(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 569 086**

(51) Int. CI.:

H04L 9/08 (2006.01)
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)
H04W 12/00 (2009.01)
H04W 12/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **03.06.2010 E 10850969 (6)**

(97) Fecha y número de publicación de la concesión europea: **17.02.2016 EP 2568654**

(54) Título: **Método para acceder a comunicación de radiofrecuencia con una comunicación magnética de baja frecuencia**

(30) Prioridad:

05.05.2010 CN 201010163064

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
06.05.2016

(73) Titular/es:

NATIONZ TECHNOLOGIES INC. (100.0%)
Room 301&302, Building No. 3 Shenzhen Software Park In Hi-tech Industry Zone Nanshan District
Shenzhen, Guangdong 518057, CN

(72) Inventor/es:

YANG, XIANWEI

(74) Agente/Representante:

IZQUIERDO BLANCO, María Alicia

DESCRIPCIÓN

Método para acceder a comunicación de radiofrecuencia con una comunicación magnética de baja frecuencia.

Campo de la invención

La presente invención está relacionada con el campo de las comunicaciones, en particular con un método para acceder a comunicación de radiofrecuencia con una comunicación magnética de baja frecuencia.

Descripción de la técnica anterior

Junto con el desarrollo de las tecnologías de pago electrónico, los medios de pago electrónico y por móviles son una tendencia inevitable y segura. El pago por móvil combina la portabilidad de la movilidad y la independencia del pago electrónico. La gran cantidad de usuarios con móviles representa una base excelente para el desarrollo del pago por móvil. Por consiguiente, el pago por móvil tendrá un enorme mercado, en el que un sistema de comunicación de corto alcance que consiste en un tarjeta SIM de radiofrecuencia con comunicación magnética de baja frecuencia y un lector de tarjetas de esta es una aplicación típica de pago por móvil. En el sistema de comunicación de corto alcance que consiste en una tarjeta SIM de radiofrecuencia con comunicación magnética de baja frecuencia y un lector de tarjetas de esta, la comunicación magnética de baja frecuencia se utiliza para el control de rango y las transacción se realizan mediante comunicación de radiofrecuencia.

Cuando la tarjeta SIM de radiofrecuencia con comunicación magnética de baja frecuencia se utiliza como una tarjeta de pago de autobús, una tarjeta de acceso, una tarjeta de crédito, tarjeta de débito para montos bajos, una tarjeta de asistencia y otras tarjetas inteligentes, por lo general es necesario realizar la autenticación de acceso de la tarjeta SIM de radiofrecuencia y la transacción completa en un período extremadamente corto para mejorar la conveniencia de la aplicación de la tarjeta SIM de radiofrecuencia como una herramienta de identificación o de pago de montos pequeños.

En sistemas de comunicación de corto alcance existentes de tarjetas SIM de radiofrecuencia con comunicación magnética de baja frecuencia, se introducen canales de baja frecuencia y como consecuencia, las propiedades físicas de los canales de baja frecuencia determinan que la velocidad de transmisión de datos no puede ser muy alta, provocando una velocidad de acceso relativamente baja. Por consiguiente, la velocidad de acceso total del sistema con comunicación magnética de baja frecuencia es menor que la velocidad de acceso de comunicación de radiofrecuencia sola. Hasta cierto punto, aumenta el exceso de tiempo para el acceso y por lo tanto aumenta el exceso de tiempo para toda la transacción, lo que afecta hasta cierto punto, a la satisfacción del usuario en algunas aplicaciones . Al mismo tiempo, los sistemas de comunicación de corto alcance existentes de tarjetas SIM de radiofrecuencia con comunicación magnética de baja frecuencia no consideran la autenticación entre la parte solicitante y la parte solicitada en el proceso de acceso, y en la comunicación subsiguiente, los datos no se cifran, creando ciertos riesgos para la seguridad de los datos.

La EP 0,800,293 A es un ejemplo representativo del actual estado de la técnica.

Sumario de la invención

El problema técnico que la presente invención se propone resolver es proporcionar un método para acceder a una comunicación de radiofrecuencia con comunicación magnética de baja frecuencia, acelerar la velocidad de acceso de comunicación de radiofrecuencia de un sistema de comunicación de corto alcance con comunicación magnética de baja frecuencia y mejorar la satisfacción del usuario. La presente invención proporciona un método para acceder a la comunicación de radiofrecuencia con comunicación magnética de baja frecuencia, de acuerdo con las reivindicaciones que siguen.

La presente invención propone un método para acceder a la comunicación de radiofrecuencia con comunicación magnética de baja frecuencia para resolver el problema técnico mencionado, comprendiendo:

Paso a: una parte solicitante envía una solicitud de activación a través de un canal de baja frecuencia, a saber un código característico de baja frecuencia, en el que dicho código característico de baja frecuencia comprende un primer número aleatorio generado por la parte solicitante;
Paso b: una parte solicitada recibe la solicitud de activación a través del canal de baja frecuencia, genera un mensaje de respuesta de activación y envía el mensaje de respuesta de activación en una primera dirección de comunicación de radiofrecuencia a través del canal de radiofrecuencia, en el que el mensaje de respuesta de activación comprende un segundo número aleatorio generado por la parte solicitada y un identificador de identidad de la parte solicitada;
Paso c: la parte solicitante recibe el mensaje de respuesta de activación en la primera dirección de comunicación de radiofrecuencia a través del canal de radiofrecuencia y realiza la verificación, genera una solicitud de conexión si pasa la verificación, y envía la solicitud de conexión en una segunda dirección de comunicación de radiofrecuencia a través del canal de radiofrecuencia, en el que la solicitud de conexión comprende un tercer

número aleatorio;
Paso d: la parte solicitada recibe la solicitud de conexión en la segunda dirección de comunicación de radiofrecuencia a través del canal de radiofrecuencia y realiza la verificación, genera un mensaje de respuesta de conexión si pasa la verificación, y envía el mensaje de respuesta de conexión en la segunda dirección de comunicación de radiofrecuencia a través del canal de radiofrecuencia;
Paso e: la parte solicitante recibe el mensaje de respuesta de conexión en la segunda dirección de comunicación de radiofrecuencia a través del canal de radiofrecuencia, verifica si el acceso es exitoso, y negocia con la parte solicitada en la segunda dirección de comunicación de radiofrecuencia a través del canal de radiofrecuencia si el acceso es exitoso.

Además, el método anterior puede además tener las características siguientes: la longitud de dicho código característico de baja frecuencia es igual o menor de 2 bytes.

Además, el método anterior puede además tener las características siguientes: dicho código característico de baja frecuencia comprende solamente dicho primer número aleatorio, y la longitud de dicho primer número aleatorio es 1 byte.

Además, el método anterior puede además tener las características siguientes, dicho paso b comprende:

Paso b1, la parte solicitada recibe la solicitud de activación a través del canal de baja frecuencia;
Paso b2, la parte solicitada genera un segundo número aleatorio;
Paso b3, la parte solicitada calcula la frecuencia de comunicación de radiofrecuencia según el método de cálculo de frecuencia predeterminado por las dos partes y basado en el primer número aleatorio en dicha solicitud de activación y el número máximo de puntos de frecuencia utilizados por el canal de radiofrecuencia;
Paso b4, la parte solicitada calcula la primera dirección de comunicación de radiofrecuencia según el método de cálculo de dirección predeterminado por las dos partes y basado en el primer número aleatorio;
Paso b5, la parte solicitada genera un primer identificador de cifrado, dicho primer identificador de cifrado contiene el método para cifrar las sesiones de transacción seleccionadas por la parte solicitada y el algoritmo de cifrado compatible;
Paso b6, la parte solicitada utiliza dicho segundo número aleatorio, el identificador de identidad de la parte solicitada y dicho primer identificador de cifrado como la entrada de información de cifrado, utiliza dichos primer número aleatorio y segundo número aleatorio como la clave de cifrado, adopta un algoritmo de cifrado predeterminado para realizar la operación de cifrado, y toma los primeros 4 bytes del resultado del cifrado como el primer código de control;
Paso b7, la parte solicitada genera un mensaje de respuesta de activación, dicho mensaje de respuesta de activación que comprende dicho segundo número aleatorio, el identificador de identidad de la parte solicitada, el primer identificador de cifrado y el primer código de control;
Paso b8, la parte solicitada envía dicho mensaje de respuesta de activación en la primera dirección de comunicación de radiofrecuencia en la frecuencia calculada de comunicación de radiofrecuencia a través del canal de radiofrecuencia.

