros alrededor de la localización de aparato. En una realización, la información de altura o altitud (localización) se incluye en la verificación.

En una realización, los solicitud de lectura de datos incluye además la información 212 de tiempo de dispositivo tal como se almacena en el dispositivo 2 de comunicación de corto alcance, y el procesador 14 del aparato 1 de comunicación móvil verifica además la autorización de acceso comprobando si la información de tiempo de dispositivo recibida desde el dispositivo 2 de comunicación de corto alcance corresponde a la información de tiempo de aparato almacenada (u obtenida a partir de un reloj) en el aparato 1 de comunicación móvil.

En el caso en el que la localización de dispositivo está fuera de la zona o el área de referencia alrededor de la localización de aparato (o - si procede - la información de tiempo de dispositivo se desvía de la información de tiempo de aparato en más de un umbral definido), en la etapa S12, el procesador 14 determina la autorización de acceso negativa y rechaza la solicitud de lectura. En una realización, el procesador 14 genera y transmite en la etapa S12* un mensaje de retroalimentación negativo al sistema 4 informático, informando al sistema 4 informático sobre el rechazo de una solicitud de lectura debido a la falta de correspondencia de localización (y/o de tiempo) del dispositivo 2 de comunicación de corto alcance respectivo.

De lo contrario, en el caso en el que la localización de dispositivo está fuera de la zona o el área de referencia alrededor de la localización de aparato (y - si procede - la información de tiempo de dispositivo difiere de la información de tiempo de aparato en no más que el umbral definido), en la etapa S9, el procesador 14 determina si el almacén 15 de datos seguro incluye uno o más paquetes de datos seguros que tienen información de localización de destino que coincide con la localización de dispositivo. Si hay un paquete de datos seguro con una localización de destino coincidente, se incluirá en la respuesta de lectura para el dispositivo 2 de comunicación de corto alcance. Si hay más de un paquete de datos seguro con una localización de destino coincidente, el procesador 14 muestra en la pantalla 16 una lista de los paquetes de datos seguros con la localización de destino coincidente, que incluye la información de localización de destino adicional, tal como la dirección postal, el número de piso, el número o nombre de la habitación, el número o nombre del dispositivo, el nombre del proyecto, la ID del proyecto, el nombre de la instalación, etc. A continuación se pide al usuario que seleccione de la lista el paquete de datos seguro que está destinado al dispositivo 2 de comunicación de corto alcance específico donde el usuario se localiza actualmente con el aparato 1 de comunicación móvil. Si no hay un paquete de datos seguro con la información de localización de destino correspondiente, el procesador 14 determina una autorización de acceso negativa y rechaza la solicitud de lectura como se ha descrito anteriormente en relación con las etapas S12 y S12*.

Como se indica esquemáticamente en la figura 2, en el modo fuera de línea las etapas del bloque B se ejecutan antes para el aparato 1 de comunicación móvil que entra en el alcance de comunicación del dispositivo 2 de comunicación de corto alcance y que ejecuta los protocolos de autenticación y control de acceso. En el modo en línea, por otro lado, las etapas S0, S1, S2, S3 del bloque B pueden ejecutarse en un momento posterior, por ejemplo, después de que se haya verificado la autorización en la etapa S8, tal como lo indica el número de referencia B*. En este caso, el procesador 14 del aparato 1 de comunicación móvil comprueba, después de la ejecución de las etapas del bloque B*, si ha recibido un paquete de datos seguro con una localización de destino coincidente con la localización actual del aparato 1 de comunicación móvil. Si no hay un paquete de datos seguro con una localización de destino coincidente, el procesador 14 genera un mensaje de alerta, que informa al usuario del aparato 1 de comunicación móvil que no se ha recibido ningún paquete de datos seguro para la localización actual; de lo contrario, el procesador 14 continúa en la etapa S9.

Además, en la etapa S9, el procesador 14 genera y transmite al dispositivo 2 de comunicación de corto alcance una respuesta de lectura de datos, que incluye el paquete de datos seguro determinado y/o seleccionado, a través de los circuitos 13, 23 de comunicación de corto alcance. En una realización, en la etapa S9*, el procesador 14 genera y transmite un mensaje de retroalimentación positiva al sistema 4 informático.

En una realización, el paquete de datos seguro se elimina en el aparato 1 de comunicación móvil una vez que el aparato 1 de comunicación móvil ya no está en proximidad al dispositivo 2 de comunicación de corto alcance, es decir, una vez que la localización de dispositivo está fuera de la zona o área de referencia alrededor de la localización de aparato. Para ese fin, el procesador 14 está configurado además para comprobar la correspondencia de la localización de dispositivo determinada anteriormente y la localización de aparato, por ejemplo, en un período de tiempo establecido después de la transmisión del paquete de datos seguro en la etapa S9, y eliminar el paquete de datos seguro en el caso de la falta de correspondencia. Como alternativa, la eliminación del paquete de datos seguro se inicia de manera remota por el sistema 4 informático.

En una realización, el procesador 14 incluye en la respuesta de lectura de datos la localización actual del aparato 1 de comunicación móvil determinada en la etapa S7, y en la etapa opcional S90, el procesador 22 del dispositivo 2 de comunicación de corto alcance verifica la autorización de acceso del aparato 1 de comunicación móvil basándose en la localización actual recibida desde el aparato 1 de comunicación móvil. Específicamente, tal como se ilustra en la figura 5, en la etapa S91, el procesador 22 obtiene la información de localización de aparato incluida en la respuesta de lectura de datos recibida desde el aparato 1 de comunicación móvil. En la etapa S92, el procesador 22 verifica la correspondencia de localización comprobando si la información de localización de dispositivo almacenada en el dispositivo 2 de comunicación de corto alcance corresponde a la localización de aparato recibida desde el aparato 1 de comunicación móvil. Por lo tanto, el procesador 22 comprueba si la localización de aparato está dentro de una zona o área definida alrededor de la localización de dispositivo, por ejemplo, una zona o área con un radio de cinco, diez, veinte, cincuenta o cien metros alrededor de la localización de dispositivo. En una realización, la información de altura o altitud (localización) se incluye en la verificación.

