(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 386 749**

(51) Int. CI.:

H04B 5/00 (2006.01)
H04W 12/06 (2009.01)
H04W 76/02 (2009.01)
H04L 29/06 (2006.01)
H04W 88/02 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08749466 .2**
(96) Fecha de presentación: **15.05.2008**
(97) Número de publicación de la solicitud: **2162998**
(97) Fecha de publicación de la solicitud: **17.03.2010**

(54) Título: **Comunicado de datos entre dos soportes de datos móviles pasivos**

(30) Prioridad:
16.05.2007 DE 102007022944

(45) Fecha de publicación de la mención BOPI:
29.08.2012

(45) Fecha de la publicación del folleto de la patente:
29.08.2012

(73) Titular/es:
GIESECKE & DEVRIENT GMBH
PRINZREGENTENSTRASSE 159
81677 MÜNCHEN, DE

(72) Inventor/es:
FINKENZELLER, Klaus y
MARTINI, Ullrich

(74) Agente/Representante:
Arpe Fernández, Manuel

DESCRIPCIÓN

Comunicación de datos entre dos soportes de datos portátiles pasivos

La invención se refiere a un procedimiento para el establecimiento y el funcionamiento de un enlace de comunicación de datos sin contacto entre dos soportes de datos portátiles pasivos por medio de un equipo de comunicación, así como a un equipo de comunicación correspondiente.

Los soportes de datos que se comunican sin contacto se conocen ya en las más diversas formas de realización y para numerosas aplicaciones, por ejemplo como tarjetas de circuitos sin contacto para la compra de tiques o en el servicio de pagos, como módulos de seguridad para el control de acceso o como etiquetas RFID para la protección de mercancía.

Con este fin se aplican distintas tecnologías y protocolos propios y normalizados para la comunicación sin contacto, por ejemplo tarjetas de circuitos sin contacto según ISO/IEC 14443 ó ISO/IEC 15693 o soportes de datos que se comunican según los protocolos NFC ("Near Field Communication [comunicación de campo cercano]") NFCIP-1 ó NFCIP-2 según ECMA-340 ó ECMA-352.

Usualmente y de manera sujeta al sistema, un soporte de datos portátil, por ejemplo una tarjeta de circuitos o un módulo de seguridad, adopta durante la comunicación con un dispositivo lector un papel pasivo y reactivo como, así llamado, "Esclavo" (Slave) también denominado "Objetivo" (Target) en el contexto NFC) y depende de que el dispositivo lector correspondiente, en el papel activo de un, así llamado, "Maestro" (Master) también denominado "Iniciador" (Initiator) en el contexto NFC), lo seleccione entre un número eventualmente mayor de soportes de datos de igual categoría y lo invite a la comunicación. Después, el soporte de datos puede únicamente recibir consultas, instrucciones u órdenes del dispositivo lector y responder a éstas de acuerdo con el protocolo de comunicación elegido. Por lo tanto, una comunicación entre dos soportes de datos pasivos de este tipo no es posible, ya que en cualquier caso se necesita un asociado de comunicación activo como "Maestro".

Por ejemplo en el servicio de pagos o en la compra de tiques, pueden guardarse además datos de aplicación para un almacenamiento seguro y una protección contra manipulación en un módulo de seguridad en forma de un soporte de datos portátil que pueda integrarse en un equipo NFC, o en forma de un módulo conectado de manera fija al equipo NFC. El equipo NFC pone aquí a disposición una interfaz de comunicación pasiva para los soportes de datos, que así pueden emplearse en un papel pasivo como "Objetivo". El equipo NFC, por ejemplo un equipo terminal de radiotelefonía móvil correspondientemente configurado, sirve aquí por lo tanto de interfaz de comunicación y módem entre el módulo de seguridad pasivo, que actúa de "Objetivo", y el dispositivo lector activo, que actúa de "Iniciador". En un contexto de este tipo se habla de "NFC segura (Secure-NFC)".

El documento US 7150407 B1 da a conocer un sistema para el intercambio de datos entre al menos dos soportes de datos sin contacto, en el que al menos uno de los soportes de datos controla activamente el intercambio de datos como "Maestro" y al menos otro soporte de datos es controlado pasivamente como "Esclavo". El soporte de datos que adopta el papel de "Maestro" pone aquí a disposición la energía necesaria para el funcionamiento de al menos otro soporte de datos "Esclavo". Una aplicación de mando, que implementa la función de "Maestro", está almacenada en el soporte de datos "Maestro" de control y es ejecutada por éste.

El documento US 7128274 B2 describe una tarjeta de transacciones segura con una interfaz NFC, pudiendo la interfaz NFC activarse o desactivarse opcionalmente y, en el estado activado, hacerse funcionar como "Iniciador" o como "Objetivo" para, como "Iniciador", enviar activamente datos almacenados en la tarjeta a otro equipo de comunicación NFC tras el establecimiento de un enlace de comunicación con el mismo o, como "Objetivo", responder pasivamente a consultas de un equipo de comunicación NFC de este tipo relativas a los datos almacenados en la tarjeta. El software que controla la interfaz NFC está almacenado en la tarjeta y se ejecuta en un procesador de la tarjeta. La tarjeta dispone además de un suministro de energía propio.

El documento WO2006/137740 da a conocer un procedimiento para el establecimiento de un enlace de comunicación de datos entre dos soportes de datos portátiles pasivos según el preámbulo de la reivindicación 1.

El objetivo de la presente invención es proponer un procedimiento para la comunicación de datos sin contacto entre soportes de datos portátiles pasivos, en particular tarjetas de circuitos sin contacto.

Este objetivo se logra mediante un procedimiento y un equipo de comunicación con las características de las reivindicaciones independientes. En las reivindicaciones dependientes de éstas se indican configuraciones ventajosas y perfeccionamientos.

La idea fundamental del procedimiento según la invención consiste en proporcionar un equipo de comunicación con una aplicación de coordinación que coordine una comunicación de datos sin contacto entre dos soportes de datos portátiles pasivos y, mediante esta coordinación de la comunicación entre los dos soportes de datos pasivos, permitir que uno de los soportes de datos, en sí pasivos, aparezca ante el otro como asociado de comunicación activo.

En el marco de la invención, un asociado de comunicación de una comunicación entre dos asociados de comunicación se designa como pasivo si está habilitado únicamente para aceptar de manera reactiva consultas, instrucciones, órdenes y similares de otro asociado de comunicación activo y responder a las mismas o ejecutarlas. Queda reservado al asociado de comunicación activo iniciar, controlar y terminar una comunicación. Son numerosos los protocolos de comunicación que prevén una comunicación entre un asociado de comunicación activo y uno pasivo. El asociado de comunicación activo se denomina también "Maestro" o "Iniciador" y el asociado de comunicación pasivo "Esclavo" o "Objetivo".