Además, el método anterior puede además tener las características siguientes: en dicho paso b2, la longitud de dicho segundo número aleatorio es 4 bytes.

Además, el método anterior puede además tener las características siguientes, en dicho paso b3, dicho método de cálculo de frecuencia predeterminado es: con el número máximo de puntos de frecuencia utilizados por el canal de radiofrecuencia como el modo, realizando una operación para obtener un resto en dicho primer número aleatorio, el resto obtenido corresponde a la numeración de la frecuencia utilizada por la comunicación de radiofrecuencia, y dicha frecuencia de la comunicación de radiofrecuencia es obtenida según dicha numeración.

Además, el método anterior puede además tener las características siguientes: en dicho paso b5, se indica que no hay cifrado cuando dicho primer identificador de cifrado es igual a 0, y se indica que hay cifrado y el cifrado es realizado con el algoritmo identificado por el primer identificador de cifrado cuando dicho primer identificador de cifrado no es igual a 0.

Además, el método anterior puede además tener las características siguientes: en dicho paso b6, la entrada de cifrado es RN2| |ID2| |ALG1, y la clave de cifrado es RN1| |RN2, en la que «| |» representa una concatenación.

Además, el método anterior puede además tener las características siguientes, dicho paso c comprende:

Paso c1, la parte solicitante calcula la frecuencia de comunicación de radiofrecuencia según el método de cálculo de frecuencia predeterminado por las dos partes y basado en el primer número aleatorio y el número máximo de puntos de frecuencia utilizados por el canal de radiofrecuencia;
Paso c2, la parte solicitante calcula la primera dirección de comunicación de radiofrecuencia según el método de cálculo de dirección predeterminado por las dos partes y basado en el primer número aleatorio;
Paso c3, la parte solicitante recibe dicho mensaje de respuesta de activación en la primera dirección de

comunicación de radiofrecuencia en la frecuencia calculada de comunicación de radiofrecuencia a través del canal de radiofrecuencia.

Paso c4, la parte solicitante utiliza el segundo número aleatorio, el identificador de identidad de la parte solicitada y dicho primer identificador de cifrado en dicho mensaje de respuesta de activación como la entrada de cifrado, utiliza dichos primer número aleatorio y segundo número aleatorio como la clave de cifrado, adopta un algoritmo predeterminado para realizar la operación de cifrado, toma los primeros 4 bytes del resultado del cifrado como el primer código de control, y después compara dicho primer código de control con el primer código de control contenido en dicho mensaje de respuesta de activación; si los dos son idénticos, entonces pasa la verificación, y va al paso c5; de lo contrario, el acceso es incorrecto y se termina este proceso de acceso;

Paso c5, la parte solicitante genera un tercer número aleatorio;

Paso c6, la parte solicitante genera un segundo identificador de cifrado, dicho segundo identificador de cifrado contiene el método para cifrar las sesiones de transacción seleccionadas por la parte solicitante y el algoritmo de cifrado compatible;

Paso c7, la parte solicitante utiliza dicho tercer número aleatorio, el identificador de identidad de la parte solicitante y dicho segundo identificador de cifrado como la entrada de información de cifrado, utiliza dichos primer número aleatorio, segundo número aleatorio y tercer número aleatorio como la clave de cifrado, adopta un algoritmo de cifrado predeterminado para realizar la operación de cifrado, y toma los primeros 4 bytes del resultado del cifrado como el segundo código de control;

Paso c8, la parte solicitante genera una solicitud de conexión, dicha solicitud de conexión contiene dicho tercer número aleatorio, el identificador de identidad de la parte solicitante, el segundo identificador de cifrado y el segundo código de control;

Paso c9, la parte solicitante calcula la segunda dirección de comunicación de radiofrecuencia según el método de cálculo de dirección predeterminado por las dos partes y basado en el primer número aleatorio y el segundo número aleatorio;

Paso c10, la parte solicitante envía dicha solicitud de conexión en la segunda dirección de comunicación de radiofrecuencia a la frecuencia de comunicación de radiofrecuencia a través del canal de radiofrecuencia.

Además, el método anterior puede además tener las características siguientes: en dicho paso c5, la longitud de dicho tercer número aleatorio es 3 bytes.

Además, el método anterior puede además tener las características siguientes: en dicho paso c7, la entrada de cifrado es RN3 | | ID1 | |ALG2, y la clave de cifrado es RN1 | | RN2 | | RN3, en la que «| |» representa una concatenación.

Además, el método anterior puede además tener las características siguientes: en dicho paso c9, dicho método de cálculo de la segunda dirección de comunicación de radiofrecuencia es: con dichos primer número aleatorio y segundo número aleatorio como entrada, realizando una operación de función unidireccional predeterminada, y asignado todos o parte de los resultados operativos obtenidos como la segunda dirección de comunicación de radiofrecuencia.

Además, el método anterior puede además tener las características siguientes: en dicho paso c9, dicho método de cálculo de la segunda dirección de comunicación de radiofrecuencia es: tomar toda o parte de RN1 | | RN2 como la segunda dirección de comunicación de radiofrecuencia, en el que «| |» representa una concatenación.

Además, el método anterior puede además tener las características siguientes, dicho paso d comprende:

Paso d1, la parte solicitada calcula la segunda dirección de comunicación de radiofrecuencia según el método de cálculo de dirección predeterminado por las dos partes y basado en el primer número aleatorio y el segundo número aleatorio;

Paso d2, la parte solicitada recibe dicha solicitud de conexión en la segunda dirección de comunicación de radiofrecuencia a la frecuencia de comunicación de radiofrecuencia a través del canal de radiofrecuencia;

Paso d3, la parte solicitada utiliza el tercer número aleatorio, el identificador de identidad de la parte solicitante y dicho segundo identificador de cifrado en dicha solicitud de conexión como la entrada de cifrado, utiliza dichos primer número aleatorio, segundo número aleatorio y tercer número aleatorio como la clave de cifrado, adopta un algoritmo de cifrado predeterminado para realizar la operación de cifrado, toma los primeros 4 bytes del resultado del cifrado como el segundo código de control, y después compara dicho segundo código de control con el segundo código de control contenido en dicha solicitud de conexión, si los dos son idénticos, entonces pasa la verificación, de lo contrario, falla la verificación;

Paso d4, la parte solicitada fija un identificador de estado de conexión exitosa/fallida según el resultado de verificación del segundo código de control. Si el segundo código de control pasa la verificación, después dicho identificador de estado de conexión exitosa/fallida se establece como conexión exitosa, y va al paso d5; de lo contrario, dicho identificador de estado de la conexión exitosa/fallida se establece como conexión fallida, y va al paso d6;

Paso d5, la parte solicitada genera un tercer identificador de cifrado, dicho tercer identificador de cifrado contiene el método para cifrar las sesiones de transacción finalmente seleccionadas por la parte solicitada y el algoritmo de cifrado compatible;

Paso d6, la parte solicitada utiliza el tercer número aleatorio, el identificador de estado de conexión exitosa/fallida y dicho tercer identificador de cifrado como la entrada de información de cifrado, utiliza dichos primer número aleatorio, segundo número aleatorio y tercer número aleatorio como la clave de cifrado, adopta un algoritmo de cifrado predeterminado para realizar la operación de cifrado, y toma los primeros 4 bytes del resultado del cifrado como el tercer código de control;
Paso d7, la parte solicitada genera un mensaje de respuesta de conexión, dicho mensaje de respuesta de conexión contiene el identificador de estado de la conexión exitosa/fallida, el tercer identificador de cifrado y el tercer código de control;
Paso d8, la parte solicitada envía dicho mensaje de respuesta de conexión en la segunda dirección de comunicación de radiofrecuencia a través del canal de radiofrecuencia.