En una realización, la respuesta de lectura de datos incluye, además, el tiempo de aparato incluido por el procesador 14 del aparato 1 de comunicación móvil, y el procesador 22 del dispositivo 2 de comunicación de corto alcance verifica además la autorización de acceso del aparato 1 de comunicación móvil verificando si la información de tiempo de aparato recibida desde el aparato 1 de comunicación móvil corresponde a la información 212 de tiempo de dispositivo tal como está almacenada en el dispositivo 2 de comunicación de corto alcance, por ejemplo, de acuerdo con lo programado o determinado por un reloj interno del dispositivo 2 de comunicación de corto alcance.

En el caso en el que la localización de aparato está fuera de la zona o área de referencia alrededor de la localización de dispositivo (o - si procede - la información de tiempo de aparato se desvía de la información de tiempo de dispositivo en más de un umbral definido), en la etapa S93, el procesador 22 determina la autorización de acceso negativa y rechaza el paquete de datos del aparato 1 de comunicación móvil. En una realización, el procesador 22 genera y transmite en la etapa S94 un mensaje de retroalimentación negativo al aparato 1 de comunicación móvil, informando al aparato 1 de comunicación móvil sobre el rechazo de un paquete de datos debido a la falta de correspondencia de localización (y/o de tiempo) del aparato 1 de comunicación móvil respectivo.

De lo contrario, en el caso en el que la localización de aparato esté dentro de la zona o área de referencia alrededor de la localización de dispositivo (y - si procede - la información de tiempo de aparato difiere de la información de tiempo de dispositivo en no más que el umbral definido), el procesador 22 del dispositivo 2 de comunicación de corto alcance acepta el paquete de datos del aparato 1 de comunicación móvil y continúa en la etapa S10.

En la etapa S10, el procesador 22 extrae el contenido o carga útil cifrado del paquete de datos seguro incluido en la respuesta de lectura de datos, usando una clave criptográfica secreta correspondiente para descifrar el nivel de jerarquía o de anidamiento respectivo del paquete de datos seguro del sistema 4 informático.

En la etapa S11, el procesador 22 almacena los contenidos o carga útil extraídos y descifrados del paquete de datos seguro en el almacén de datos protegido 21 del dispositivo 2 de comunicación de corto alcance. Específicamente, el procesador 22 almacena en el almacén 21 de datos seguro las claves de acceso y/o los derechos 213 de acceso, los datos 214 de configuración, la información 211 de localización y/o la información 212 de tiempo extraídos y descifrados del paquete de datos seguro.

La figura 3 ilustra una secuencia de etapas a modo de ejemplo para el aparato 1 de comunicación móvil que configura la información de localización de dispositivo en el dispositivo 2 de comunicación de corto alcance.

En la etapa S13, el aparato 1 de comunicación móvil está dentro del alcance de comunicación del dispositivo 2 de comunicación de corto alcance, y los protocolos de autenticación y control de acceso se ejecutan entre el dispositivo 2 de comunicación de corto alcance y el aparato 1 de comunicación móvil o su procesador 14 o la tarjeta 141 virtual, respectivamente, tal como se ha descrito anteriormente en el contexto de la etapa S4. Como parte de la autenticación y del control de acceso de la etapa S13, el aparato 1 de comunicación móvil o su procesador 14 o la tarjeta 141 virtual, respectivamente, se autentica como un “dispositivo localizador” autorizado para establecer la localización 211 de dispositivo del dispositivo 2 de comunicación de corto alcance.

En la etapa S14, tras la autenticación y la autorización con éxito, el dispositivo 2 de comunicación de corto alcance o su procesador 22, respectivamente, genera una consulta de localización, por ejemplo, como parte de un procedimiento de preparación o configuración.

En la etapa S15, la consulta de localización se transmite desde el dispositivo 2 de comunicación de corto alcance al aparato 1 de comunicación móvil a través de los circuitos 13, 23 de comunicación de corto alcance.

En la etapa S16, al usar el circuito 12 de determinación de localización de aparatos, el procesador 14 del aparato 1 de comunicación móvil determina su localización actual (en el caso de un punto muerto, se usa la última localización disponible determinada).

En la etapa S17, el procesador 14 (o la tarjeta 141 virtual, respectivamente) genera y transmite al dispositivo 2 de comunicación de corto alcance una respuesta de consulta de localización a través de los circuitos 13, 23 de comunicación de corto alcance. La respuesta de consulta de localización incluye la localización de aparato actual

determinada, preferentemente de manera segura (cifrada).

En la etapa S18, el procesador 22 recibe la respuesta de consulta de localización y almacena la localización de aparato recibida como la localización 211 de dispositivo del dispositivo 2 de comunicación de corto alcance en el almacén 21 de datos seguro.

Posteriormente, la localización 211 de dispositivo se usa para verificar la autorización de acceso de terminales basándose en la correspondencia de la localización de terminal y de aparato, tal como se ha descrito anteriormente en el contexto de la etapa S8.

La figura 4 ilustra una secuencia de etapas a modo de ejemplo para el acceso controlado del dispositivo 2 de comunicación de corto alcance al aparato 1 de comunicación móvil.

Como se ha descrito anteriormente, en la etapa S4, el aparato 1 de comunicación móvil está dentro del alcance de comunicación del dispositivo 2 de comunicación de corto alcance, y los protocolos de autenticación y control de acceso se ejecutan entre el dispositivo 2 de comunicación de corto alcance y el aparato 1 de comunicación móvil o su procesador 14 o la tarjeta 141 virtual, respectivamente.

En la etapa S20, tras la autenticación y la autorización con éxito, el dispositivo 2 de comunicación de corto alcance o su procesador 22, respectivamente, determina la clave 213 de acceso criptográfica para acceder al aparato 1 de comunicación móvil o a sus aplicaciones 142 o a la tarjeta 141 virtual, respectivamente. El dispositivo 2 de comunicación de corto alcance ha almacenado una o más claves 213 de acceso criptográficas, que son específicas de la aplicación y/o del proveedor. El fin de la consulta de claves es identificar la clave 213 de acceso criptográfica que el dispositivo 2 de comunicación de corto alcance debe usar en una solicitud de acceso posterior, por ejemplo, solicitudes de lectura/escritura, interacciones de aplicación, transacciones, sesiones, etc., con el aparato 1 de comunicación móvil, sus aplicaciones 142 o su tarjeta 141 virtual, respectivamente.