En consecuencia, para establecer un enlace de comunicación de datos entre un primer y un segundo soporte de datos portátil pasivo en el procedimiento según la invención, la aplicación de coordinación del equipo de comunicación establece un primer enlace de comunicación de datos entre el equipo de comunicación y el primer soporte de datos. Además, la aplicación de coordinación establece también un segundo enlace de comunicación de datos sin contacto entre el equipo de comunicación como asociado de comunicación activo y el segundo soporte de datos como asociado de comunicación pasivo. Con la mediación del equipo de comunicación se establece por lo tanto entre los dos soportes de datos un enlace de comunicación de datos indirecto y continuo, estando la trayectoria entre el equipo de comunicación y el segundo soporte de datos configurado como un enlace de comunicación Maestro/Esclavo o Iniciador/Objetivo sin contacto, mientras que la trayectoria entre el equipo de comunicación y el primer soporte de datos puede ser un enlace de comunicación configurado a voluntad, siempre que el primer soporte de datos no sea técnicamente inadecuado para funcionar como asociado de comunicación activo. A este respecto, el equipo de comunicación constituye en cierto modo un puente para la comunicación de datos entre los dos soportes de datos.

La aplicación de coordinación coordina una comunicación de datos entre el primer y el segundo soportes de datos mediante el primer y el segundo enlaces de comunicación de datos de tal manera que el primer soporte de datos aparece ante el segundo soporte de datos como asociado de comunicación activo, es decir que el segundo soporte de datos recibe y responde a consultas del primer soporte de datos. El equipo de comunicación puede aparecer aquí, junto con el primer soporte de datos, ante el segundo soporte de datos como una Black Box (caja negra) que adopta en suma el papel de un asociado de comunicación activo ante el segundo soporte de datos pasivo, de modo que la aplicación de coordinación establece una comunicación Maestro/Esclavo entre la unidad activa, consistente en el primer soporte de datos y el equipo de comunicación, y el segundo soporte de datos pasivo. Así pues, por medio de la aplicación de coordinación es posible unir el primer soporte de datos al equipo de comunicación formando casi una unidad, que como tal adopta conjuntamente el papel de "Maestro" en relación con el segundo soporte de datos como "Esclavo". Al segundo soporte de datos le corresponde aquí el papel de responder a consultas e instrucciones del primer soporte de datos. Así, mediante la coordinación de la aplicación de coordinación, el primer soporte de datos pasivo adopta poco más o menos un papel activo ante el segundo soporte de datos.

Mediante el procedimiento según la invención se hace por consiguiente fácilmente posible una comunicación de datos entre dos soportes pasivos usuales en el comercio, sin que para ello sea necesario modificar ni reequipar los soportes de datos. Además es posible asignar el papel "activo" a cualquiera de los dos soportes de datos.

El primer enlace de comunicación de datos entre el equipo de comunicación y el primer soporte de datos puede estar configurado de distintas maneras. Una comunicación entre la aplicación de coordinación y el primer soporte de datos puede por supuesto seguir un protocolo de comunicación Maestro/Esclavo, en el que el primer soporte de datos adopte el papel pasivo y la aplicación de coordinación el papel activo. Sin embargo, también es posible que la aplicación de coordinación y el primer soporte de datos intercambien datos mediante otros mecanismos distintos de éste, por ejemplo estando el primer soporte de datos acoplado al equipo de comunicación y teniendo ambos acceso a un área de memoria común. Esta área de memoria puede estar asignada tanto al primer soporte de datos como al equipo de comunicación.

El equipo de comunicación según la invención comprende un procesador, una memoria, una interfaz sin contacto y la aplicación de coordinación almacenada en la memoria y ejecutable en el procesador, que está configurada para realizar las etapas del procedimiento según la invención. La interfaz sin contacto del equipo de comunicación puede, al mismo tiempo, estar configurada de manera que sea compatible con soportes de datos sin contacto corrientes, y la aplicación de coordinación puede igualmente soportar los protocolos de comunicación sin contacto corrientes.

La coordinación de la comunicación de datos por parte de la aplicación de coordinación puede comprender el envío de una consulta del equipo de comunicación al segundo soporte de datos mediante el segundo enlace de comunicación de datos Maestro/Esclavo y la recepción de una respuesta del segundo soporte de datos a la consulta mediante la segunda interfaz de comunicación de datos. La aplicación de coordinación puede además recibir datos de consulta del primer soporte de datos mediante la primera interfaz de comunicación de datos y generar una consulta que comprenda los datos de consulta, para transmitir ésta en forma de consulta del primer soporte de datos al segundo soporte de datos. Como alternativa o adicionalmente, la aplicación de coordinación puede extraer datos de la respuesta recibida del segundo soporte de datos y enviar estos datos de respuesta al primer soporte de datos mediante la primera interfaz de comunicación de datos, por ejemplo para contestar a datos de consulta recibidos con anterioridad.

Así pues, de este modo es posible realizar una comunicación de datos completa entre el primer y el segundo soportes de datos. La aplicación de coordinación sirve en esta comunicación para integrar los datos de consulta en una consulta correspondiente o extraer los datos de respuesta de una respuesta correspondiente, sirviendo las consultas y las respuestas, que están configuradas en un formato según un protocolo de comunicación Maestro/Esclavo adecuado, en cierto modo como cápsulas de transporte para los datos de consulta y respuesta que realmente han de intercambiarse entre el primer y el segundo soportes de datos. Otra tarea de la aplicación de coordinación es crear las condiciones previas y básicas para la comunicación de datos correspondiente, o sea establecer un enlace de comunicación de datos e iniciar, controlar y terminar la comunicación.

El aspecto del control por parte de la aplicación de coordinación puede comprender también el seleccionar el segundo soporte de datos entre una pluralidad de soportes de datos pasivos antes de establecer el segundo enlace de comunicación de datos, por ejemplo en el marco de un procedimiento anticolisión. De este modo se permite al primer soporte de datos intercambiar datos con varios segundos soportes de datos, si los segundos soportes de datos respectivos son seleccionados por la aplicación de coordinación del equipo de comunicación sucesivamente o por turnos para la comunicación con el primer soporte de datos.

