

19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 643 904**

51 Int. Cl.:

**H04W 4/00** (2009.01)

**G06F 21/35** (2013.01)

**H04W 12/08** (2009.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **19.06.2013 PCT/CN2013/077439**

87 Fecha y número de publicación internacional: **31.07.2014 WO14114047**

96 Fecha de presentación y número de la solicitud europea: **19.06.2013 E 13872468 (7)**

97 Fecha y número de publicación de la concesión europea: **06.09.2017 EP 2930857**

54 Título: **Método para llevar a cabo la selección de la unidad de seguridad en la comunicación de campo cercano y terminal móvil para aquella**

30 Prioridad:

**22.01.2013 CN 201310022697**

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

**27.11.2017**

73 Titular/es:

**HUAWEI DEVICE CO., LTD. (100.0%)  
Building B2 Huawei Industrial Base Bantian  
Longgang  
Shenzhen, Guangdong 518129, CN**

72 Inventor/es:

**JIN, ZHIHAO;  
WANG, MIAO;  
CHANG, XINMIAO y  
WU, HUANGWEI**

74 Agente/Representante:

**LEHMANN NOVO, María Isabel**

ES 2 643 904 T3

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

**DESCRIPCIÓN**

Método para llevar a cabo la selección de la unidad de seguridad en la comunicación de campo cercano y terminal móvil para aquella.

Campo técnico

5 La presente invención se refiere al campo de las tecnologías de las comunicaciones y, en particular, a un método, una terminal móvil y una máquina POS para implementar la selección de un elemento seguro en la comunicación de campo cercano.

Antecedentes

10 Actualmente, una tecnología NFC (Comunicación de Campo Cercano) se refiere a una tecnología que implementa la comunicación de corto alcance entre dispositivos electrónicos mediante el uso de un principio de inducción de campo magnético. Un usuario puede implementar el intercambio sin contacto de información o contenido, o una transacción entre dispositivos electrónicos colocando los dispositivos electrónicos de manera cercana entre sí. Una frecuencia de funcionamiento de la tecnología NFC es de 13,56 MHz, y un alcance efectivo para la comunicación es de 0-20 cm.

15 Con la popularización de la tecnología NFC, una función NFC también se encuentra disponible en una terminal móvil. Por ejemplo, como una aplicación de la tecnología NFC, el pago móvil se ha aplicado y desarrollado rápidamente. El usuario realiza el pago usando una terminal móvil con NFC habilitada (como, por ejemplo, un teléfono móvil) en combinación con una máquina POS (Punto de Venta) correspondiente.

20 En un estándar NCI (Interfaz de Controlador NFC, especificaciones de interfaz de controlador NFC) publicado por el foro NFC, se establece una tabla de encaminamiento SE (Elemento de Seguridad, elemento seguro). La tabla de encaminamiento SE permite la selección por defecto de un SE, en un caso en el cual se apaga un DH (Ordenador Principal del Dispositivo) de la terminal móvil, según la información básica de la comunicación NFC que se obtiene por un controlador NFC, por ejemplo, permite la selección por defecto de un SE según una AID (ID de Aplicación, ID de tipo) del SE, un protocolo de radiofrecuencia, y un tipo de tecnología NFC.

25 Sin embargo, cuando el DH se apaga, las características de la comunicación se encuentran limitadas. En una solución en la técnica anterior, el SE puede seleccionarse solamente usando las características de la comunicación NFC que se obtienen por el controlador NFC. Como resultado, existen algunos riesgos de seguridad cuando el SE seleccionado por el controlador NFC realiza el pago con una máquina POS correspondiente, lo cual provoca pérdidas para el usuario y también reduce la practicidad de la técnica anterior.

30 El documento "*NFC Controller Interface (NCI) Specification*" (6 de noviembre de 2012) de NFC Forum™ especifica un protocolo de comunicación llamado Interfaz de Controlador NFC (NCI, por sus siglas en inglés) entre un Controlador NFC (NFCC, por sus siglas en inglés) y un Ordenador Principal de Dispositivo (DH, por sus siglas en inglés).