Específicamente, en la etapa S21, el dispositivo 2 de comunicación de corto alcance o su procesador 22, respectivamente, genera una consulta de clave.

En la etapa S22, la consulta de clave se transmite desde el dispositivo 2 de comunicación de corto alcance al aparato 1 de comunicación móvil a través de los circuitos 13, 23 de comunicación de corto alcance.

En la etapa S23, el aparato 1 de comunicación móvil, es decir, el procesador 14 o la tarjeta 141 virtual, respectivamente, determina la clave k_i de acceso criptográfica que debe usarse por el dispositivo 2 de comunicación de corto alcance en la transacción o sesión actual con el aparato 1 de comunicación móvil, sus aplicaciones 142 o su tarjeta 141 virtual, respectivamente. El procesador 14 determina un identificador K_{IDi} de clave para la clave k_i de acceso criptográfica identificada. El identificador K_{IDi} de clave se genera a partir de la clave k_i de acceso criptográfica identificada que usa una función h de una vía criptográfica, es decir, una función que es inviable o extremadamente difícil de invertir, por ejemplo una función hash criptográfica, $K_{IDi} = h(k_i)$. En función de la realización, el identificador K_{IDi} de clave se genera anteriormente (por ejemplo, en el sistema 4 informático) y se almacena en el aparato 1 de comunicación móvil, por ejemplo, en una tabla de identificador de clave, o el identificador K_{IDi} de clave se genera "sobre la marcha" en el aparato 1 de comunicación móvil, siempre que la clave k_i de acceso criptográfica esté realmente disponible y almacenada de manera segura en el aparato 1 de comunicación móvil.

En la etapa S24, el procesador 14 (o la tarjeta 141 virtual, respectivamente) genera y transmite al dispositivo 2 de comunicación de corto alcance una respuesta de consulta de clave a través de los circuitos 13, 23 de comunicación de corto alcance. La respuesta de consulta de clave incluye el identificador K_{IDi} de clave generado.

En la etapa S25, el procesador 22 recibe la respuesta de consulta de clave y compara el identificador K_{IDi} de clave recibido con los identificadores K_{IDn} de clave de las k_n claves 213 de acceso criptográficas almacenadas en el almacén 21 de datos seguro del dispositivo 2 de comunicación de corto alcance. Los identificadores K_{IDn} de clave se obtienen a partir de las k_n claves 213 de acceso criptográficas que usan la misma función h de una vía criptográfica, $K_{IDn} = h(k_n)$. Preferentemente, los identificadores K_{IDn} de clave de las claves 213 de acceso criptográficas están "precalculados" y se almacenan en el almacén 21 de datos seguro vinculado a las k_n claves 213 de acceso criptográficas respectivas.

En la etapa S26, tras la identificación exitosa de $K_{IDn} = K_{IDi}$ de la clave k_i de acceso criptográfica, el dispositivo 2 de comunicación de corto alcance o su procesador 22, respectivamente, genera una solicitud de acceso, usando la clave k_i de acceso identificada.

En la etapa S27, la solicitud de acceso se transmite desde el dispositivo 2 de comunicación de corto alcance al aparato 1 de comunicación móvil a través de los circuitos 13, 23 de comunicación de corto alcance.

En la etapa S28, el aparato 1 de comunicación móvil, es decir, el procesador 14 o la tarjeta 141 virtual, verifica la legitimidad o la autorización de la solicitud de acceso basándose en la clave k_i de acceso criptográfica especificada para el dispositivo 2 de comunicación de corto alcance en la respuesta de consulta de clave de la etapa S24 con el identificador K_{IDi} de clave. En una realización, para mayor seguridad, el aparato 1 de comunicación móvil, es decir, el

procesador 14 o la tarjeta 141 virtual, verifica además la legitimidad o la autorización de la solicitud de acceso realizando la verificación de autorización basada en la localización y/o el tiempo descrita anteriormente en el contexto de la etapa S8.

En la etapa S29, tras la verificación de autorización exitosa y positiva, el procesador 14 (o la tarjeta 141 virtual, respectivamente) ejecuta la solicitud de acceso y genera una respuesta de solicitud de acceso. En función del escenario, la respuesta de solicitud de acceso incluye una respuesta de datos para una solicitud de lectura de datos ejecutada, una confirmación de escritura para una solicitud de escritura de datos ejecutada, una respuesta de transacción para una solicitud de transacción ejecutada, una respuesta de aplicación para una solicitud de interacción de aplicación ejecutada, una respuesta de sesión para una solicitud de sesión ejecutada, etc.

En la etapa S30, el procesador 14 (o la tarjeta 141 virtual, respectivamente) transmite la respuesta de solicitud de acceso al dispositivo 2 de comunicación de corto alcance a través de los circuitos 13, 23 de comunicación de corto alcance. En una realización, el procesador 22 verifica la legitimidad o la autorización del aparato 1 de comunicación móvil o su procesador 14 o la tarjeta 141 virtual, respectivamente, realizando la verificación de autorización, basándose en la localización y/o en el tiempo, descrita anteriormente en el contexto de la etapa S90. Por lo tanto, la correspondencia del tiempo y/o la localización del aparato con la hora y/o la localización del dispositivo no solo se aplica para transferir paquetes de datos seguros con fines de configuración o distribución de claves, sino también para cualquier otra interacción operativa e intercambio de datos entre el aparato 1 de comunicación móvil y el dispositivo 2 de comunicación de corto alcance.

Debería observarse que, en la descripción, el código de programa informático se ha asociado con unos módulos funcionales específicos y la secuencia de las etapas se ha presentado en un orden específico, un experto en la materia entenderá, sin embargo, que el código de programa informático puede estructurarse de manera diferente y el orden de al menos algunas de las etapas podría alterarse, sin desviarse del ámbito de la invención.