La coordinación de la comunicación de datos entre el primer y el segundo soportes de datos por parte de la aplicación de coordinación, puede comprender además la coordinación de una autenticación recíproca entre el primer y el segundo soportes de datos. La autenticación recíproca se coordina de manera que la aplicación de coordinación no está en ningún momento del procedimiento de autenticación en posesión de información secreta por medio de la cual se realice la autenticación recíproca. Por consiguiente, si por ejemplo se negocia entre el primer y el segundo soportes de datos una clave de sesión calculada mediante datos secretos respectivamente almacenados en el primer y el segundo soportes de datos, la aplicación de coordinación no está en ningún momento en posesión de estos datos secretos, sino que únicamente impulsa las etapas necesarias para el procedimiento de autenticación y transmite los cálculos intermedios necesarios. De este modo se asegura a continuación una comunicación protegida entre el primer y el segundo soportes de datos.

El equipo de comunicación puede estar configurado para suministrar energía al primer y/o al segundo soporte de datos. Para ello, el segundo soporte de datos recibe usualmente energía mediante un acoplamiento inductivo del campo electromagnético alterno que el equipo de comunicación establece con este fin y con el fin de establecer el segundo enlace de comunicación de datos sin contacto. Siempre que también esté previsto que el primer enlace de comunicación de datos sea sin contacto, el primer soporte de datos puede obtener asimismo su energía mediante un acoplamiento inductivo con el equipo de comunicación. Sin embargo, también es posible que el primer soporte de datos esté acoplado con contacto al equipo de comunicación y se le suministre energía a través de contacto por ejemplo mediante un acumulador del equipo de comunicación. De este modo, una comunicación de datos entre el primer y el segundo soportes de datos depende sólo del equipo de comunicación, que de todos modos es necesario, y no de fuentes de energía adicionales, cuya avería impediría una comunicación de datos.

El primer enlace de comunicación entre el equipo de comunicación y el primer soporte de datos puede establecerse como enlace de comunicación de datos sin contacto, cuando el equipo de comunicación y el primer soporte de datos están conectados mediante una interfaz sin contacto. Igualmente es posible que el primer enlace de comunicación de datos se establezca como un enlace de comunicación de datos con contacto, cuando el equipo de comunicación y el primer soporte de datos están conectados mediante una interfaz de contacto. Así pues, el establecimiento del enlace de comunicación de datos sin contacto entre el primer y el segundo soportes de datos puede realizarse mediante el equipo de comunicación independientemente del tipo del primer soporte de datos, con lo que el procedimiento gana adicionalmente en flexibilidad.

El segundo enlace de comunicación de datos entre el equipo de comunicación y el segundo soporte de datos puede establecerse mediante una interfaz NFC del equipo de comunicación y una interfaz NFC correspondiente del segundo soporte de datos y la comunicación de datos puede coordinarse por medio del protocolo de comunicación NFC. En este caso, el equipo de comunicación puede intercambiar datos como "Iniciador" con un segundo soporte de datos como "Objetivo" NFC, si el segundo soporte de datos es por ejemplo una tarjeta de circuitos sin contacto según ISO/IEC 14443 ó ISO/IEC 15693. Igualmente es posible un primer enlace de comunicación de datos establecido análogamente entre el primer soporte de datos y el equipo de comunicación. De este modo se hace posible por ejemplo una comunicación de datos entre dos tarjetas de circuitos pasivas según ISO/IEC 14443.

El equipo de comunicación puede ser un equipo terminal de radiotelefonía móvil con interfaz NFC adicional. La aplicación de coordinación se ejecuta entonces en un procesador del equipo terminal de radiotelefonía móvil, por ejemplo el controlador de banda base. En tal caso, el primer soporte de datos puede integrarse en el equipo terminal de radiotelefonía móvil, por ejemplo en forma de tarjeta de radiotelefonía móvil (U)SIM u otro módulo de seguridad. En este caso, la aplicación de coordinación establece el primer enlace de comunicación de datos entre el equipo terminal de radiotelefonía móvil y la tarjeta de radiotelefonía móvil (U)SIM en forma de primer enlace de comunicación de datos con contacto. De esta manera es posible para un módulo de seguridad en un equipo terminal de radiotelefonía móvil no sólo participar en una comunicación como asociado de comunicación pasivo (como por ejemplo en la NFC segura), sino también aparecer en el papel de un asociado de comunicación activo en combinación con la aplicación de coordinación.

El equipo de comunicación puede asimismo estar configurado como un dispositivo lector RFID portátil que disponga de un procesador y un suministro de energía propio adecuado. En el procesador se ejecuta la aplicación de coordinación. En este caso, el primer enlace de comunicación de datos entre el primer soporte de datos y el dispositivo lector RFID, se establece como enlace de comunicación de datos sin contacto entre la interfaz RFID del dispositivo lector y una interfaz correspondiente del primer soporte de datos. La comunicación de datos entre el dispositivo lector RFID y el primer soporte de datos se desarrolla entonces, mediante un protocolo de comunicación que prevé para el primer soporte de datos el papel pasivo y para el dispositivo lector el papel activo. En particular, se suministra energía tanto al primer como al segundo soporte de datos mediante un campo electromagnético alterno generado por el dispositivo lector.

Como primer soporte de datos se emplea preferentemente un módulo de seguridad, por ejemplo una tarjeta de radiotelefonía móvil (U)SIM, un TPM (Trusted Platform Module) o similar, o un módulo de transacciones, como por ejemplo una tarjeta de circuitos de servicio de pagos. El segundo soporte de datos puede estar configurado análogamente, o sea también como un módulo de seguridad o de transacciones. Sin embargo, puede tratarse también de un simple transpondedor o similar.

A continuación se describe la invención a modo de ejemplo por medio de los dibujos adjuntos, que muestran:

- figura 1, componentes que participan en una primera forma de realización del procedimiento según la invención y

- figura 2, componentes que participan en una segunda forma de realización del procedimiento según la invención.

Con respecto a la figura 1, un equipo de comunicación 100, configurado como equipo terminal de radiotelefonía móvil, comprende un procesador (CPU) 120, una memoria regrabable no volátil 130, una interfaz sin contacto 140, por ejemplo una interfaz NFC, y un suministro de energía 150, por ejemplo en forma de acumulador, que suministra energía al procesador y en caso dado a la interfaz sin contacto. En la memoria 130 pueden estar almacenados datos y aplicaciones, como por ejemplo la aplicación de coordinación 132 descrita a continuación. Un sistema operativo para el control general del equipo de comunicación puede estar almacenado igualmente en la memoria 130, pero también en una memoria ROM adicional (no mostrada).