35 El documento US2011/0130095 describe un método y sistema para manejar múltiples aplicaciones en un dispositivo de Comunicación de Campo Cercano (NFC). El método se lleva a cabo en un Controlador NFC (NFCC). El método incluye almacenar una identidad (ID) de ordenador principal fuente, una ID de ordenador principal destino, y una ID de enlace asociadas a cada aplicación de una o más aplicaciones. El método también incluye gestionar la única o más aplicaciones de manera simultánea según la ID de ordenador principal fuente, la ID de ordenador principal destino y la ID de enlace almacenadas en el NFCC.

40 Compendio

Las realizaciones de la presente invención proveen un método, una terminal móvil y una máquina POS para implementar la selección de un elemento seguro en la comunicación de campo cercano de modo que la terminal móvil selecciona un elemento seguro según una característica de entorno y completa la comunicación e interacción con la máquina POS.

45 Los aspectos de la presente invención se presentan en las reivindicaciones anexas.

Según un primer aspecto, se provee un método de configuración para implementar la selección de un elemento seguro en la comunicación de campo cercano, donde el método de configuración incluye:

50 recibir, por un controlador de comunicación de campo cercano en un extremo local, una primera instrucción de configuración enviada por un ordenador principal de dispositivo en el extremo local, donde la primera instrucción de configuración incluye una característica de entorno usada para seleccionar el elemento seguro;

configurar, por el controlador de comunicación de campo cercano, la característica de entorno en el controlador de comunicación de campo cercano según la primera instrucción de configuración;

recibir, por el controlador de comunicación de campo cercano, una segunda instrucción de configuración enviada por el ordenador principal de dispositivo; y

- 5 configurar, por el controlador de comunicación de campo cercano según la segunda instrucción de configuración, la característica de entorno en una instrucción de respuesta de atributo para comunicarse e interactuar con un extremo par, para continuar comunicándose e interactuando con el extremo par según la instrucción de respuesta de atributo configurada y además completar la selección del elemento seguro.

- 10 En una primera manera de implementación posible, después de la configuración, por el controlador de comunicación de campo cercano según la segunda instrucción de configuración, la característica de entorno en una instrucción de respuesta de atributo para comunicarse e interactuar con un extremo par, el método además incluye:

recibir, por el controlador de comunicación de campo cercano, una tabla de encaminamiento generada por el ordenador principal de dispositivo según la característica de entorno.

- 15 Con referencia al primer aspecto o a la primera manera de implementación posible del primer aspecto, en una segunda manera de implementación posible, la característica de entorno específicamente incluye un conjunto de uno o más de los siguientes atributos: un atributo de ubicación, un atributo de límite, un atributo de tiempo, y un atributo de máquina POS.

- 20 Con referencia al primer aspecto o a la segunda manera de implementación posible del primer aspecto, en una tercera manera de implementación posible, la característica de entorno incluye el atributo de límite y, antes de recibir, por un controlador de comunicación de campo cercano en un extremo local, una primera instrucción de configuración enviada por un ordenador principal de dispositivo en el extremo local, el método de configuración además incluye:

ordenar, por el ordenador principal de dispositivo, a un primer elemento seguro correspondiente al atributo de límite que separe un segundo elemento seguro del primer elemento seguro; y

- 25 recibir, por el controlador de comunicación de campo cercano, un comando de registro enviado por el segundo elemento seguro.

Según un segundo aspecto, se provee un método de interacción para implementar la selección de un elemento seguro en la comunicación de campo cercano, donde el método de interacción incluye:

- 30 recibir, por un controlador de comunicación de campo cercano, una instrucción de solicitud de atributo enviada por un extremo par, donde la instrucción de solicitud de atributo incluye una primera característica de entorno admitida por el extremo par;

- 35 enviar, por el controlador de comunicación de campo cercano según la instrucción de solicitud de atributo, una instrucción de respuesta de atributo al extremo par, donde la instrucción de respuesta de atributo incluye una segunda característica de entorno usada por el controlador de comunicación de campo cercano para seleccionar el elemento seguro;

recibir, por el controlador de comunicación de campo cercano, una instrucción de selección enviada por el extremo par, donde la instrucción de selección incluye un identificador de tipo del elemento seguro requerido por el extremo par; y

- 40 seleccionar, por el controlador de comunicación de campo cercano según la instrucción de selección, un elemento seguro correspondiente a la primera característica de entorno y al identificador de tipo, para completar la interacción con el extremo par.