REIVINDICACIONES

1. Un aparato (1) de comunicación móvil, que comprende:

un primer circuito (11) configurado para la comunicación de datos a través de una red (3) de radio móvil;
un segundo circuito (13) configurado para la comunicación de corto alcance con un dispositivo (2) de comunicación de corto alcance;
un tercer circuito (12) configurado para determinar la información de localización de aparato, indicativa de una localización actual del aparato (1) de comunicación móvil; y
un procesador (14) conectado a los circuitos (11, 12, 13) primero, segundo y tercero y configurado para recibir (S2) a través de la red (3) de radio móvil un paquete de datos seguro desde un sistema (4) informático, para recibir (S6) información de localización de dispositivo desde el dispositivo (2) de comunicación de corto alcance, para determinar (S8) la autorización de acceso basándose en verificar la correspondencia de la información de localización de dispositivo y la información de localización de aparato, determinar la autorización de acceso afirmativa en caso de correspondencia de la información de localización de dispositivo y la información de localización de aparato, y determinar la autorización de acceso negativa a falta de correspondencia de la información de localización de dispositivo y la información de localización de aparato, y para transferir (S9) el paquete de datos seguro al dispositivo (2) de comunicación de corto alcance, en el caso de una autorización de acceso afirmativa, y para no transferir el paquete de datos seguro al dispositivo (2) de comunicación de corto alcance, en el caso de una autorización de acceso negativa.

2. El aparato (1) de comunicación móvil de la reivindicación 1, en el que la información de localización de dispositivo se recibe (S6) desde el dispositivo (2) de comunicación de corto alcance incluida en una solicitud de lectura de datos; y el procesador (14) está configurado para rechazar (S12) la solicitud de lectura, en el caso de una autorización de acceso negativa.

3. El aparato (1) de comunicación móvil de una de las reivindicaciones 1 o 2, en el que el paquete de datos seguro se recibe con la información de localización de destino, y el procesador (14) está configurado para determinar (S8) la autorización de acceso basándose además en verificar la correspondencia de la información de localización de dispositivo y la información de localización de destino, determinar la autorización de acceso afirmativa en caso de correspondencia de la información de localización de dispositivo y la información de localización de destino, y determinar la autorización de acceso negativa a falta de correspondencia de la información de localización de dispositivo y la información de localización de destino.

4. El aparato (1) de comunicación móvil de una de las reivindicaciones 1 a 3, en el que el procesador (14) está configurado para recibir (S2) además la información de tiempo de dispositivo desde el dispositivo (2) de comunicación de corto alcance, para determinar (S8) la autorización de acceso basándose además en verificar la correspondencia de la información de tiempo de dispositivo y la información de tiempo almacenada en el aparato (1) de comunicación móvil, determinar la autorización de acceso afirmativa en caso de correspondencia de la información de tiempo de dispositivo y la información de tiempo almacenada en el aparato (1) de comunicación móvil, y determinar la autorización de acceso negativa a falta de correspondencia de la información de tiempo de dispositivo y la información de tiempo almacenada en el aparato (1) de comunicación móvil.

5. El aparato (1) de comunicación móvil de una de las reivindicaciones 1 a 4, en el que el paquete de datos seguro incluye al menos uno de: una o más claves de acceso secretas, uno o más derechos de acceso, datos de configuración para el dispositivo (2) de comunicación de corto alcance, e información de tiempo; y el procesador (14) está configurado para transferir el paquete de datos seguro que incluye la una o más claves de acceso secretas, el uno o más derechos de acceso, los datos de configuración y/o la información de tiempo, respectivamente, en el caso de una autorización de acceso afirmativa, y para no transferir el paquete de datos seguro al dispositivo (2) de comunicación de corto alcance, en el caso de una autorización de acceso negativa.

6. El aparato (1) de comunicación móvil de una de las reivindicaciones 1 a 5, en el que el procesador (14) está configurado para ejecutar (S4) protocolos de autenticación y control de acceso, que rigen la autenticación y el control de acceso entre el aparato (1) de comunicación móvil y el dispositivo (2) de comunicación de corto alcance, para acceder al dispositivo (2) de comunicación de corto alcance para establecer la información de localización de dispositivo en el dispositivo (2) de comunicación de corto alcance, y, en el caso de autenticación afirmativa y control de acceso, para usar la información de localización de aparato para establecer la información de localización de dispositivo en el dispositivo (2) de comunicación de corto alcance.

7. El aparato (1) de comunicación móvil de una de las reivindicaciones 1 a 6, en el que el procesador (14) está configurado para ejecutar (S4) protocolos de autenticación y control de acceso, que rigen la autenticación y el control de acceso entre el aparato (1) de comunicación móvil y el dispositivo (2) de comunicación de corto alcance, para acceder al aparato (1) de comunicación móvil, usando una o más claves de acceso secretas y/o derechos de acceso, para realizar al menos una de: una lectura de datos de un almacén de datos seguro del aparato (1) de comunicación móvil, una escritura de datos en el almacén de datos seguro e interactuar con una aplicación segura del aparato (1) de comunicación móvil.

8. Un dispositivo (2) de comunicación de corto alcance, que comprende:

un circuito (23) configurado para la comunicación de corto alcance con un aparato (1) de comunicación móvil; y
un procesador (22) conectado al circuito (23), y configurado para recibir del aparato (1) de comunicación móvil un paquete de datos, incluyendo el paquete de datos información de localización de aparato, indicativa de una localización actual del aparato (1) de comunicación móvil, para determinar (S8) la autorización de acceso basándose en verificar la correspondencia de la información de localización de dispositivo almacenada en el dispositivo (2) de comunicación de corto alcance y la información de localización de aparato recibida desde el aparato (1) de comunicación móvil, determinar la autorización de acceso afirmativa en caso de correspondencia de la información de localización de dispositivo y la información de localización de aparato, y determinar la autorización de acceso negativa a falta de correspondencia entre la información de localización de dispositivo y la información de localización de aparato, y para determinar y almacenar (S11) en el dispositivo (2) de comunicación de corto alcance un contenido del paquete de datos recibido desde el aparato (1) de comunicación móvil, en el caso de una autorización de acceso afirmativa, y rechazar (S12) el paquete de datos, en el caso de una autorización de acceso negativa.