Un primer soporte de datos portátil 10 está integrado en el equipo terminal de radiotelefonía móvil 100 en forma de una tarjeta de radiotelefonía móvil (U)SIM. La tarjeta de radiotelefonía móvil (U)SIM puede servir de módulo de seguridad, por ejemplo en la autenticación del equipo terminal de radiotelefonía móvil 100 ante una red de radiotelefonía móvil, pero también en otras aplicaciones, como se describe a continuación. El soporte de datos portátil 10 comprende, no representado ninguno de ellos, un procesador, al menos una memoria, una interfaz de contacto, para conectarse con contacto al equipo de comunicación 100, y un sistema operativo para controlar el soporte de datos 10. Como alternativa, el soporte de datos portátil 10 puede ser también otro módulo de seguridad integrado en el equipo terminal de radiotelefonía móvil 100, por ejemplo una tarjeta inteligente (*SmartCard)*. También es posible un soporte de datos portátil 10 que esté conectado sin contacto al equipo terminal de radiotelefonía móvil 100 mediante la interfaz sin contacto 140 del mismo y que disponga correspondientemente de una interfaz sin contacto.

En la figura 1 está representado un segundo soporte de datos portátil 20 como unidad de seguridad y mando de un actuador 200 sin batería, por ejemplo de un cilindro de cierre sin batería. En el documento DE 10348569 A1 se muestra un ejemplo de un actuador sin batería. También es posible que el soporte de datos portátil 20 esté integrado en otro aparato, por ejemplo en un implante médico, o actúe como un segundo soporte de datos 20 autónomo, por ejemplo como una tarjeta de circuitos sin contacto. El segundo soporte de datos portátil 20 comprende, no representado ninguno de ellos, un procesador, una memoria al menos y un sistema operativo, para controlar el segundo soporte de datos 20, y está acoplado a una interfaz sin contacto 240 y a un actuador 260 del cilindro de cierre 200. El actuador 260 del cilindro de cierre 200 recibe energía a través de la interfaz sin contacto 240 cuando ésta se halla en un campo electromagnético alterno correspondiente, generado por ejemplo por un dispositivo lector RFID. El cilindro de cierre 200 puede disponer adicionalmente de un acumulador de energía (no mostrado) en el que se almacene la energía excedente tomada a través de la interfaz sin contacto 240. Un accionamiento del actuador 260 puede controlarse adicionalmente mediante el segundo soporte de datos portátil 20, que recibe su energía para el funcionamiento a través de la interfaz sin contacto 240 tal y como se describió anteriormente, no disparándose el accionamiento hasta recibirse unos datos predeterminados de un aparato externo, por ejemplo un código que autorice la apertura del cilindro de cierre 200. Un código tal puede por ejemplo almacenarse en el primer soporte de datos portátil 10 o ser generado por éste.

Tras un arranque de la aplicación de coordinación 132 del equipo de comunicación 100, por ejemplo al encender el equipo de comunicación 100 o por acción de un usuario, la aplicación de coordinación 132 establece un primer enlace de comunicación de datos con el primer soporte de datos 10, en este caso con contacto. La transmisión de datos entre la aplicación de coordinación 132 y el primer soporte de datos 10 puede realizarse entonces por ejemplo mediante unas APDU (application protocol data units [unidades de datos de protocolo de aplicación]) correspondientes. Igualmente existe la posibilidad de que tanto la aplicación de coordinación 132 como una rutina de sistema del soporte de datos 10 puedan escribir y leer un área de memoria, por ejemplo en la memoria del soporte de datos 10, para de este modo intercambiar datos, es decir que la comunicación de datos entre el equipo de

comunicación 100 y el primer soporte de datos 10 no tiene que desarrollarse necesariamente según el principio Maestro/Esclavo.

La aplicación de coordinación 132 establece además un segundo enlace de comunicación de datos con el segundo soporte de datos 20. Para ello, la aplicación de coordinación 132 induce al equipo de comunicación 100 a generar un campo electromagnético alterno, preferentemente con una frecuencia de 13,56 MHz, por medio de la interfaz sin contacto 140. Mediante acoplamiento inductivo se suministra así energía al segundo soporte de datos 20 a través de la interfaz sin contacto 240 y es posible establecer un enlace de comunicación de datos sin contacto. Este segundo enlace de comunicación de datos se aplica siempre de manera que la aplicación de coordinación aparezca como asociado de comunicación activo ante el segundo soporte de datos 20 y, en consecuencia, el segundo soporte de datos portátil 20 aparezca como asociado de comunicación pasivo. Este segundo enlace de comunicación de datos puede establecerse de manera respectiva, por ejemplo mediante una interfaz NFC 140, 240 del equipo de comunicación 100 y del cilindro de cierre 200. Los datos se intercambian entonces mediante el protocolo de comunicación NFC, adoptando la aplicación de coordinación el papel del “Iniciador” y el segundo soporte de datos portátil 20, que está conectado a la interfaz sin contacto 240, el papel del “Objetivo”.

En el caso de que haya dos o más soportes de datos 20 en el campo alterno generado por el equipo de comunicación 100, la aplicación de coordinación lleva a cabo un procedimiento anticolisión con el fin de seleccionar un soporte de datos 20 de la pluralidad de soportes de datos, para asegurar una comunicación de datos sin fallos entre el equipo de comunicación 100 y el segundo soporte de datos 20 respectivo. La aplicación de coordinación puede seleccionar para la comunicación varios soportes de datos 20 sucesivamente o por turnos.

Una vez establecidos ambos enlaces de comunicación de datos, el primero entre el equipo de comunicación 100 y el primer soporte de datos 10 y el segundo entre el equipo de comunicación 100 y el segundo soporte de datos 20, la aplicación de coordinación 132 puede pedir información sobre el segundo soporte de datos 20. Los datos de información recibidos entonces del segundo soporte de datos 20 pueden comunicarse al usuario del equipo de comunicación 100 y/o utilizarse para posterior comunicación de datos. Estos datos de información pueden incluir en particular, en forma formalizada y normalizada, información sobre cómo debe realizarse una autenticación recíproca, descrita a continuación, entre el primer soporte de datos 10 y el segundo soporte de datos 20. Una información tal puede recibirse por ejemplo en forma de un archivo guión (*script*) o *batch* (lotes), preferentemente en sintaxis concisa, con lo que bastan unos pocos octetos para codificar la información necesaria y la ejecución de las instrucciones no supone peligro alguno para el equipo de comunicación 100.

La aplicación de coordinación 132 puede además recibir del segundo soporte de datos 20 información específica sobre cómo debe desarrollarse el procedimiento de autenticación. De este modo es posible adaptar un protocolo de autenticación a realizar a distintos segundos soportes de datos 20. Una información específica de este tipo puede estar construida por ejemplo de manera similar a un código de octetos Java, pero en forma simplificada. Un primer octeto puede contener la información de ejecutar una orden “get challenge” descrita a continuación, otro octeto la instrucción de firmar el número aleatorio obtenido a través de la orden “get challenge”, un tercer octeto la información de con qué clave debe tener lugar esto, etc.