Además, el método anterior puede además tener las características siguientes: en dicho paso d6, la entrada de cifrado es RN3 | | SFF | |ALG3, y la clave de cifrado es RN1 | | RN2 | | RN3, en la que «| |» representa una concatenación.

Además, el método anterior puede además tener las características siguientes, dicho paso e comprende:

Paso e1, la parte solicitante recibe dicho mensaje de respuesta de conexión en la segunda dirección de comunicación de radiofrecuencia a través del canal de radiofrecuencia;
Paso e2, la parte solicitante utiliza el tercer número aleatorio, el identificador de estado de la conexión exitosa/fallida y dicho tercer identificador de cifrado en dicho mensaje de respuesta de conexión como la entrada de cifrado, utiliza dichos primer número aleatorio, segundo número aleatorio y tercer número aleatorio como la clave de cifrado, adopta un algoritmo de cifrado predeterminado para realizar la operación de cifrado, toma los primeros 4 bytes del resultado del cifrado como el tercer código de control, y después compara dicho tercer código de control con el tercer código de control contenido en dicho mensaje de respuesta de conexión, si los dos son idénticos, entonces pasa la verificación, y va al paso e3; de lo contrario, falla la verificación y se termina este proceso de acceso;
Paso e3, la parte solicitante determina si el acceso por la parte solicitada es exitoso, o no, basado en el identificador de estado de la conexión exitosa/fallida en dicho mensaje de respuesta de conexión, si falla el acceso, después se termina este proceso de acceso; de lo contrario, va al paso e4;
Paso e4, la parte solicitante y la parte solicitada realizan transacciones en la segunda dirección de comunicación de radiofrecuencia a través del canal de radiofrecuencia.

Además, el método anterior puede además tener las características siguientes: en dicho paso e4, una clave de cifrado de sesión se utiliza en dichas transacciones.

Además, el método anterior puede además tener las características siguientes: dicha clave de cifrado de sesión tiene 8 bytes RN1 | | RN2 | | RN3 | | o 16 bytes RN1 | | RN2| | RN3 | | RN1 | | RN2 | | RN3 | |, en la que «| |» representa una concatenación y RN1 | | RN2 | | RN3 es la inversión bit por bit de RN1 | | RN2 | | RN3.

El método para acceder a una comunicación de radiofrecuencia con comunicación magnética de baja frecuencia según la presente invención puede acelerar la velocidad de acceso de comunicación de radiofrecuencia de un sistema de comunicación de corto alcance con comunicación magnética de baja frecuencia y mejorar la satisfacción del usuario.

Breve descripción de los dibujos adjuntos

La figura 1 es un diagrama de bloques de la estructura de la parte solicitante;
La figura 2 es un diagrama de bloques de la estructura de la parte solicitada;
La figura 3 es un diagrama de flujo del método para el acceso a la comunicación de radiofrecuencia con comunicación magnética de baja frecuencia según una forma de realización de la presente invención.

Descripción detallada de las formas de realización preferidas

Los principios y las características de la presente invención serán descritos a continuación con referencia a los dibujos adjuntos. La realización es solo para describir la presente invención y no tiene como objetivo limitar el alcance de la presente invención.

En primer término, se describirán las estructuras de la parte solicitante y la parte solicitada en el sistema que emplea el método para acceder a una comunicación de radiofrecuencia con comunicación magnética de baja frecuencia según la presente invención. La figura 1 es un diagrama de bloques de la estructura de la parte solicitante. Como se muestra en la figura 1, parte solicitante 100 comprende por lo menos un primer módulo de control 101, por lo menos un primer módulo de control de baja frecuencia 102, y por lo menos un primer módulo de comunicación magnética de baja frecuencia 103. El primer módulo de control 101 está por lo menos conectado a por lo menos por lo menos un primer módulo de comunicación de radiofrecuencia 102 y por lo menos un primer módulo de comunicación magnética de baja frecuencia 103. La figura 2 es un diagrama de bloques de la estructura de la parte solicitada. Como se muestra en la figura 2, parte

solicitada 200 comprende por lo menos un segundo módulo de control 201, por lo menos un segundo módulo de control de baja frecuencia 202, y por lo menos un segundo módulo de comunicación magnética de baja frecuencia 203. El segundo módulo de control 201 está conectado a por lo menos un segundo módulo de comunicación de radiofrecuencia 202 y por lo menos un segundo módulo de comunicación magnética de baja frecuencia 203. Por supuesto, en este documento solo se proporcionan estructuras representativas de la parte solicitante y la parte solicitada. En otras realizaciones, puede combinarse una pluralidad de módulos de la parte solicitante y la parte solicitada en un gran módulo, y alternativamente, un módulo puede dividirse en una pluralidad de módulos pequeños.

La figura 3 es un diagrama de flujo del método para el acceso a la comunicación de radiofrecuencia con comunicación magnética de baja frecuencia según una forma de realización de la presente invención. Como se muestra en la figura 3, en esta realización, el método para acceder a una comunicación de radiofrecuencia con comunicación magnética de baja frecuencia comprende los pasos siguientes:

Paso 301: la parte solicitante genera y envía una solicitud de activación, a saber, un código característico de baja frecuencia;
La solicitud de activación de este punto se envía a través de un canal de baja frecuencia; la solicitud de activación es, a saber, un código característico de baja frecuencia, en el que dicho código característico de baja frecuencia comprende un primer número aleatorio RN1 generado por la parte solicitante. Preferentemente, la longitud de dicho código característico de baja frecuencia es igual o menor de 2 bytes. De manera más preferente, para acelerar la velocidad de acceso, el código característico de baja frecuencia puede comprender solamente el primer número aleatorio RN1, y la longitud del primer número aleatorio RN1 es 1 byte. Ya que el código característico de baja frecuencia comprende un número aleatorio, y el número aleatorio cambia constantemente, puede garantizarse que el código característico de baja frecuencia es diferente en cada autenticación de acceso.
La parte solicitante mantiene el envío de la solicitud de activación, y cuando la parte solicitada ingresa el rango de acceso permitido, la parte solicitada comienza a responder.
Paso 302: la parte solicitada recibe la solicitud de activación;
La parte solicitada recibe la solicitud de activación a través del canal de baja frecuencia.
Paso 303: la parte solicitada genera y envía un mensaje de respuesta de activación;
La parte solicitada envía el mensaje de respuesta de activación en una primera dirección de comunicación de radiofrecuencia add1 a través del canal de radiofrecuencia, en el que el mensaje de respuesta de activación comprende un segundo número aleatorio RN2 generado por la parte solicitada y un identificador de identidad de la parte solicitada ID2.

Específicamente, el paso 303 puede comprender los subpasos siguientes:

Paso 31, la parte solicitada genera un segundo número aleatorio RN2;
Preferentemente, la longitud de dicho segundo número aleatorio RN2 puede ser 4 bytes.
Paso 32, la parte solicitada calcula la frecuencia de comunicación de radiofrecuencia según el método de cálculo de frecuencia predeterminado por las dos partes y basado en el primer número aleatorio RN1 en dicha solicitud de activación y el número máximo de puntos de frecuencia utilizados por el canal de radiofrecuencia;
Preferentemente, dicho método de cálculo de frecuencia es: con el número máximo de puntos de frecuencia utilizados por el canal de radiofrecuencia como el modo, realizando una operación para obtener un resto en dicho primer número aleatorio RN1, el resto obtenido corresponde a la numeración de la frecuencia utilizada por la comunicación de radiofrecuencia, y dicho frecuencia de la comunicación de radiofrecuencia es obtenida según dicha numeración.
Paso 33, la parte solicitante calcula la primera dirección de comunicación de radiofrecuencia add1 según el método de cálculo de dirección predeterminado por las dos partes y basado en el primer número aleatorio RN1;
Preferentemente, dicho método de cálculo de la primera dirección de comunicación de radiofrecuencia add1 es: con dicho primer número aleatorio RN1 como entrada, realizando una operación de función unidireccional predeterminada, y asignando todos o parte de los resultados operativos obtenidos como la primera dirección de comunicación de radiofrecuencia add1. Además, el algoritmo SHA-1 puede utilizarse como el método de cálculo para la primera dirección de comunicación de radiofrecuencia add1, y los primeros 5 bytes del resultado se toman como la primera dirección de comunicación de radiofrecuencia add1.
Paso 34, la parte solicitada genera un primer identificador de cifrado ALG1; dicho primer identificador de cifrado ALG1 contiene el método para cifrar las sesiones de transacción seleccionadas por la parte solicitada (es decir, independientemente de si se cifra o no) y el algoritmo de cifrado compatible;
Preferentemente, si ALG1 = 0, significa que no hay cifrado; si ALG1 ≠ 0, significa que se llevó a cabo el cifrado usando el algoritmo identificado por ALG1.
Paso 35, la parte solicitada utiliza dicho segundo número aleatorio RN2, el identificador de identidad de la parte solicitada ID2 y el primer identificador de cifrado ALG1 como la entrada de información de cifrado, utiliza dichos primer número aleatorio RN1 y segundo número aleatorio RN2 como la clave de cifrado, adopta un algoritmo de cifrado predeterminado para realizar la operación de cifrado, y toma los primeros 4 bytes del resultado del cifrado como el primer código de control MAC1;
Preferentemente, la entrada de cifrado es (RN2 | | ID2 | | ALG1), y la clave de cifrado es (RN1 | | RN2), en el que «|

|» representa una concatenación.