9. El dispositivo (2) de comunicación de corto alcance de la reivindicación 8, en el que el procesador (22) está configurado para recibir desde el aparato (1) de comunicación móvil la información de tiempo, para determinar (S8) la autorización de acceso basándose además en verificar la correspondencia de la información de tiempo de dispositivo almacenada en el dispositivo (2) de comunicación de corto alcance y la información de tiempo recibida desde el aparato (1) de comunicación móvil, determinar la autorización de acceso afirmativa en caso de correspondencia de la información de tiempo de dispositivo y la información de tiempo recibida desde el aparato (1) de comunicación móvil, y determinar la autorización de acceso negativa a falta de correspondencia de la información de tiempo de dispositivo y la información de tiempo recibida desde el aparato (1) de comunicación móvil.

10. El dispositivo (2) de comunicación de corto alcance de una de las reivindicaciones 8 o 9, en el que el procesador (22) está configurado para extraer del paquete de datos al menos uno de: una o más claves de acceso secretas, uno o más derechos de acceso, datos de configuración para el dispositivo (2) de comunicación de corto alcance, e información de tiempo; y para almacenar en un almacén de datos seguro del dispositivo (2) de comunicación de corto alcance la una o más claves de acceso secretas, el uno o más derechos de acceso, los datos de configuración y/o la información de tiempo, respectivamente.

11. El dispositivo (2) de comunicación de corto alcance de una de las reivindicaciones 8 a 10, en el que el procesador (22) está configurado para ejecutar (S4) protocolos de autenticación y control de acceso, que rigen la autenticación y el control de acceso entre el dispositivo (2) de comunicación de corto alcance y el aparato (1) de comunicación móvil, para acceder al dispositivo (2) de comunicación de corto alcance para establecer la información de localización de dispositivo en el dispositivo (2) de comunicación de corto alcance, y, en el caso de autenticación afirmativa y control de acceso, para recibir desde el aparato (1) de comunicación móvil la información de localización de aparato, y para establecer la información de localización de dispositivo en el dispositivo (2) de comunicación de corto alcance usando la información de localización de aparato.

12. El dispositivo (2) de comunicación de corto alcance de una de las reivindicaciones 8 a 11, en el que el procesador (22) está configurado para ejecutar (S4) protocolos de autenticación y control de acceso, que rigen la autenticación y el control de acceso entre el dispositivo (2) de comunicación de corto alcance y el aparato (1) de comunicación móvil, para acceder al aparato (1) de comunicación móvil, usando una o más claves de acceso secretas y/o derechos de acceso, para realizar al menos una de: una lectura de datos de un almacén de datos seguro del aparato (1) de comunicación móvil, una escritura de datos en el almacén de datos seguro e interactuar con una aplicación segura del aparato (1) de comunicación móvil.

13. Un procedimiento de transmisión de un paquete de datos seguro desde un sistema (4) informático a un dispositivo (2) de comunicación de corto alcance, comprendiendo el procedimiento:

transmitir (S2) el paquete de datos seguro desde el sistema (4) informático a través de una red (3) de radio móvil a un aparato (1) de comunicación móvil;
colocar el aparato (1) de comunicación móvil en un intervalo de comunicación del dispositivo (2) de comunicación de corto alcance;
determinar (S8) una autorización de acceso basándose en verificar la correspondencia de la información de localización de aparato, indicativa de una localización actual del aparato (1) de comunicación móvil, y la información de localización de dispositivo almacenada en el dispositivo (2) de comunicación de corto alcance, determinar la autorización de acceso afirmativa en caso de correspondencia de la información de localización de aparato y la información de localización de dispositivo, y determinar la autorización de acceso negativa a falta de correspondencia de la información de localización de aparato y la información de localización de dispositivo, y
en el caso de una autorización de acceso afirmativa, transferir (S9) el paquete de datos seguro al dispositivo (2) de comunicación de corto alcance y determinar y almacenar (S11) en el dispositivo (2) de comunicación de corto alcance un contenido del paquete de datos seguro recibido desde el aparato (1) de comunicación móvil.

14. El procedimiento de la reivindicación 13, que comprende además: recibir (S6) en el aparato (1) de comunicación móvil una solicitud de lectura de datos desde el dispositivo (2) de comunicación de corto alcance, incluyendo la solicitud de lectura de datos la información de localización de dispositivo; determinar (S7) en el aparato (1) de comunicación móvil la información de localización de aparato; determinar (S8) en el aparato (1) de comunicación móvil una primera autorización del acceso basándose en la información de localización de dispositivo recibida desde el dispositivo (2) de comunicación de corto alcance y la información de localización de aparato; y transferir (S9) el paquete de datos seguro desde el aparato (1) de comunicación móvil al dispositivo (2) de comunicación de corto alcance, en el caso de una primera autorización afirmativa del acceso, o rechazar la solicitud de lectura, en el caso de una primera autorización negativa del acceso.

15. El procedimiento de una de las reivindicaciones 13 o 14, que comprende además: recibir (S6) en el dispositivo (2) de comunicación de corto alcance la información de localización de aparato desde el aparato (1) de comunicación móvil; determinar (S8) en el dispositivo (2) de comunicación de corto alcance una segunda autorización del acceso basándose en la información de localización de dispositivo almacenada en el dispositivo (2) de comunicación de corto alcance y la información de localización de aparato recibida desde el aparato (1) de comunicación móvil; y determinar y almacenar (S11) en el dispositivo (2) de comunicación de corto alcance el contenido del paquete de datos seguro recibido desde el aparato (1) de comunicación móvil, en el caso de una segunda autorización afirmativa del acceso, o rechazar (S12) el paquete de datos seguro, en el caso de una segunda autorización negativa del acceso.