La aplicación de coordinación 132 puede ahora invocar un protocolo de autenticación mediante el cual puedan autenticarse recíprocamente el primer soporte de datos 10 y el segundo soporte de datos 20, para que a continuación pueda garantizarse una transmisión de datos protegida entre los dos soportes de datos y excluirse una manipulación de la transmisión de datos por parte de terceros. Para ello, la aplicación de coordinación 132 puede invocar un protocolo de autenticación conocido (por ejemplo CWA 14890-1, ESignK), junto con la indicación de qué claves deben utilizarse. Como alternativa, la autenticación puede llevarse a cabo por ejemplo de manera similar a una “autenticación recíproca [mutal autentícate]” según ISO/IEC7816. Sin embargo, en ésta están previstos un soporte de datos y un terminal como asociados de comunicación. Por este motivo, la aplicación de coordinación 132 debe por ejemplo adoptar el papel de dicho terminal ante el segundo soporte de datos 20 y solicitar a éste por ejemplo que genere un número aleatorio. El primer soporte de datos 10 debe entonces llevar también a cabo las etapas del protocolo de autenticación destinados al terminal en la “autenticación recíproca” según ISO/IEC7816. Esto puede lograrse mediante un reformateado correspondiente de los datos del protocolo. Por ejemplo: la aplicación de coordinación 132 pide al segundo soporte de datos 20 con la orden “get challenge” un número aleatorio y transmite éste al primer soporte de datos 10 para la firma según ESignK. Acto seguido, la aplicación de coordinación 132 reformatea el juego de datos así obtenido a una instrucción “autenticación recíproca”, que se ejecuta en el segundo soporte de datos 20.

Con variantes de este procedimiento entre el primer soporte de datos 10 y el segundo soporte de datos 20 puede también negociarse un secreto, por ejemplo una clave de sesión, que a continuación puede utilizarse para codificar la transmisión de datos entre los dos soportes de datos.

Hay que observar que una clave de sesión negociada en la manera antes indicada sólo es respectivamente conocida caso por el primer soporte de datos 10 y el segundo soporte de datos 20, pero no por la aplicación de coordinación 132. Si al menos uno de los dos soportes de datos comprende un sistema operativo Java, en un perfeccionamiento puede simplificarse el procedimiento antes descrito, implementando APDU especiales para la comunicación de datos entre el equipo de comunicación 100 y el soporte de datos correspondiente. En este caso,

una mini-aplicación *(applet)* Java correspondiente previsto en el soporte de datos puede, mediante un procesador de cifrado también presente, realizar directamente las firmas y codificaciones requeridas por el protocolo.

Ahora, una vez realizada la autenticación recíproca, de la que opcionalmente también puede prescindirse, puede tener lugar la comunicación de datos real entre el primer soporte de datos 10 y el segundo soporte de datos 20 coordinada por la aplicación de coordinación 132. Para ello, la aplicación de coordinación 132 envía una consulta, por ejemplo mediante la instrucción NFC DEP_REQ (Data Exchange Protocol Request [petición de protocolo de intercambio de datos]) al segundo soporte de datos 20 a través del segundo enlace de comunicación de datos sin contacto y recibe a través de éste una respuesta del segundo soporte de datos 20 a esta consulta, por ejemplo mediante la respuesta NFC correspondiente DEP_RES (Data Exchange Protocol Response [Respuesta de protocolo de intercambio de datos]). La consulta puede comprender datos de consulta que la aplicación de coordinación 132 haya recibido del primer soporte de datos 10 mediante el primer enlace de comunicación de datos. Estos datos de consulta pueden enviarse mediante la instrucción de consulta al segundo soporte de datos 20 conforme al protocolo y “empaquetados” en la parte de datos útiles de las tramas correspondientes. De este modo, el primer soporte de datos 10 aparece ante el segundo soporte de datos como “Iniciador” (o “Maestro”), ya que, en un desarrollo tal de la comunicación de datos, el segundo soporte de datos 20 identifica la aplicación de coordinación 132 y el primer soporte de datos 10 como una unidad. La respuesta del segundo soporte de datos 20 puede incluir análogamente datos de respuesta, que son extraídos por la aplicación de coordinación 132 mediante una eliminación por parte de ésta de la información de control de la trama dependiente del formato recibida. Estos datos de respuesta son enviados a continuación por la aplicación de coordinación 132 al primer soporte de datos 10 mediante el primer enlace de comunicación de datos.

Una vez concluida la comunicación de datos, la aplicación de coordinación 132 puede desconectar el primer y el segundo enlaces de comunicación de datos y de este modo terminar la comunicación de datos entre el primer soporte de datos 10 y el segundo soporte de datos 20.

Con respecto a la figura 2, otro equipo de comunicación 300, en forma de un dispositivo lector RFID portátil, comprende un procesador 320, una memoria 330, una interfaz sin contacto 340 y un suministro de energía 350, por ejemplo en forma de un acumulador. Una aplicación de coordinación 332 está almacenada en la memoria 330 y puede ejecutarse en el procesador 320. Un sistema operativo, que por ejemplo puede estar almacenado en una memoria ROM adicional (no mostrada), controla el dispositivo lector RFID.

La funcionalidad de la aplicación de coordinación 332 corresponde a la de la aplicación de coordinación 132 arriba descrita y el dispositivo lector RFID 300 puede emplearse como alternativa al equipo de comunicación 100 para, mediante la aplicación de coordinación 332, establecer un enlace de comunicación de datos entre el primer soporte de datos 10 y el segundo soporte de datos 20 y coordinar una comunicación de datos entre los dos soportes de datos. El dispositivo lector RFID 300 puede emplearse por ejemplo como una especie de equipo de emergencia si se ha agotado el suministro de energía 150 del equipo de comunicación 100. En este caso ya no sería posible un uso normal del equipo de comunicación 100, o sea por ejemplo un accionamiento del cilindro de cierre 200 por medio del primer soporte de datos 10 en comunicación con el segundo soporte de datos 20 previsto en el cilindro de cierre 200.

Generando un campo electromagnético alterno adecuado por medio del suministro de energía propio 350 a través de la interfaz sin contacto 340 y colocándolo adecuadamente en el lugar de empleo, el dispositivo lector RFID 300 suministra entonces energía simultáneamente tanto al primer soporte de datos 10 mediante la interfaz sin contacto 140 como al segundo soporte de datos 20 del cilindro de cierre 200 mediante la interfaz sin contacto 240. Aquí hay que observar que en el diseño del equipo de comunicación 100 se ha tenido en cuenta que debe ser posible suministrar energía al primer soporte de datos 10 no sólo mediante el acumulador 150 del equipo de comunicación 100, sino también mediante la interfaz sin contacto 140 (representado con una línea en trazos). Para ello no es necesario que el equipo de comunicación 100 esté en funcionamiento. De este modo, aunque falte el suministro de energía 150 por parte del equipo de comunicación 100, el soporte de datos 10 puede seguir empleándose como asociado de comunicación pasivo en una comunicación de datos sin contacto.