En una primera manera de implementación posible, la selección, por el controlador de comunicación de campo cercano según la instrucción de selección, de un elemento seguro correspondiente a la primera característica de entorno y al identificador de tipo, específicamente incluye:

- 45 seleccionar, por el controlador de comunicación de campo cercano según una tabla de encaminamiento, el elemento seguro correspondiente a la primera característica de entorno y al identificador de tipo.

Según un tercer aspecto, se provee un método de interacción para implementar la selección de un elemento seguro en la comunicación de campo cercano, donde el método de interacción incluye:

- 50 enviar una primera instrucción de solicitud de atributo, donde la primera instrucción de solicitud de atributo incluye una primera característica de entorno admitida por un extremo local;

recibir una primera instrucción de respuesta de atributo, donde la primera instrucción de respuesta de atributo incluye una segunda característica de entorno usada por un extremo par para seleccionar el elemento seguro;

determinar si un conjunto de atributos de la primera característica de entorno incluye un conjunto de atributos de la segunda característica de entorno; y

- 5 enviar una instrucción de selección si el conjunto de atributos de la primera característica de entorno incluye el conjunto de atributos de la segunda característica de entorno, donde la instrucción de selección incluye un identificador de tipo de un elemento seguro requerido por el extremo local.

En una primera manera de implementación posible, determinar si un conjunto de atributos de la primera característica de entorno incluye un conjunto de atributos de la segunda característica de entorno además incluye:

- 10 obtener una tercera característica de entorno si el conjunto de atributos de la primera característica de entorno excluye el conjunto de atributos de la segunda característica de entorno, donde la tercera característica de entorno incluye un conjunto de atributos que se excluye de la primera característica de entorno y se incluye en la segunda característica de entorno; y

- 15 enviar una segunda instrucción de solicitud de atributo, donde la segunda instrucción de solicitud de atributo incluye la tercera característica de entorno.

Según un cuarto aspecto, se provee una terminal móvil para implementar la selección de un elemento seguro en la comunicación de campo cercano, donde la terminal móvil incluye:

- 20 una unidad de recepción, configurada para recibir una primera instrucción de configuración enviada por un ordenador principal de dispositivo en un extremo local, donde la primera instrucción de configuración incluye una característica de entorno usada para seleccionar el elemento seguro; y

una unidad de configuración, configurada para configurar la característica de entorno en un controlador de comunicación de campo cercano según la primera instrucción de configuración;

donde la unidad de recepción se configura además para recibir una segunda instrucción de configuración enviada por el ordenador principal de dispositivo; y

- 25 la unidad de configuración se configura además para: según la segunda instrucción de configuración, configurar la característica de entorno en una instrucción de respuesta de atributo para comunicarse e interactuar con un extremo par, para continuar comunicándose e interactuando con el extremo par según la instrucción de respuesta de atributo configurada y además completar la selección del elemento seguro.

- 30 En una primera manera de implementación posible, la unidad de recepción se configura además para recibir una tabla de encaminamiento generada por el ordenador principal de dispositivo según la característica de entorno.

Con referencia al cuarto aspecto o a la primera manera de implementación posible del cuarto aspecto, en una segunda manera de implementación posible, la característica de entorno recibida por la unidad de recepción específicamente incluye un conjunto de uno o más de los siguientes atributos: un atributo de ubicación, un atributo de límite, un atributo de tiempo, y un atributo de máquina POS.