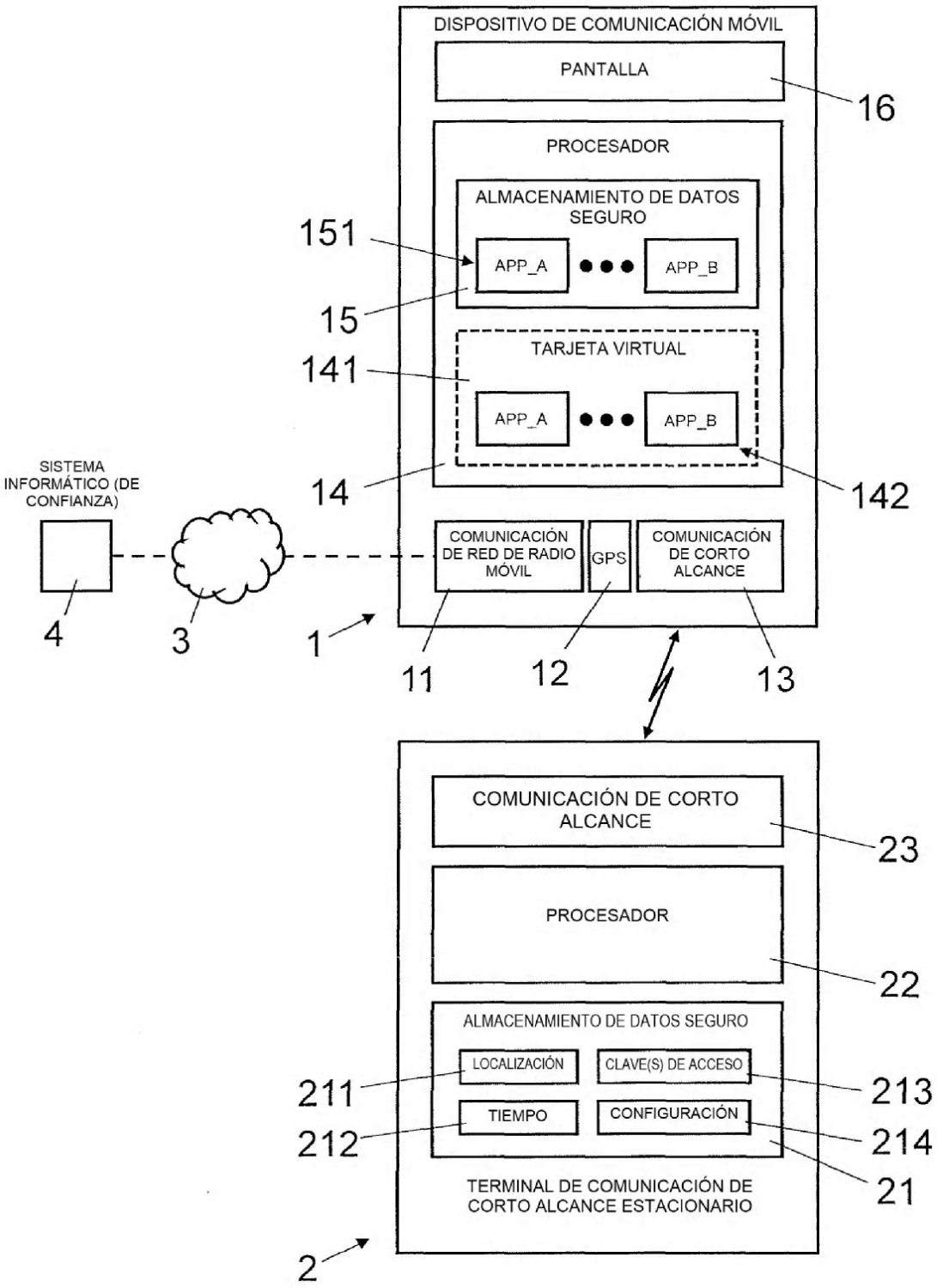
DISPOSITIVO DE COMUNICACIÓN MÓVIL
PANTALLA
16
PROCESADOR
ALMACENAMIENTO DE DATOS SEGURO
151
APP_A
APP_B
15
TARJETA VIRTUAL
141
APP_A
APP_B
142
14
SISTEMA INFORMÁTICO (DE CONFIANZA)
COMUNICACIÓN DE RED DE RADIO MÓVIL
GPS
COMUNICACIÓN DE CORTO ALCANCE
4
3
1
11
12
13
COMUNICACIÓN DE CORTO ALCANCE
23
PROCESADOR
22
ALMACENAMIENTO DE DATOS SEGURO
LOCALIZACIÓN
CLAVE(S) DE ACCESO
211
213
TIEMPO
CONFIGURACIÓN
212
214
21
TERMINAL DE COMUNICACIÓN DE CORTO ALCANCE ESTACIONARIO
2