La comunicación de datos entre el primer soporte de datos 10 y el segundo soporte de datos 20 coordinada mediante la aplicación de coordinación 332, se desarrolla en esencia como se describió anteriormente en relación con la comunicación de datos coordinada mediante la aplicación de coordinación 132. A diferencia de ésta, la aplicación de coordinación 332 establece ahora un primer enlace de comunicación de datos sin contacto entre el dispositivo lector RFID 300 y el primer soporte de datos 10, que puede soportar el mismo protocolo de comunicación que el segundo enlace de comunicación de datos sin contacto entre el dispositivo lector RFID 300 y el segundo soporte de datos 20.

El dispositivo lector RFID 300 puede por supuesto utilizarse también como equipo de comunicación 300 “de pleno valor” y no sólo en los casos de emergencia arriba descritos, por ejemplo para coordinar una comunicación de datos entre dos tarjetas de circuitos sin contacto usuales según ISO/IEC14443.

REIVINDICACIONES

1. Procedimiento para establecer un enlace de comunicación de datos entre un primer (10) y un segundo (20) soportes de datos portátiles pasivos mediante un equipo de comunicación (100; 300) con una aplicación de coordinación (132; 332), con etapas de:
- establecimiento de un primer enlace de comunicación de datos entre el equipo de comunicación (100; 300) y el primer soporte de datos (10) por parte de la aplicación de coordinación (132; 332);
- establecimiento de un segundo enlace de comunicación de datos, sin contacto, entre el equipo de comunicación (100; 300), como asociado de comunicación activo, y el segundo soporte de datos (20), como asociado de comunicación pasivo, por parte de la aplicación de coordinación (132, 332) y
- coordinación de una comunicación de datos entre el primer (10) y el segundo (20) soportes de datos mediante el primer y el segundo enlaces de comunicación de datos por parte de la aplicación de coordinación (132; 332),
caracterizado porque la coordinación se realiza de manera que el primer soporte de datos (10) aparece ante el segundo soporte de datos (20) como asociado de comunicación activo.

2. Procedimiento según la reivindicación 1, caracterizado porque la coordinación de la comunicación de datos comprende etapas de:
- envío de una consulta del equipo de comunicación (100; 300) al segundo soporte de datos (20) mediante el segundo enlace de comunicación de datos por parte de la aplicación de coordinación (132; 332) y
- recepción de una respuesta del segundo soporte de datos (20) a la consulta mediante el segundo enlace de comunicación de datos por parte de la aplicación de coordinación (132; 332),
así como etapas adicionales de:
- recepción de datos de consulta del primer soporte de datos (10) mediante el primer enlace de comunicación de datos y generación de una consulta que comprende los datos de consulta por parte de la aplicación de coordinación (132; 332) antes de enviar la consulta del equipo de comunicación (100; 300) al segundo soporte de datos (20) y/o
- extracción de datos de respuesta de la respuesta recibida del segundo soporte de datos (20) y envío de los datos de respuesta al primer soporte de datos (10) mediante el primer enlace de comunicación de datos por parte de la aplicación de coordinación (132; 332).

3. Procedimiento según la reivindicación 1 ó 2, caracterizado porque la aplicación de coordinación (132; 332) selecciona el segundo soporte de datos (20) entre varios soportes de datos portátiles pasivos para establecer un enlace de comunicación de datos, sin contacto, entre el equipo de comunicación (100; 300) y el segundo soporte de datos (20).

4. Procedimiento según una de las reivindicaciones 1 a 3, caracterizado porque, durante la coordinación de una comunicación de datos entre el primer (10) y el segundo (20) soportes de datos, la aplicación de coordinación (132; 332) coordina una autenticación recíproca entre el primer (10) y el segundo (20) soportes de datos.

5. Procedimiento según una de las reivindicaciones 1 a 4, caracterizado porque se suministra energía al primer soporte de datos (10) y/o al segundo soporte de datos (20) mediante el equipo de comunicación (100; 300).

6. Procedimiento según una de las reivindicaciones 1 a 5, caracterizado porque la aplicación de coordinación (132; 332) establece el primer enlace de comunicación de datos entre el equipo de comunicación (100; 300) y el primer soporte de datos (10) en forma de un enlace de comunicación de datos sin contacto, cuando el equipo de comunicación (300) y el primer soporte de datos (10) están conectados mediante una interfaz sin contacto (140; 340), o en forma de un enlace de comunicación de datos con contacto, cuando el equipo de comunicación (100) y el primer soporte de datos (10) están conectados mediante una interfaz de contacto.

7. Procedimiento según una de las reivindicaciones 1 a 6, caracterizado porque el primer enlace de comunicación de datos entre el equipo de comunicación (100; 300) y el primer soporte de datos (10) y/o el segundo enlace de comunicación de datos entre el equipo de comunicación (100; 300) y el segundo soporte de datos (20) se establece entre una interfaz NFC (140; 340) del equipo de comunicación (100; 300) y una interfaz NFC del primer soporte de datos (10) y/o una interfaz NFC del segundo soporte de datos (20), coordinándose la comunicación de datos a través del primer enlace de comunicación de datos y/o a través del segundo enlace de comunicación de datos por medio del protocolo de comunicación NFC.

8. Procedimiento según una de las reivindicaciones 1 a 7, caracterizado porque el equipo de comunicación (100) es un equipo terminal de radiotelefonía móvil y la aplicación de coordinación (132) se ejecuta en un procesador (120) del equipo terminal de radiotelefonía móvil, siendo el primer soporte de datos (10) una tarjeta de radiotelefonía móvil (U)SIM empleada en el equipo terminal de radiotelefonía móvil, estableciendo la aplicación de coordinación (132) un primer enlace de comunicación de datos, con contacto, con la tarjeta de radiotelefonía móvil (U)SIM mediante una interfaz de contacto entre el equipo terminal de radiotelefonía móvil y la tarjeta de radiotelefonía móvil (U)SIM.

9. Procedimiento según una de las reivindicaciones 1 a 7, caracterizado porque el equipo de comunicación (300) es un dispositivo lector RFID portátil y la aplicación de coordinación (332) se ejecuta en un procesador (320) del dispositivo lector RFID, estableciendo la aplicación de coordinación (332) un primer enlace de comunicación de

datos, sin contacto, con el primer soporte de datos (10) mediante una interfaz RFID (340) entre dicho dispositivo lector RFID y dicho primer soporte de datos (10).