- 35 Con referencia al cuarto aspecto o a la segunda manera de implementación posible del cuarto aspecto, en una tercera manera de implementación posible, cuando la característica de entorno incluye el atributo de límite y después el ordenador principal de dispositivo ordena a un primer elemento seguro correspondiente al atributo de límite que separe un segundo elemento seguro del primer elemento seguro,

- 40 la unidad de recepción se configura además para recibir un comando de registro enviado por el segundo elemento seguro.

Según un quinto aspecto, se provee una terminal móvil para implementar la selección de un elemento seguro en la comunicación de campo cercano, donde la terminal móvil incluye:

- 45 una unidad de recepción, configurada para recibir una instrucción de solicitud de atributo enviada por un extremo par, donde la instrucción de solicitud de atributo incluye una primera característica de entorno admitida por el extremo par;

una unidad de envío, configurada para: según la instrucción de solicitud de atributo, enviar una instrucción de respuesta de atributo al extremo par, donde la instrucción de respuesta de atributo incluye una segunda característica de entorno usada por la terminal móvil para seleccionar el elemento seguro;

la unidad de recepción, configurada además para recibir una instrucción de selección enviada por el extremo par, donde la instrucción de selección incluye un identificador de tipo del elemento seguro requerido por el extremo par; y

5 una unidad de selección, configurada para seleccionar, según la instrucción de selección, un elemento seguro correspondiente a la primera característica de entorno y al identificador de tipo, para completar la interacción con el extremo par.

En una primera manera de implementación posible, la unidad de selección se configura específicamente para seleccionar, según una tabla de encaminamiento, el elemento seguro correspondiente a la primera característica de entorno y al identificador de tipo.

10 Según un sexto aspecto, se provee una máquina POS para implementar la selección de un elemento seguro en la comunicación de campo cercano, donde la máquina POS incluye:

una unidad de envío, configurada para enviar una primera instrucción de solicitud de atributo, donde la primera instrucción de solicitud de atributo incluye una primera característica de entorno admitida por un extremo local;

15 una unidad de recepción, configurada para recibir una primera instrucción de respuesta de atributo, donde la primera instrucción de respuesta de atributo incluye una segunda característica de entorno usada por un extremo par para seleccionar el elemento seguro; y

una unidad de determinación, configurada para determinar si un conjunto de atributos de la primera característica de entorno incluye un conjunto de atributos de la segunda característica de entorno, donde

20 la unidad de envío se configura además para enviar una instrucción de selección si el conjunto de atributos de la primera característica de entorno incluye el conjunto de atributos de la segunda característica de entorno, donde la instrucción de selección incluye un identificador de tipo del elemento seguro requerido por un extremo local.

En una primera manera de implementación posible, la máquina POS además incluye:

25 una unidad de obtención, configurada para obtener una tercera característica de entorno si el conjunto de atributos de la primera característica de entorno excluye el conjunto de atributos de la segunda característica de entorno, donde la tercera característica de entorno incluye un conjunto de atributos que se excluye de la primera característica de entorno y se incluye en la segunda característica de entorno, donde

la unidad de envío se configura además para enviar una segunda instrucción de solicitud de atributo, donde la segunda instrucción de solicitud de atributo incluye la tercera característica de entorno.

30 Según un séptimo aspecto, se provee un sistema para implementar la selección de un elemento seguro en la comunicación de campo cercano, donde el sistema incluye la terminal móvil provista en el cuarto aspecto o el quinto aspecto de la realización de la presente invención y la máquina POS provista en el sexto aspecto de la realización de la presente invención.

Según un octavo aspecto, se provee una terminal móvil para implementar la selección de un elemento seguro en la comunicación de campo cercano, donde la terminal móvil incluye:

un controlador de comunicación de campo cercano y un ordenador principal de dispositivo, donde

35 el ordenador principal de dispositivo se configura para enviar una primera instrucción de configuración, donde la primera instrucción de configuración incluye una característica de entorno usada para seleccionar el elemento seguro;

el controlador de comunicación de campo cercano se configura para recibir la primera instrucción de configuración y configurar la característica de entorno según la primera instrucción de configuración;

40 el ordenador principal de dispositivo se configura además para enviar una segunda instrucción de configuración; y

45 el controlador de comunicación de campo cercano se configura además para recibir la segunda instrucción de configuración, y configurar, según la segunda instrucción de configuración, la característica de entorno en una instrucción de respuesta de atributo para comunicarse e interactuar con un extremo par, para continuar comunicándose e interactuando con el extremo par según la instrucción de respuesta de atributo configurada y además completar la selección del elemento seguro.