Paso 36, la parte solicitada genera un mensaje de respuesta de activación, dicho mensaje de respuesta de activación que comprende dicho segundo número aleatorio RN2, el identificador de identidad de la parte solicitada ID2, el primer identificador de cifrado ALG1 y el primer código de control MAC1;

Paso 37, la parte solicitada envía dicho mensaje de respuesta de activación en la primera dirección de comunicación de radiofrecuencia add1 a la frecuencia de comunicación de radiofrecuencia a través del canal de radiofrecuencia.

Paso 304: la parte solicitante recibe y verifica el mensaje de respuesta de activación;

La parte solicitante recibe el mensaje de respuesta de activación enviado por la parte solicitada en la primera dirección de comunicación de radiofrecuencia add1 a través del canal de radiofrecuencia, y realiza la verificación. Si pasa la verificación, entonces va al paso 305; de lo contrario, se termina este proceso de acceso.

Específicamente, el paso 304 puede comprender los subpasos siguientes:

Paso 41, la parte solicitante calcula la frecuencia de comunicación de radiofrecuencia según el método de cálculo de frecuencia predeterminado por las dos partes y basado en el primer número aleatorio RN1 y el número máximo de puntos de frecuencia utilizados por el canal de radiofrecuencia, en el que el método de cálculo de la frecuencia es el mismo que el método de cálculo de frecuencia en el paso 32;

Paso 42, la parte solicitante calcula la primera dirección de comunicación de radiofrecuencia add1 según el método de cálculo de dirección predeterminado por las dos partes y basado en el primer número aleatorio RN1;

Paso 43, la parte solicitante recibe dicho mensaje de respuesta de activación enviado por la parte solicitada en la primera dirección de comunicación de radiofrecuencia add1 a la frecuencia de comunicación de radiofrecuencia a través del canal de radiofrecuencia;

Paso 44, la parte solicitante utiliza el segundo número aleatorio RN2, el identificador de identidad de la parte solicitada ID2 y el primer identificador de cifrado ALG1 en dicho mensaje de respuesta de activación como la entrada de cifrado, utiliza dichos primer número aleatorio RN1 y segundo número aleatorio RN2 como la clave de cifrado, adopta un algoritmo predeterminado para realizar la operación de cifrado, toma los primeros 4 bytes del resultado del cifrado como el primer código de control MAC1, y después compara dicho primer código de control MAC1 con el primer código de control MAC1 contenido en dicho mensaje de respuesta de activación, si los dos son idénticos, entonces pasa la verificación, y va al paso 305; de lo contrario, el acceso es incorrecto y se termina este proceso de acceso;

Paso 305, la parte solicitante genera y envía una solicitud de conexión;

La parte solicitante envía la solicitud de conexión en la segunda dirección de comunicación de radiofrecuencia add2 a través del canal de radiofrecuencia, la solicitud de conexión que contiene un tercer número aleatorio RN3 generado por la parte solicitante.

Específicamente, el paso 305 puede comprender los subpasos siguientes:

Paso 51, la parte solicitante genera un tercer número aleatorio RN3;

Paso 52, la parte solicitante genera un segundo identificador de cifrado ALG2, dicho segundo identificador de cifrado ALG2 contiene el método para cifrar las sesiones de transacción seleccionadas por la parte solicitante y el algoritmo de cifrado compatible;

Preferentemente, los mismos métodos de cifrado y algoritmo se seleccionan para el segundo identificador de cifrado ALG2 en cuanto al primer identificador de cifrado ALG1. Si es imposible mantener los mismos, se seleccionarán un nuevo mismo método de cifrado y algoritmo. Si la parte solicitante está de acuerdo con la selección hecha del cifrado por la parte solicitada, entonces se establece ALG2=ALG1. En tal circunstancia, si ALG2=0, significa que la parte solicitante eligió de manera similar no cifrar; si ALG2≠0, significa que la parte solicitante eligió el mismo algoritmo que la parte solicitada para cifrar. Si la parte solicitante no está de acuerdo con la selección hecha del cifrado por la parte solicitada, entonces puede seleccionarse otro ALG2 (ALG2≠ALG1). En tal circunstancia, si ALG2=0, significa que la parte solicitante eligió no cifrar; si ALG2≠0, significa que la parte solicitante eligió el un algoritmo diferente del seleccionado por la parte solicitada para cifrar.

Paso 53, la parte solicitante utiliza dicho tercer número aleatorio RN3, el identificador de identidad de la parte solicitante ID1 y dicho segundo identificador de cifrado ALG2 como la entrada de información de cifrado, utiliza dichos primer número aleatorio RN1, segundo número aleatorio RN2 y tercer número aleatorio RN3 como la clave de cifrado, adopta un algoritmo de cifrado predeterminado para realizar la operación de cifrado, y toma los primeros 4 bytes del resultado del cifrado como el segundo código de control MAC2;

Preferentemente, la entrada de cifrado es (RN3 | | ID | | ALG2), y la clave de cifrado es (RN1 | | RN2 | |RN3), en el que «| |» representa una concatenación.

Paso 54, la parte solicitante genera una solicitud de conexión, dicha solicitud de conexión contiene dicho tercer número aleatorio RN3, el identificador de identidad de la parte solicitante ID1, el segundo identificador de cifrado ALG2 y el segundo código de control MAC2;

Paso 55, la parte solicitante calcula la segunda dirección de comunicación de radiofrecuencia add2 según el método de cálculo de dirección predeterminado por las dos partes y basado en el primer número aleatorio RN1 y el segundo número aleatorio RN2;

El método de cálculo de la segunda dirección de comunicación de radiofrecuencia add2 es: con dichos primer número aleatorio RN1 y segundo número aleatorio RN2 como entrada, realizando una operación de función unidireccional predeterminada, y asignando todos o parte de los resultados operativos obtenidos como la segunda dirección de comunicación de radiofrecuencia add2. Preferentemente, el algoritmo SHA-1 puede utilizarse como el método de cálculo para la segunda dirección de comunicación de radiofrecuencia add2, la entrada es (RN1 | | RN2), y los primeros 5 bytes del resultado se toman como la segunda dirección de comunicación de radiofrecuencia add2. Alternativamente, el método de cálculo de la segunda dirección de comunicación de radiofrecuencia add2 también puede ser: intersección de toda o una parte de (RN1 | | RN2) como la segunda dirección de comunicación de radiofrecuencia add2. Preferentemente, (RN1 | | RN2) es 5 bytes y se utiliza directamente como add2.

Paso 56, la parte solicitante envía dicha solicitud de conexión en la segunda dirección de comunicación de radiofrecuencia add2 a la frecuencia de comunicación de radiofrecuencia a través del canal de radiofrecuencia.

Paso 306: la parte solicitante recibe y verifica la solicitud de conexión;

La parte solicitada recibe la solicitud de conexión enviada por la parte solicitante en la segunda dirección de comunicación de radiofrecuencia add2 a través del canal de radiofrecuencia, y realiza la verificación; si pasa la verificación, entonces va al paso 307; de lo contrario, se termina este proceso de acceso.