Fig. 1

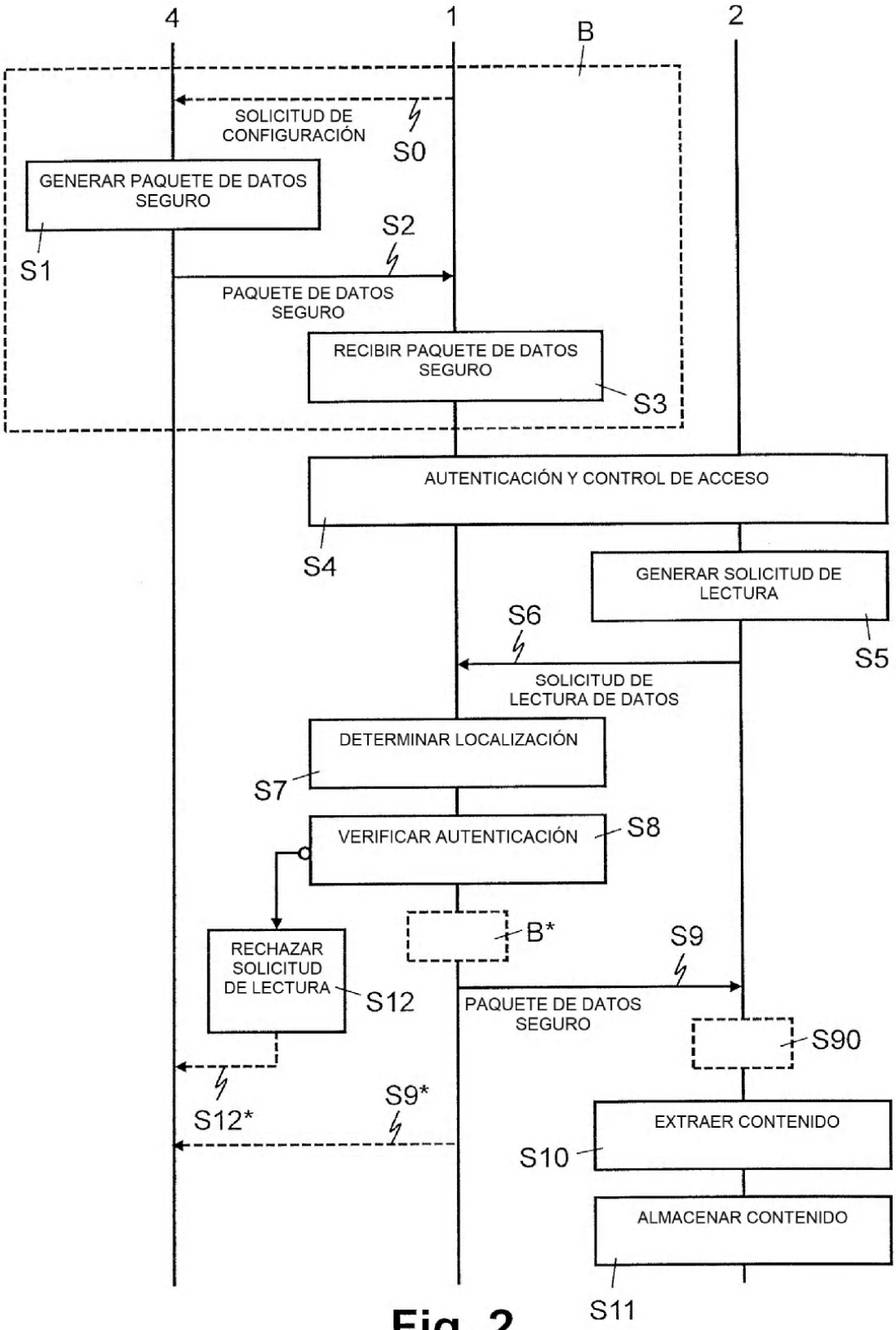
4
1
B
2
SOLICITUD DE CONFIGURACIÓN
S0
GENERAR PAQUETE DE DATOS SEGURO
S1
S2
PAQUETE DE DATOS SEGURO
RECIBIR PAQUETE DE DATOS SEGURO
S3
AUTENTICACIÓN Y CONTROL DE ACCESO
S4
GENERAR SOLICITUD DE LECTURA
S5
S6
SOLICITUD DE LECTURA DE DATOS
DETERMINAR LOCALIZACIÓN
S7
VERIFICAR AUTENTICACIÓN
S8
B*
S9
RECHAZAR SOLICITUD DE LECTURA
S12
PAQUETE DE DATOS SEGURO
S90
S12*
S9*
EXTRAER CONTENIDO
S10
ALMACENAR CONTENIDO
S11

Fig. 2

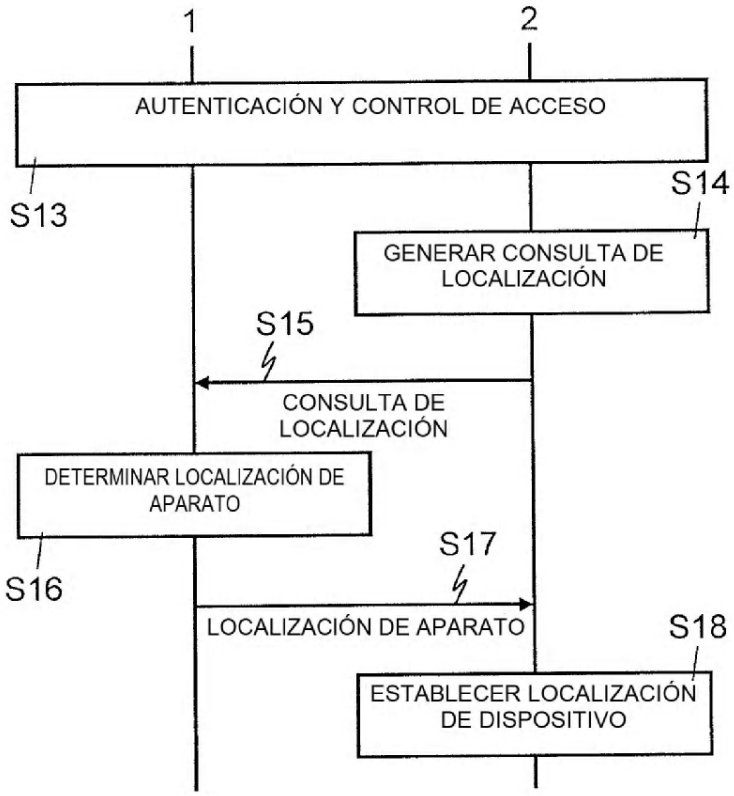
1
2
AUTENTICACIÓN Y CONTROL DE ACCESO
S13
S14
GENERAR CONSULTA DE LOCALIZACIÓN
S15
CONSULTA DE LOCALIZACIÓN
DETERMINAR LOCALIZACIÓN DE APARATO
S16
S17
LOCALIZACIÓN DE APARATO
S18
ESTABLECER LOCALIZACIÓN DE DISPOSITIVO