Por lo tanto, mediante la aplicación de un método, una terminal móvil y una máquina POS para implementar la selección de un elemento seguro en la comunicación de campo cercano, un controlador NFC en un extremo local recibe una instrucción de configuración enviada por un DH en el extremo local, donde la instrucción de configuración incluye una característica de entorno usada para seleccionar un SE; y configura la característica de entorno, la cual

se usa para seleccionar el SE, en una instrucción de respuesta de atributo para comunicarse e interactuar con un extremo par. Ello resuelve el problema en la solución de la técnica anterior de que un SE puede seleccionarse solamente usando las características de la comunicación NFC que se obtienen por el controlador NFC. Además, según el método anterior, cuando la comunicación e interacción se llevan a cabo con el extremo par posteriormente, el controlador NFC en el extremo local puede seleccionar un SE según una característica de entorno configurada independientemente de si el DH en el extremo local se enciende o apaga, y así mejorar la practicalidad de la técnica anterior.

Breve descripción de los dibujos

- 10 La Figura 1 es un diagrama de flujo de un método de configuración para implementar la selección de un elemento seguro en la comunicación de campo cercano según la Realización 1 de la presente invención;
- la Figura 2 es un diagrama de señalización de un método de configuración para implementar la selección de un elemento seguro en la comunicación de campo cercano según la Realización 2 de la presente invención;
- la Figura 3 es un diagrama de flujo de un método de interacción para implementar la selección de un elemento seguro en la comunicación de campo cercano según la Realización 3 de la presente invención;
- 15 la Figura 4 es un diagrama de flujo de un método de interacción para implementar la selección de un elemento seguro en la comunicación de campo cercano según la Realización 4 de la presente invención;
- la Figura 5 es un diagrama de señalización de un método de interacción para implementar la selección de un elemento seguro en la comunicación de campo cercano según la Realización 5 de la presente invención;
- 20 la Figura 6 es un diagrama estructural esquemático de una terminal móvil para implementar la selección de un elemento seguro en la comunicación de campo cercano según la Realización 6 de la presente invención;
- la Figura 7 es un diagrama estructural esquemático de una terminal móvil para implementar la selección de un elemento seguro en la comunicación de campo cercano según la Realización 7 de la presente invención;
- la Figura 8 es un diagrama estructural esquemático de una terminal móvil para implementar la selección de un elemento seguro en la comunicación de campo cercano según la Realización 8 de la presente invención;
- 25 la Figura 9 es un diagrama estructural esquemático de una terminal móvil para implementar la selección de un elemento seguro en la comunicación de campo cercano según la Realización 9 de la presente invención;
- la Figura 10 es un diagrama estructural esquemático de una máquina POS para implementar la selección de un elemento seguro en la comunicación de campo cercano según la Realización 10 de la presente invención;
- 30 la Figura 11 es un diagrama estructural esquemático de una máquina POS para implementar la selección de un elemento seguro en la comunicación de campo cercano según la Realización 11 de la presente invención; y
- la Figura 12 es un diagrama estructural esquemático de una terminal móvil para implementar la selección de un elemento seguro en la comunicación de campo cercano según la Realización 12 de la presente invención.

Descripción de las realizaciones

35 Con el fin de aclarar aún más los objetivos, las soluciones técnicas y las ventajas de la presente invención, a continuación se describen las realizaciones de la presente invención en detalle con referencia a los dibujos anexos.