Específicamente, el paso 306 puede comprender los subpasos siguientes:

Paso 61, la parte solicitada calcula la segunda dirección de comunicación de radiofrecuencia add2 según el método de cálculo de dirección predeterminado por las dos partes y basado en el primer número aleatorio RN1 y el segundo número aleatorio RN2; el método de cálculo en el paso 61 es el mismo que el método de cálculo de la dirección en el paso 55.

Paso 62, la parte solicitada recibe dicha solicitud de conexión en la segunda dirección de comunicación de radiofrecuencia add2 a la frecuencia de comunicación de radiofrecuencia a través del canal de radiofrecuencia;

Paso 63, la parte solicitada utiliza el tercer número aleatorio RN3, el identificador de identidad de la parte solicitante ID1 y dicho segundo identificador de cifrado ALG2 en dicha solicitud de conexión como la entrada de cifrado, utiliza dichos primer número aleatorio RN1, segundo número aleatorio RN2 y tercer número aleatorio RN3 como la clave de cifrado, adopta un algoritmo de cifrado predeterminado para realizar la operación de cifrado, toma los primeros 4 bytes del resultado del cifrado como el segundo código de control MAC2, y después compara dicho segundo código de control MAC2 con el segundo código de control MAC2 contenido en dicha solicitud de conexión; si los dos son idénticos, entonces pasa la verificación, de lo contrario, falla la verificación.

Paso 307, la parte solicitada genera y envía un mensaje de respuesta de conexión;

La parte solicitada envía dicho mensaje de respuesta de conexión en la segunda dirección de comunicación de radiofrecuencia add2 a través del canal de radiofrecuencia.

Específicamente, el paso 307 puede comprender los subpasos siguientes:

Paso 71, la parte solicitada fija un identificador de estado SFF de conexión exitosa/fallida según el resultado de verificación del segundo código de control MAC2. Si el segundo código de control MAC2 pasa la verificación, después dicho identificador de estado SFF de conexión exitosa/fallida se establece como conexión exitosa, y va al paso 72; de lo contrario, dicho identificador de estado SFF de la conexión exitosa/fallida se establece como conexión fallida, y va al paso 73;

Paso 72, la parte solicitada genera un tercer identificador de cifrado ALG3; dicho tercer identificador de cifrado ALG3 contiene el método para cifrar las sesiones de transacción finalmente seleccionadas por la parte solicitada y el algoritmo de cifrado compatible;

El tercer identificador de cifrado ALG3 puede ser el mismo o diferente del segundo identificador de cifrado ALG2 seleccionado por la parte solicitante en la solicitud de conexión. Si la parte solicitada está de acuerdo con la selección hecha del cifrado por la parte solicitante, entonces se establece ALG3=ALG2. En tal circunstancia, si ALG3=0, significa que la parte solicitada eligió finalmente no cifrar, tal como hizo la parte solicitante; si ALG3≠0, significa que la parte solicitada eligió finalmente el mismo algoritmo que el especificado por ALG2 seleccionado por la parte solicitante en la solicitud de conexión para el cifrado. Si la parte solicitada no está de acuerdo con la selección de cifrado hecha por la parte solicitante, entonces solo puede establecerse ALG3=0, lo cual significa que la parte solicitada eligió finalmente no cifrar. Por consiguiente, puede observarse que la estrategia, de la que la parte solicitada tiene la prioridad, es adoptada en el proceso de consulta del algoritmo de cifrado de sesión según la presente invención.

Paso 73, la parte solicitada utiliza el tercer número aleatorio RN3, el identificador de estado SFF de conexión exitosa/fallida y dicho tercer identificador de cifrado ALG3 como la entrada de información de cifrado, utiliza dichos

primer número aleatorio RN1, segundo número aleatorio RN2 y tercer número aleatorio RN3 como la clave de cifrado, adopta un algoritmo de cifrado predeterminado para realizar la operación de cifrado, y toma los primeros 4 bytes del resultado del cifrado como el tercer código de control MAC3;
Preferentemente, la entrada de cifrado es (RN3 | | SFF | | ALG3), y la clave de cifrado es (RN1 | | RN2 || RN3), en el que «| |» representa una concatenación.
Paso 74, la parte solicitada genera un mensaje de respuesta de conexión, dicho mensaje de respuesta de conexión contiene el identificador de estado SFF de la conexión exitosa/fallida, el tercer identificador de cifrado ALG3 y el tercer código de control MAC3;
Paso 75, la parte solicitada envía dicho mensaje de respuesta de conexión en la segunda dirección de comunicación de radiofrecuencia add2 a través del canal de radiofrecuencia.
Paso 308: la parte solicitante recibe y verifica el mensaje de respuesta de conexión;

La parte solicitante recibe el mensaje de respuesta de conexión en la segunda dirección de comunicación de radiofrecuencia add2 a través del canal de radiofrecuencia, y verifica si el acceso es exitoso, entonces va al paso 309; de lo contrario, se termina este proceso de acceso.

Específicamente, el paso 308 puede comprender los subpasos siguientes:

Paso 81, la parte solicitante recibe dicho mensaje de respuesta de conexión en la segunda dirección de comunicación de radiofrecuencia add2 a través del canal de radiofrecuencia;
Paso 82, la parte solicitante utiliza el tercer número aleatorio RN3, el identificador de estado SFF de la conexión exitosa/fallida y dicho tercer identificador de cifrado ALG3 en dicho mensaje de respuesta de conexión como la entrada de cifrado, utiliza dichos primer número aleatorio RN1, segundo número aleatorio RN2 y tercer número aleatorio RN3 como la clave de cifrado, adopta un algoritmo de cifrado predeterminado para realizar la operación de cifrado, toma los primeros 4 bytes del resultado del cifrado como el tercer código de control MAC3, y después compara dicho tercer código de control MAC3 con el tercer código de control MAC3 contenido en dicho mensaje de respuesta de conexión; si los dos son idénticos, entonces pasa la verificación, y va al paso 83; de lo contrario, falla la verificación y se termina este proceso de acceso;
Paso 83, la parte solicitante determina si el acceso por la parte solicitada es exitoso, o no, basado en el identificador de estado de la conexión exitosa/fallida en dicho mensaje de respuesta de conexión; si falla el acceso, después se termina este proceso de acceso; de lo contrario, va al paso 309.

En este punto, tanto la parte solicitante como la parte solicitada han completado una autenticación de acceso rápido y seguro y el proceso de consulta del algoritmo de cifrado y las claves de sesión, e ingresan al flujo de proceso de transacción subsiguiente.

Paso 309, se ingresa el flujo de transacción anticonflicto;

La parte solicitante y la parte solicitada realizan transacciones en la segunda dirección de comunicación de radiofrecuencia add2 a través del canal de radiofrecuencia. Si la sesión de transacción debe ser cifrada, los números aleatorios (RN1, RN2 y RN3) que las dos partes han intercambiado en la fase de autenticación de acceso pueden utilizarse para generar una clave de cifrado de sesión. Preferentemente, dicha clave de cifrado de sesión tiene 8 bytes (RN1 | | RN2 | | RN3) o 16 bytes (RN1 | | RN2 | | RN3 | | RN1 | | RN2 | | RN3), en la que (RN1 | | RN2 | | RN3) es la inversión bit por bit de (RN1 | | RN2 | | RN3).

Paso 310, se termina la transacción;

Paso 311, se desconecta la conexión y se sale.

Puede observarse de la descripción anterior que la presente invención no solo hace uso completo de las ventajas de la comunicación magnética de baja frecuencia en control del rango, sino también acelera la velocidad de acceso tanto como sea posible, así aumentando la velocidad de respuesta de toda la transacción, mejorando la satisfacción del usuario y asegurando la seguridad del acceso y la confidencialidad de la transmisión de datos de la sesión de la transacción.