Fig. 3

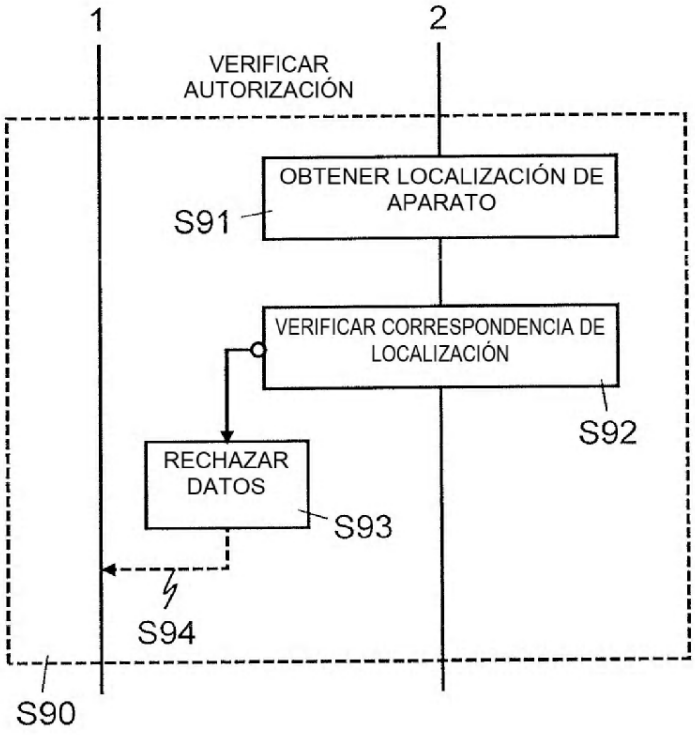
1
2
VERIFICAR AUTORIZACIÓN
OBTENER LOCALIZACIÓN DE APARATO
S91
VERIFICAR CORRESPONDENCIA DE LOCALIZACIÓN
S92
RECHAZAR DATOS
S93
S94
S90

Fig. 5

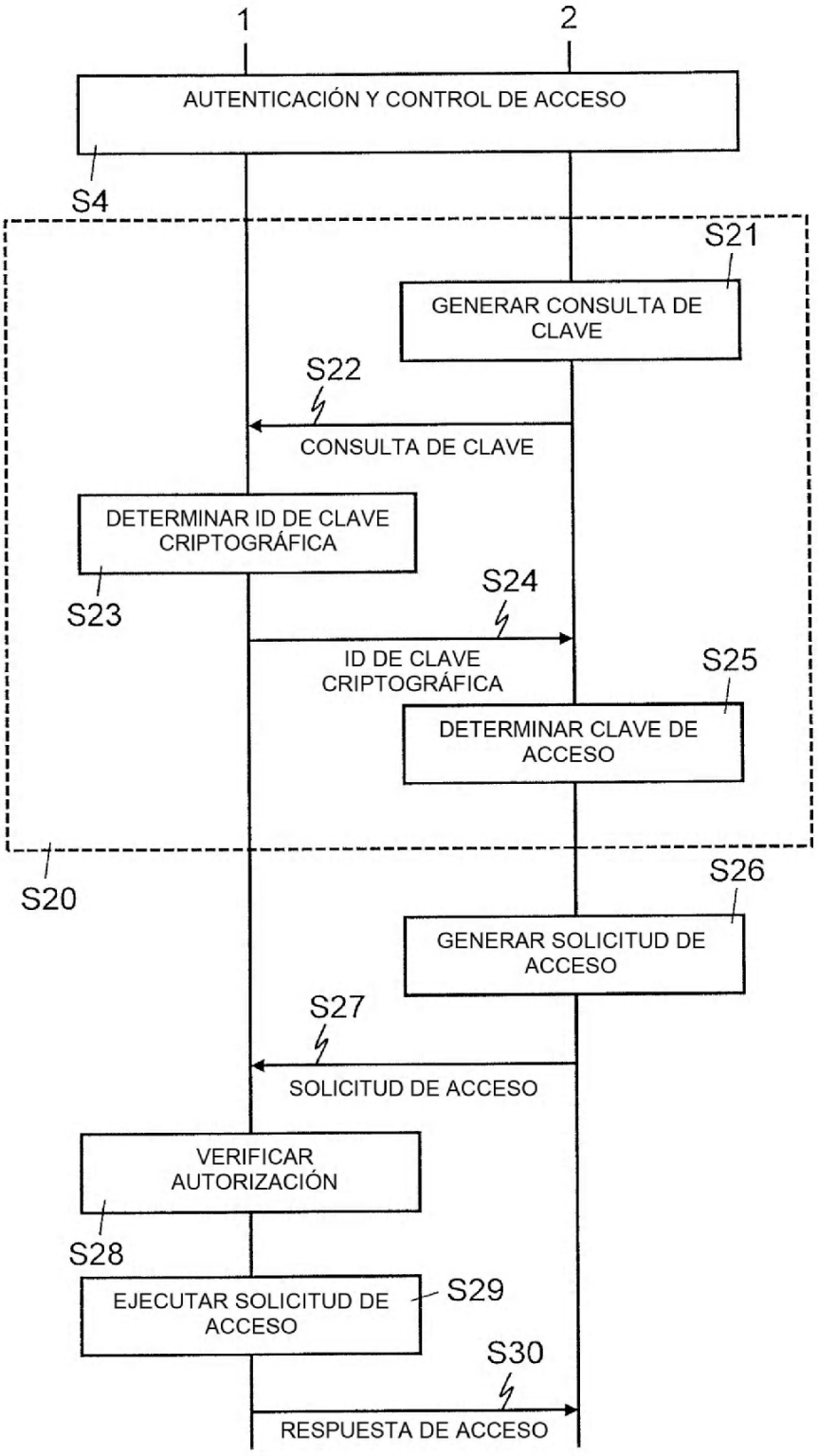
1
2
AUTENTICACIÓN Y CONTROL DE ACCESO
S4
S21
GENERAR CONSULTA DE CLAVE
S22
CONSULTA DE CLAVE
DETERMINAR ID DE CLAVE CRIPTOGRÁFICA
S23
S24
ID DE CLAVE CRIPTOGRÁFICA
S25
DETERMINAR CLAVE DE ACCESO
S20
S26
GENERAR SOLICITUD DE ACCESO
S27
SOLICITUD DE ACCESO
VERIFICAR AUTORIZACIÓN
S28
EJECUTAR SOLICITUD DE ACCESO
S29
S30
RESPUESTA DE ACCESO

Fig. 4