Realización 1

40 Mediante el uso de la Figura 1 a modo de ejemplo, a continuación se describe un método de configuración para implementar la selección de un elemento seguro en la comunicación de campo cercano según una realización de la presente invención. La Figura 1 es un diagrama de flujo de un método de configuración para implementar la selección de un elemento seguro en la comunicación de campo cercano según la Realización 1 de la presente invención. Una entidad para implementar la realización que se muestra en la Figura 1 es un controlador NFC ubicado en una terminal móvil. Como se muestra en la Figura 1, la realización incluye las siguientes etapas:

45 Etapa 110: un controlador de comunicación de campo cercano en un extremo local recibe una primera instrucción de configuración enviada por un ordenador principal de dispositivo en el extremo local, donde la primera instrucción de configuración incluye una característica de entorno usada para seleccionar el elemento seguro.

De manera específica, en la realización de la presente invención, la terminal móvil funciona como el extremo local, y la terminal móvil incluye un DH, una NFC, y múltiples SE. Un proceso de configuración necesita llevarse a cabo cuando se enciende (o acciona) el DH en el extremo local. El DH en el extremo local envía la primera instrucción de

configuración al controlador NFC en el extremo local, donde la primera instrucción de configuración incluye la característica de entorno usada para seleccionar el elemento seguro; y el controlador NFC en el extremo local recibe la primera instrucción de configuración.

5 En la realización de la presente invención, la característica de entorno es una característica excepto las características de señal NFC como, por ejemplo, una forma de onda NFC y un formato de trama cuando la terminal móvil lleva a cabo la interacción NFC con una máquina POS.

Es a modo de ejemplo, pero sin limitación, que la primera instrucción de configuración puede ser específicamente una instrucción CORE\_SET\_CONFIG\_CMD.

10 Etapa 120: el controlador de comunicación de campo cercano configura la característica de entorno en el controlador de comunicación de campo cercano según la primera instrucción de configuración.

15 De manera específica, después de recibir la primera instrucción de configuración, el controlador NFC en el extremo local analiza la instrucción de configuración y extrae contenido transportado, es decir, la característica de entorno usada para seleccionar el SE. El controlador NFC en el extremo local configura la característica de entorno, la cual se usa para seleccionar el SE, en una ubicación de almacenamiento local especificada. En la realización de la presente invención, la característica de entorno es una base para que el controlador NFC en el extremo local seleccione un SE en un proceso de interacción subsiguiente.

Etapa 130: el controlador de comunicación de campo cercano recibe una segunda instrucción de configuración enviada por el ordenador principal de dispositivo.

20 De manera específica, después de establecer la característica de entorno usada para seleccionar un SE en la etapa 120, el controlador NFC en el extremo local recibe la segunda instrucción de configuración enviada por el DH en el extremo local.

Es a modo de ejemplo, pero sin limitación, que la segunda instrucción de configuración puede ser específicamente una instrucción CORE\_SET\_CONFIG\_CMD.

25 Etapa 140: según la segunda instrucción de configuración, el controlador de comunicación de campo cercano configura la característica de entorno en una instrucción de respuesta de atributo para comunicarse e interactuar con un extremo par, para continuar comunicándose e interactuando con el extremo par según la instrucción de respuesta de atributo configurada y además completar la selección del elemento seguro.

30 De manera específica, según la segunda instrucción de configuración, el controlador NFC en el extremo local configura la característica de entorno, la cual se usa para seleccionar un SE, en la instrucción de respuesta de atributo para comunicarse e interactuar con el extremo par. En la realización de la presente invención, en la etapa 130 y etapa 140, el controlador NFC en el extremo local configura la instrucción para comunicarse con el extremo par, de modo que la característica de entorno usada para seleccionar un SE se transporta cuando el controlador NFC en el extremo local se comunica con el extremo par posteriormente, y además la selección del SE se completa.