REIVINDICACIONES

1. Un método para acceder a una comunicación de radiofrecuencia con comunicación magnética de baja frecuencia, por el que:

Paso a (301): una parte solicitante (100) envía una solicitud de activación a través de un canal de baja frecuencia, a saber un código característico de baja frecuencia, en el que dicho código característico de baja frecuencia comprende un primer número aleatorio generado por la parte solicitante, y la longitud de dicho código característico de baja frecuencia es igual o menor de 2 bytes;
Paso b (302, 303): una parte solicitada (200) recibe la solicitud de activación a través del canal de baja frecuencia, genera un mensaje de respuesta de activación y envía el mensaje de respuesta de activación en una primera dirección de comunicación de radiofrecuencia a través de un canal de radiofrecuencia, en el que el mensaje de respuesta de activación comprende un segundo número aleatorio generado por la parte solicitada y un identificador de identidad de la parte solicitada;
Paso c (304, 305): la parte solicitante (100) recibe el mensaje de respuesta de activación en la primera dirección de comunicación de radiofrecuencia a través del canal de radiofrecuencia y realiza la verificación, genera una solicitud de conexión si pasa la verificación, y envía la solicitud de conexión en una segunda dirección de comunicación de radiofrecuencia a través del canal de radiofrecuencia, en el que la solicitud de conexión comprende un tercer número aleatorio;
Paso d (306, 307): la parte solicitada (200) recibe la solicitud de conexión en la segunda dirección de comunicación de radiofrecuencia a través del canal de radiofrecuencia y realiza la verificación, genera un mensaje de respuesta de conexión si pasa la verificación, y envía el mensaje de respuesta de conexión en la segunda dirección de comunicación de radiofrecuencia a través del canal de radiofrecuencia;
Paso e (308): la parte solicitante (100) recibe el mensaje de respuesta de conexión en la segunda dirección de comunicación de radiofrecuencia a través del canal de radiofrecuencia, verifica si el acceso es exitoso, y negocia con la parte solicitada en la segunda dirección de comunicación de radiofrecuencia a través del canal de radiofrecuencia si el acceso es exitoso.

2. El método para acceder a una comunicación de radiofrecuencia con comunicación magnética de baja frecuencia como la presentada en la Reivindicación 1, **caracterizado porque** dicho código característico de baja frecuencia solo comprende dicho primer número aleatorio, y la longitud de dicho primer número aleatorio es 1 byte.

3. El método para acceder a una comunicación de radiofrecuencia con comunicación magnética de baja frecuencia como la presentada en la Reivindicación 1, **caracterizado porque** dicho paso b comprende:

Paso b1 (302), la parte solicitada (200) recibe la solicitud de activación a través del canal de baja frecuencia;
Paso b2(31), la parte solicitada (200) genera un segundo número aleatorio;
Paso b3(32), la parte solicitada (200) calcula la frecuencia de comunicación de radiofrecuencia según el método de cálculo de frecuencia predeterminado por las dos partes y basado en el primer número aleatorio en dicha solicitud de activación y el número máximo de puntos de frecuencia utilizados por el canal de radiofrecuencia;
Paso b4(33), la parte solicitada (200) calcula la primera dirección de comunicación de radiofrecuencia según el método de cálculo de dirección predeterminado por las dos partes y basado en el primer número aleatorio;
Paso b5(34), la parte solicitada (200) genera un primer identificador de cifrado, dicho primer identificador de cifrado contiene el método para cifrar las sesiones de transacción seleccionadas por la parte solicitada y el algoritmo de cifrado compatible;
Paso b6(35), la parte solicitada (200) utiliza dicho segundo número aleatorio, el identificador de identidad de la parte solicitada (200) y dicho primer identificador de cifrado como la entrada de información de cifrado, utiliza dichos primer número aleatorio y segundo número aleatorio como la clave de cifrado, adopta un algoritmo de cifrado predeterminado para realizar la operación de cifrado, y toma los primeros 4 bytes del resultado del cifrado como el primer código de control;
Paso b7(36), la parte solicitada (200) genera un mensaje de respuesta de activación, dicho mensaje de respuesta de activación que comprende dicho segundo número aleatorio, el identificador de identidad de la parte solicitada (200), el primer identificador de cifrado y el primer código de control;
Paso b8(37), la parte solicitada (200) envía dicho mensaje de respuesta de activación en la primera dirección de comunicación de radiofrecuencia en la frecuencia calculada de comunicación de radiofrecuencia a través del canal de radiofrecuencia.

4. El método para acceder a una comunicación de radiofrecuencia con comunicación magnética de baja frecuencia como la presentada en la Reivindicación 3, **caracterizado porque** en dicho paso b2(31), la longitud de dicho segundo número aleatorio es 4 bytes.

5. El método para acceder a una comunicación de radiofrecuencia con comunicación magnética de baja frecuencia como la presentada en la Reivindicación 3, **caracterizado porque** en dicho paso b3(32), dicho método de cálculo de frecuencia predeterminado es: con el número máximo de puntos de frecuencia utilizados por el canal de radiofrecuencia como el modo, realizando una operación para obtener un resto en dicho primer número aleatorio, el resto obtenido corresponde a

la numeración de la frecuencia utilizada por la comunicación de radiofrecuencia, y dicho frecuencia de la comunicación de radiofrecuencia es obtenida según dicha numeración.

6. El método para acceder a una comunicación de radiofrecuencia con comunicación magnética de baja frecuencia como la presentada en la Reivindicación 3, **caracterizado porque** en dicho paso b5(34), se indica que no hay cifrado cuando dicho primer identificador de cifrado es igual a 0, y se indica que hay cifrado y el cifrado es realizado con el algoritmo identificado por el primer identificador de cifrado cuando dicho primer identificador de cifrado no es igual a 0.

7. El método para acceder a una comunicación de radiofrecuencia con comunicación magnética de baja frecuencia como la presentada en la Reivindicación 3, **caracterizado porque** en dicho paso b6(35), la entrada de cifrado es (RN2 | | ID2 | | ALG1, y la clave de cifrado es (RN1 | | RN2, en la que «| |» representa una concatenación, RN1 es el primer número aleatorio, RN2 es el segundo número aleatorio, ID2 es el identificador de identidad de la parte solicitada y ALG1 es el primer identificador de cifrado.

8. El método para acceder a una comunicación de radiofrecuencia con comunicación magnética de baja frecuencia como la presentada en la Reivindicación 1, **caracterizado porque** dicho paso c comprende:

Paso c1 (41), la parte solicitante (100) calcula la frecuencia de comunicación de radiofrecuencia según el método de cálculo de frecuencia predeterminado por las dos partes y basado en el primer número aleatorio y el número máximo de puntos de frecuencia utilizados por el canal de radiofrecuencia;
Paso c2 (42), la parte solicitante (100) calcula la primera dirección de comunicación de radiofrecuencia según el método de cálculo de dirección predeterminado por las dos partes y basado en el primer número aleatorio;
Paso c3 (43), la parte solicitante (100) recibe dicho mensaje de respuesta de activación en la primera dirección de comunicación de radiofrecuencia en la frecuencia calculada de comunicación de radiofrecuencia a través del canal de radiofrecuencia.
Paso c4 (44), la parte solicitante (100) utiliza el segundo número aleatorio, el identificador de identidad de la parte solicitada (200) y dicho primer identificador de cifrado en dicho mensaje de respuesta de activación como la entrada de cifrado, utiliza dichos primer número aleatorio y segundo número aleatorio como la clave de cifrado, adopta un algoritmo predeterminado para realizar la operación de cifrado, toma los primeros 4 bytes del resultado del cifrado como el primer código de control, y después compara dicho primer código de control con el primer código de control contenido en dicho mensaje de respuesta de activación, si los dos son idénticos, entonces pasa la verificación, y va al paso c5 (51); de lo contrario, el acceso es incorrecto y se termina este proceso de acceso;
Paso c5(51), la parte solicitante genera un tercer número aleatorio;
Paso c6(52), la parte solicitante (100) genera un segundo identificador de cifrado, dicho segundo identificador de cifrado contiene el método para cifrar las sesiones de transacción seleccionadas por la parte solicitante y el algoritmo de cifrado compatible;
Paso c7 (53), la parte solicitante (100) utiliza dicho tercer número aleatorio, el identificador de identidad de la parte solicitante (100) y dicho segundo identificador de cifrado como la entrada de información de cifrado, utiliza dichos primer número aleatorio, segundo número aleatorio y tercer número aleatorio como la clave de cifrado, adopta un algoritmo de cifrado predeterminado para realizar la operación de cifrado, y toma los primeros 4 bytes del resultado del cifrado como el segundo código de control;
Paso c8 (54), la parte solicitante genera una solicitud de conexión, dicha solicitud de conexión contiene dicho tercer número aleatorio, el identificador de identidad de la parte solicitante (100), el segundo identificador de cifrado y el segundo código de control;
Paso c9 (55), la parte solicitante (100) calcula la segunda dirección de comunicación de radiofrecuencia según el método de cálculo de dirección predeterminado por las dos partes y basado en el primer número aleatorio y el segundo número aleatorio;
Paso c10 (56), la parte solicitante (100) envía dicha solicitud de conexión en la segunda dirección de comunicación de radiofrecuencia a la frecuencia de comunicación de radiofrecuencia a través del canal de radiofrecuencia.