10. Procedimiento según una de las reivindicaciones 1 a 9, caracterizado porque la aplicación de coordinación (132; 332) establece el primer enlace de comunicación de datos con un módulo de seguridad, en particular una tarjeta de radiotelefonía móvil (U)SIM, o con un módulo de transacciones, en particular una tarjeta de circuitos de servicio de pagos, como primer soporte de datos (10).

11. Equipo de comunicación (100; 300), que comprende un procesador (120; 320), una memoria (130; 330), una interfaz sin contacto (140; 340) y una aplicación de coordinación (132; 332) presente en la memoria (130; 330) y ejecutable en el procesador (120; 320), estando la aplicación de coordinación (132; 332) configurada para
- establecer un primer enlace de comunicación de datos entre el equipo de comunicación (100; 300) y un primer soporte de datos portátil pasivo (10) y
- establecer un segundo enlace de comunicación de datos, sin contacto, entre la interfaz sin contacto (140; 340) del equipo de comunicación (100; 300) y un segundo soporte de datos portátil pasivo (20), de manera que el equipo de comunicación (100; 300) funcione como asociado de comunicación activo ante el segundo soporte de datos pasivo (20),
estando el equipo de comunicación caracterizado porque la aplicación de coordinación está configurada además para
- coordinar una comunicación de datos del equipo de comunicación (100; 300) entre el primer (10) y el segundo (20) soportes de datos mediante el primer y el segundo enlaces de comunicación de datos de manera que el primer soporte de datos (10) aparezca ante el segundo soporte de datos (20) como asociado de comunicación activo.

12. Equipo de comunicación (100; 300) según la reivindicación 11, caracterizado porque la aplicación de coordinación (132; 332) está configurada para efectuar la coordinación de la comunicación de datos mediante
- el envío de una consulta al segundo soporte de datos (20) por medio del segundo enlace de comunicación de datos y
- la recepción de una respuesta del segundo soporte de datos (20) a la consulta por medio del segundo enlace de comunicación de datos,
y además mediante
- la recepción de datos de consulta del primer soporte de datos (10) mediante el primer enlace de comunicación de datos y la generación de una consulta que comprenda los datos de consulta para el envío al segundo soporte de datos (20) y/o
- la extracción de datos de respuesta de la respuesta recibida del segundo soporte de datos (20) y el envío de éstos al primer soporte de datos (10) mediante el primer enlace de comunicación de datos.

13. Equipo de comunicación (100; 300) según la reivindicación 11 o 12, caracterizado porque la aplicación de coordinación (132; 332) está configurada para seleccionar el segundo soporte de datos (20) entre varios soportes de datos portátiles pasivos accesibles a través de la interfaz sin contacto (140; 340), con el fin de establecer el enlace de comunicación de datos sin contacto entre el equipo de comunicación (100; 300) y el segundo soporte de datos (20).

14. Equipo de comunicación (100; 300) según una de las reivindicaciones 11 a 13, caracterizado porque la aplicación de coordinación (132; 332) está configurada para, durante la coordinación de la comunicación de datos entre el primer (10) y el segundo (20) soportes de datos, coordinar una autenticación recíproca entre el primer (10) y el segundo (20) soportes de datos.

15. Equipo de comunicación (100; 300) según una de las reivindicaciones 11 a 14, caracterizado porque la aplicación de coordinación (132; 332) está configurada para originar un suministro de energía al segundo soporte de datos (20) mediante la interfaz sin contacto (240) y/o suministrar energía al primer soporte de datos (10) mediante la interfaz sin contacto (140) o una interfaz de suministro de energía con contacto.

16. Equipo de comunicación (100; 300) según una de las reivindicaciones 11 a 15, caracterizado porque la aplicación de coordinación (132; 332) está configurada para establecer el primer enlace de comunicación de datos entre la interfaz sin contacto (140; 340) del equipo de comunicación (100; 300) y una interfaz sin contacto correspondiente del primer soporte de datos (10), en forma de un enlace de comunicación de datos sin contacto, o entre una interfaz de contacto del equipo de comunicación (100; 300) y una interfaz de contacto correspondiente del primer soporte de datos (10).

17. Equipo de comunicación (100; 300) según una de las reivindicaciones 11 a 16, caracterizado por una interfaz NFC como interfaz sin contacto (140; 340) y porque la aplicación de coordinación (132; 332) está configurada para establecer el primer enlace de comunicación de datos con el primer soporte de datos (10) y/o el segundo enlace de comunicación de datos con el segundo soporte de datos (20) entre la interfaz NFC del equipo de comunicación (100; 300) y una interfaz NFC correspondiente del primer soporte de datos (10) y/o del segundo soporte de datos (20) y coordinar la comunicación de datos a través del primer enlace de comunicación de datos y/o a través del segundo enlace de comunicación de datos por medio del protocolo de comunicación NFC.

18. Equipo de comunicación (100; 300) según la reivindicación 17, caracterizado porque la aplicación de coordinación (132; 332) está configurada para, mediante el protocolo de comunicación NFC, enviar instrucciones al segundo soporte de datos (20) y recibir respuestas del segundo soporte de datos (20).

19. Equipo de comunicación (100; 300) según una de las reivindicaciones 11 a 18, caracterizado porque el equipo de comunicación (100) es un equipo terminal de radiotelefonía móvil con una interfaz de contacto y está configurado para admitir una tarjeta de radiotelefonía móvil (U)SIM como primer soporte de datos (10) y la aplicación de coordinación (132) está configurada para, mediante la interfaz de contacto, establecer un primer enlace de comunicación de datos, con contacto, con una interfaz de contacto correspondiente de la tarjeta de radiotelefonía móvil (U)SIM.

20. Equipo de comunicación (300) según una de las reivindicaciones 11 a 18, caracterizado porque el equipo de comunicación (300) es un dispositivo lector RFID con una interfaz RFID (340) y la aplicación de coordinación (332) está configurada para, mediante la interfaz RFID (340), establecer un primer enlace de comunicación de datos, sin contacto, con una interfaz RFID correspondiente del primer soporte de datos (10).

21. Equipo de comunicación (100; 300) según una de las reivindicaciones 11 a 20, caracterizado porque la aplicación de coordinación (132; 332) está configurada para establecer el primer enlace de comunicación de datos con un módulo de seguridad, en particular una tarjeta de radiotelefonía móvil (U)SIM, o con un módulo de transacciones, en particular una tarjeta de circuitos de servicio de pagos, como primer soporte de datos (10).