35 Por lo tanto, mediante la aplicación de un método de configuración para implementar la selección de un elemento seguro en la comunicación de campo cercano según una realización de la presente invención, un controlador NFC en un extremo local recibe una instrucción de configuración enviada por un DH en el extremo local, donde la instrucción de configuración incluye una característica de entorno usada para seleccionar un SE; y configura la característica de entorno, la cual se usa para seleccionar el SE, en una instrucción de respuesta de atributo para comunicarse e interactuar con un extremo par. Ello resuelve el problema en la solución de la técnica anterior de que un SE puede seleccionarse solamente usando las características de la comunicación NFC que se obtienen por el controlador NFC. Además, según el método anterior, cuando la comunicación e interacción se llevan a cabo con el extremo par posteriormente, el controlador NFC en el extremo local puede seleccionar un SE según una característica de entorno configurada independientemente de si el DH en el extremo local se enciende o apaga, y así mejorar la practicalidad de la técnica anterior.

45 Con el fin de aclarar aún más los objetivos, las soluciones técnicas y las ventajas de la presente invención, a continuación se describen las realizaciones específicas de la presente invención en mayor detalle con referencia a los dibujos anexos.

#### Realización 2

50 Mediante el uso de la Figura 2 a modo de ejemplo, a continuación se describe un método de configuración para implementar la selección de un elemento seguro en la comunicación de campo cercano según una realización de la presente invención. La Figura 2 es un diagrama de señalización de un método de configuración para implementar la selección de un elemento seguro en la comunicación de campo cercano según la Realización 2 de la presente invención. Como se muestra en la Figura 2, la realización incluye las siguientes etapas:

Etapa 210: un ordenador principal de dispositivo en un extremo local recibe información de características sobre el uso de un elemento seguro por un usuario, donde la información de características se ingresa por el usuario.

5 De manera específica, en la realización de la presente invención, un proceso de configuración necesita llevarse a cabo cuando se enciende el DH en el extremo local. Antes de que el DH en el extremo local reciba la información de características sobre el uso del elemento seguro por el usuario, donde la información de características se ingresa por el usuario, el usuario inicia una aplicación de pago en una terminal móvil, y el DH en el extremo local inicializa un controlador NFC en el extremo local para que entre en un estado operativo. Durante la inicialización, el DH en el extremo local obtiene una característica de entorno admitida por el controlador NFC en el extremo local.

10 Después de obtener la característica de entorno admitida por el controlador NFC en el extremo local, el DH en el extremo local muestra la característica de entorno admitida por el controlador NFC en el extremo local al usuario, y el usuario ingresa la información de características sobre el uso del SE por el usuario según la característica de entorno visualizada. El DH en el extremo local recibe la información de características sobre el uso del SE por el usuario que ingresa el usuario, donde la información de características sobre el uso del SE por el usuario incluye una característica de uso del SE, donde la característica se ingresa por el usuario.

15 La información de características sobre el uso del SE por el usuario específicamente incluye un conjunto de uno o más de los siguientes atributos: un atributo de ubicación, un atributo de límite, un atributo de tiempo, y un atributo de máquina POS.

20 En un ejemplo, la información de características sobre el uso del SE por el usuario es: el usuario preestablece que un primer SE (SE1) se usa cuando el usuario se encuentra en una ubicación A, y un límite de pago se impone cuando el DH en el extremo local se apaga; el usuario preestablece que un segundo SE (SE2) se usa cuando el usuario se encuentra en una ubicación B, y no se impone ningún límite de pago cuando el DH en el extremo local se apaga; el usuario preestablece que un tercer SE (SE3) se usa de lunes a viernes, y un límite de pago se impone cuando el DH en el extremo local se apaga; y el usuario preestablece que un cuarto SE (SE4) se usa el día sábado o domingo, y un límite de pago se impone cuando el DH en el extremo local se apaga. La información de características sobre el uso del SE por el usuario puede establecerse según las condiciones del usuario.

25 Etapa 220: cuando la información de características incluye un atributo de límite, el ordenador principal de dispositivo ordena a un primer elemento seguro correspondiente al atributo de límite que separe un segundo elemento seguro del primer elemento seguro.