9. El método para acceder a una comunicación de radiofrecuencia con comunicación magnética de baja frecuencia como la presentada en la Reivindicación 8, **caracterizado porque** en dicho paso c5 (51), la longitud de dicho tercer número aleatorio es 3 bytes.

10. El método para acceder a una comunicación de radiofrecuencia con comunicación magnética de baja frecuencia como la presentada en la Reivindicación 8, **caracterizado porque** en dicho paso c7 (53), la entrada de cifrado es (RN3 | | ID1 | | ALG2, y la clave de cifrado es RN1 | | RN2 | | RN3, en la que «| |» representa una concatenación, RN1 es el primer número aleatorio, RN2 es el segundo número aleatorio, RN3 es el tercer número aleatorio, ID1 es el identificador de identidad de la parte solicitante y ALG2 es el segundo identificador de cifrado.

11. El método para acceder a una comunicación de radiofrecuencia con comunicación magnética de baja frecuencia como la presentada en la Reivindicación 8, **caracterizado porque** en dicho paso c9 (55), dicho método de cálculo de la segunda dirección de comunicación de radiofrecuencia es: con dichos primer número aleatorio y segundo número aleatorio como entrada, realizando una operación de función unidireccional predeterminada, y asignado todos o parte de

los resultados operativos obtenidos como la segunda dirección de comunicación de radiofrecuencia.

12. El método para acceder a una comunicación de radiofrecuencia con comunicación magnética de baja frecuencia como la presentada en la Reivindicación 8, **caracterizado porque** en dicho paso c9 (55), dicho método de cálculo de la segunda dirección de comunicación de radiofrecuencia es: tomar toda o parte de RN1 | | RN2 como la segunda dirección de comunicación de radiofrecuencia, en el que «| |» representa una concatenación, RN1 es el primer número aleatorio RN2 es el segundo número aleatorio.

13. El método para acceder a una comunicación de radiofrecuencia con comunicación magnética de baja frecuencia como la presentada en la Reivindicación 1, **caracterizado porque** dicho paso d (306, 307) comprende:

Paso d1 (61), la parte solicitada (200) calcula la segunda dirección de comunicación de radiofrecuencia según el método de cálculo de dirección predeterminado por las dos partes y basado en el primer número aleatorio y el segundo número aleatorio;
Paso d2 (62), la parte solicitada (200) recibe dicha solicitud de conexión en la segunda dirección de comunicación de radiofrecuencia a la frecuencia de comunicación de radiofrecuencia a través del canal de radiofrecuencia;
Paso d3 (63), la parte solicitada (200) utiliza el tercer número aleatorio, el identificador de identidad de la parte solicitante (100) y dicho segundo identificador de cifrado en dicha solicitud de conexión como la entrada de cifrado, utiliza dichos primer número aleatorio, segundo número aleatorio y tercer número aleatorio como la clave de cifrado, adopta un algoritmo de cifrado predeterminado para realizar la operación de cifrado, toma los primeros 4 bytes del resultado del cifrado como el segundo código de control, y después compara dicho segundo código de control con el segundo código de control contenido en dicha solicitud de conexión; si los dos son idénticos, entonces pasa la verificación, de lo contrario, falla la verificación;
Paso d4 (71), la parte solicitada (200) establece un identificador de estado de conexión exitosa/fallida según el resultado de verificación del segundo código de control, si el segundo código de control pasa la verificación, después dicho identificador de estado de conexión exitosa/fallida se establece como conexión exitosa, y va al paso d5 (72); de lo contrario, dicho identificador de estado de la conexión exitosa/fallida se establece como conexión fallida, y va al paso d6 (73);
Paso d5 (72), la parte solicitada (200) genera un tercer identificador de cifrado, dicho tercer identificador de cifrado contiene el método para cifrar las sesiones de transacción finalmente seleccionadas por la parte solicitada y el algoritmo de cifrado compatible;
Paso d6 (73), la parte solicitada (200) utiliza el tercer número aleatorio, el identificador de estado de conexión exitosa/fallida y dicho tercer identificador de cifrado como la entrada de información de cifrado, utiliza dichos primer número aleatorio, segundo número aleatorio y tercer número aleatorio como la clave de cifrado, adopta un algoritmo de cifrado predeterminado para realizar la operación de cifrado, y toma los primeros 4 bytes del resultado del cifrado como el tercer código de control;
Paso d7 (74), la parte solicitada (200) genera un mensaje de respuesta de conexión, dicho mensaje de respuesta de conexión contiene el identificador de estado de la conexión exitosa/fallida, el tercer identificador de cifrado y el tercer código de control;
Paso d8 (75), la parte solicitada (200) envía dicho mensaje de respuesta de conexión en la segunda dirección de comunicación de radiofrecuencia a través del canal de radiofrecuencia.

14. El método para acceder a una comunicación de radiofrecuencia con comunicación magnética de baja frecuencia como la presentada en la Reivindicación 13, **caracterizado porque** en dicho paso d6 (73), la entrada de cifrado es (RN3 | | SFF | | ALG3, y la clave de cifrado es (RN1 | | RN2 | | RN3), en la que «| |» representa una concatenación, RN1 es el primer número aleatorio, RN2 es el segundo número aleatorio, RN3 es el tercer número aleatorio, SFF es el identificador de estado y ALG3 es el tercer identificador de cifrado.

15. El método para acceder a una comunicación de radiofrecuencia con comunicación magnética de baja frecuencia como la presentada en la Reivindicación 1, **caracterizado porque** dicho paso e (308) comprende:

Paso e1 (81), la parte solicitante (100) recibe dicho mensaje de respuesta de conexión en la segunda dirección de comunicación de radiofrecuencia a través del canal de radiofrecuencia;
Paso e2 (82), la parte solicitante (100) utiliza el tercer número aleatorio, el identificador de estado de la conexión exitosa/fallida y dicho tercer identificador de cifrado en dicho mensaje de respuesta de conexión como la entrada de cifrado, utiliza dichos primer número aleatorio, segundo número aleatorio y tercer número aleatorio como la clave de cifrado, adopta un algoritmo de cifrado predeterminado para realizar la operación de cifrado, toma los primeros 4 bytes del resultado del cifrado como el tercer código de control, y después compara dicho tercer código de control con el tercer código de control contenido en dicho mensaje de respuesta de conexión, si los dos son idénticos, entonces pasa la verificación, y va al paso e3 (83); de lo contrario, falla la verificación y se termina este proceso de acceso;
Paso e3 (83), la parte solicitante (100) determina si el acceso por la parte solicitada es exitoso, o no, basado en el identificador de estado de la conexión exitosa/fallida en dicho mensaje de respuesta de conexión, si falla el acceso, después se termina este proceso de acceso; de lo contrario, va al paso e4 (309).
Paso e4 (309), la parte solicitante (100) y la parte solicitada (200) realizan transacciones en la segunda dirección

de comunicación de radiofrecuencia a través del canal de radiofrecuencia.

16. El método para acceder a una comunicación de radiofrecuencia con comunicación magnética de baja frecuencia como la presentada en la Reivindicación 1, **caracterizado porque** en dicho paso e4 (309), una clave de cifrado de sesión se utiliza en dichas transacciones.