Fig. 1

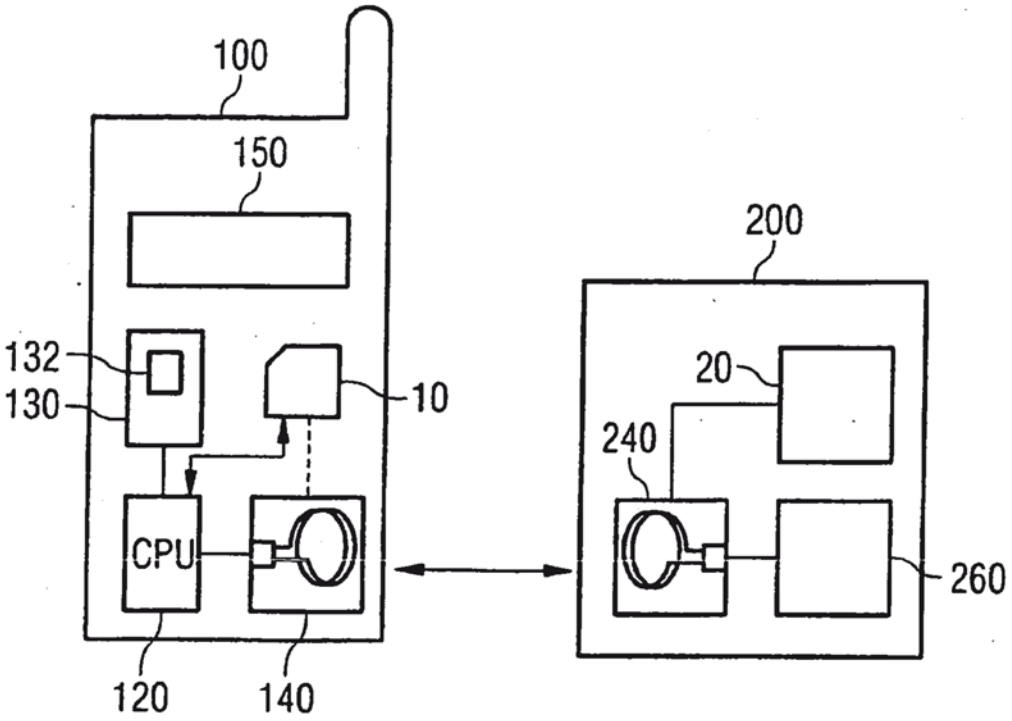
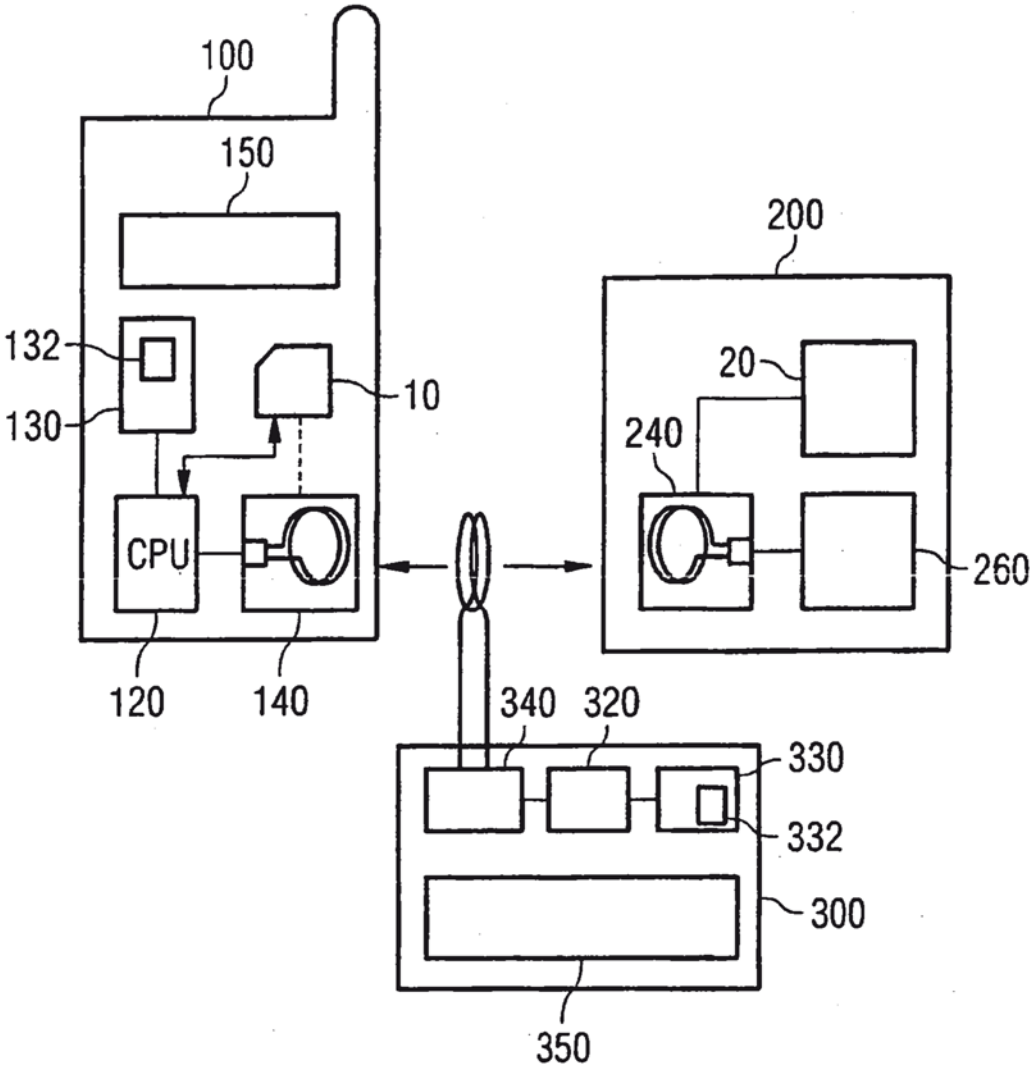


Fig. 2


100
150
200
132
130
10
20
240
CPU
260
120
140
340
320
330
332
300
350

REFERENCIAS CITADAS EN LA DESCRIPCIÓN

La lista de referencias citada por el solicitante lo es solamente para utilidad del lector, no formando parte de los documentos de patente europeos. Aún cuando las referencias han sido cuidadosamente recopiladas, no pueden excluirse errores u omisiones y la OEP rechaza toda responsabilidad a este respecto.

Documentos de patente citados en la descripción

- US 7150407 B1 **[0006]**
- US 7128274 B2 **[0007]**
- WO 2006137740 A **[0008]**
- DE 10348569 A1 **[0031]**