17. El método para acceder a una comunicación de radiofrecuencia con comunicación magnética de baja frecuencia como la presentada en la Reivindicación 16, **caracterizado porque** dicha clave de cifrado de sesión es 8 bytes RN1 | | RN2 | | RN3 o 16 bytes RN1 | | RN2 | | RN3 | | RN1 | | RN2 | | RN3, en la que «| |» representa una concatenación y RN1 | | RN2 | | RN3 es la inversión bit por bit de RN1 | | RN2 | | RN3, RN1 es el primer número aleatorio, RN2 es el segundo número aleatorio, RN3 es el tercer número aleatorio.

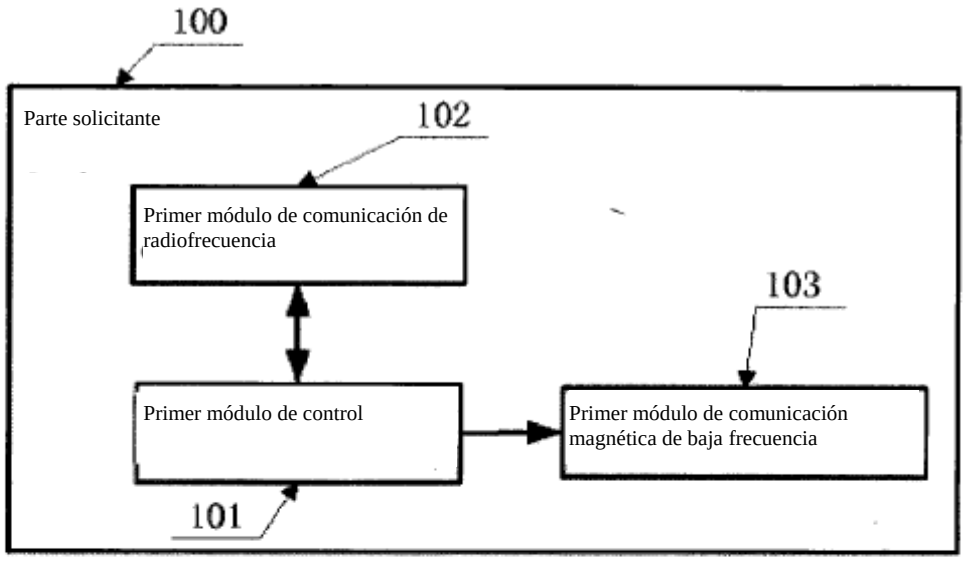

Figura 1

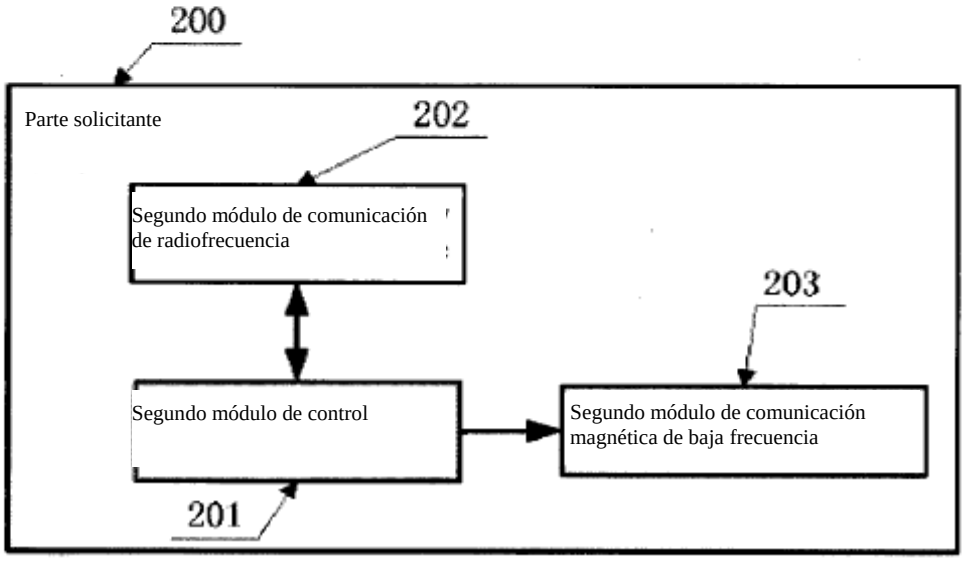

Figura 2

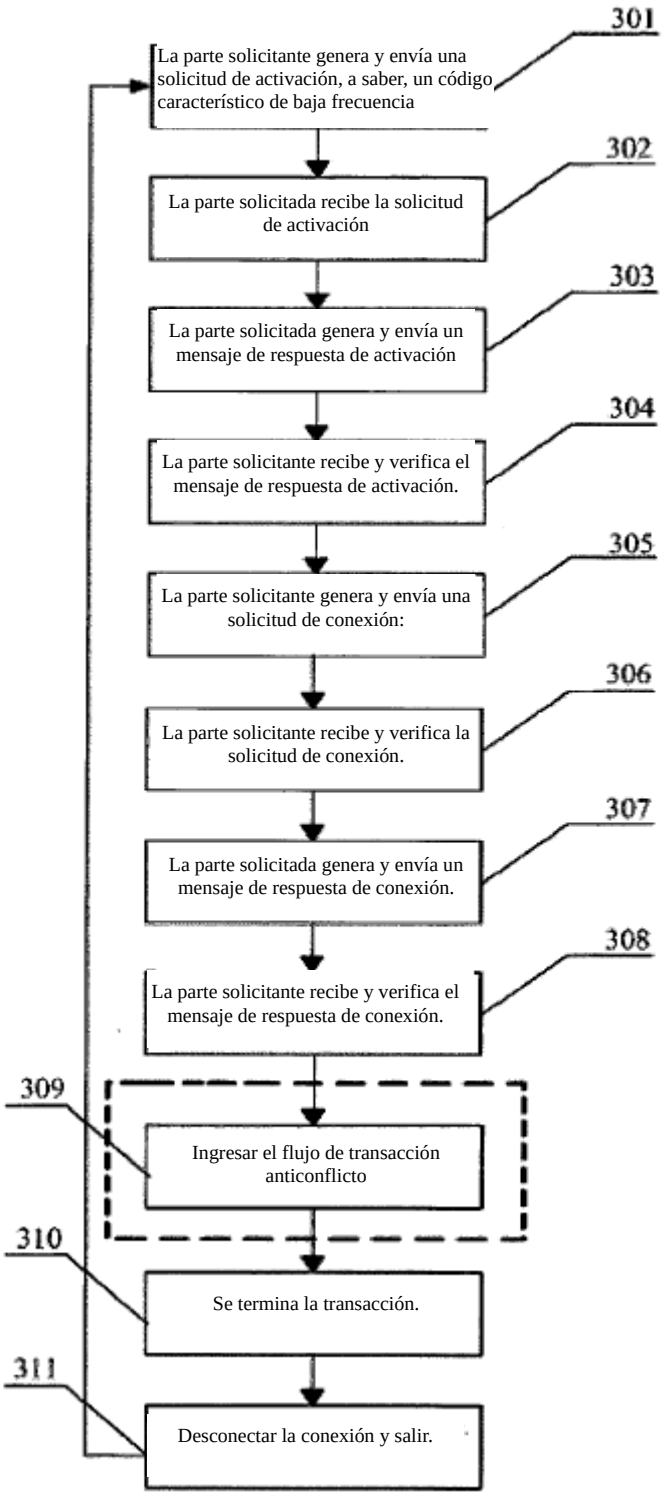
301
La parte solicitante genera y envía una solicitud de activación, a saber, un código característico de baja frecuencia
302
La parte solicitada recibe la solicitud de activación
303
La parte solicitada genera y envía un mensaje de respuesta de activación
304
La parte solicitante recibe y verifica el mensaje de respuesta de activación.
305
La parte solicitante genera y envía una solicitud de conexión:
306
La parte solicitante recibe y verifica la solicitud de conexión.
307
La parte solicitada genera y envía un mensaje de respuesta de conexión.
308
La parte solicitante recibe y verifica el mensaje de respuesta de conexión.
309
Ingresar el flujo de transacción anticonflicto
310
Se termina la transacción.
311
Desconectar la conexión y salir.

Figura 3