30 De manera específica, cuando la información de características sobre el uso del SE por el usuario incluye el atributo de límite, el DH en el extremo local envía un comando de notificación al primer SE correspondiente al atributo de límite según la información de características sobre el uso del SE por el usuario, donde el comando de notificación se usa para ordenar al primer SE que separe del primer elemento seguro un segundo SE que preestablece el usuario para imponer un límite de pago.

35 Debe notarse que un propósito principal de las instrucciones, por el DH en el extremo local, al primer SE correspondiente al atributo de límite de que separe el segundo SE del primer SE es que se imponga un límite de pago cuando el DH en el extremo local se apaga, para proteger la terminal móvil del usuario del uso no restringido después de haber perdido la terminal móvil, y asegurar la seguridad de los datos de interacción de usuario.

Etapa 230: el primer elemento seguro separa el segundo elemento seguro del primer elemento seguro.

40 De manera específica, después de que el primer SE recibe el comando de notificación enviado por el DH en el extremo local, el primer SE separa el segundo SE del primer SE, y el primer SE y el segundo SE tienen un mismo identificador de tipo.

45 Además, la separación del segundo SE del primer SE se describe más abajo usando un ejemplo en el cual "el usuario preestablece que un primer SE (SE1) se usa cuando el usuario se encuentra en la ubicación A, y un límite de pago se impone cuando el DH en el extremo local se apaga". Si la información de características sobre el uso del SE por el usuario incluye el atributo de límite, después de determinar que la información de características sobre el uso del SE por el usuario incluye el atributo de límite, el DH en el extremo local envía un comando de notificación al SE1, donde el comando de notificación se usa para ordenar al SE1 que separe del SE1 un SE1' que preestablece el usuario para imponer un límite de pago. El SE1 separa el SE1' del SE1 según el comando de notificación. El SE1 y el SE1' tienen un mismo identificador de tipo. El SE1' se usa para imponer un límite de pago cuando el DH en el extremo local se apaga, lo cual puede proteger la terminal móvil del usuario del uso no restringido después de haber perdido la terminal móvil, y asegurar la seguridad de los datos de interacción de usuario.

50 Etapa 240: el segundo elemento seguro separado envía un comando de registro a un controlador de comunicación de campo cercano en el extremo local.

De manera específica, después de que el segundo SE se separa del primer SE, el segundo SE envía el comando de registro al controlador NFC en el extremo local. El controlador NFC en el extremo local recibe el comando de registro, donde el comando de registro se usa para ordenar al controlador NFC en el extremo local que reemplace el primer SE por el segundo SE en etapas subsiguientes y use el segundo SE como un SE correspondiente al atributo de límite.

5

Etapa 250: el controlador de comunicación de campo cercano en el extremo local recibe una primera instrucción de configuración enviada por el ordenador principal de dispositivo en el extremo local, donde la primera instrucción de configuración incluye una característica de entorno usada para seleccionar el elemento seguro.

10

De manera específica, después de implementar la etapa anterior, el DH en el extremo local envía la primera instrucción de configuración al controlador NFC en el extremo local, donde la primera instrucción de configuración incluye la característica de entorno usada para seleccionar el SE; y el controlador NFC en el extremo local recibe la primera instrucción de configuración.

15

En la realización de la presente invención, la característica de entorno es una característica excepto las características de señal NFC como, por ejemplo, una forma de onda NFC y un formato de trama cuando la terminal móvil lleva a cabo la interacción NFC con una máquina POS.

Es a modo de ejemplo, pero sin limitación, que la primera instrucción de configuración puede ser específicamente una instrucción CORE\_SET\_CONFIG\_CMD.

Etapa 260: el controlador de comunicación de campo cercano configura la característica de entorno en el controlador de comunicación de campo cercano según la primera instrucción de configuración.

20

De manera específica, después de recibir la primera instrucción de configuración, el controlador NFC en el extremo local analiza la instrucción de configuración y extrae el contenido transportado, es decir, la característica de entorno usada para seleccionar el SE. El controlador NFC en el extremo local configura la característica de entorno, la cual se usa para seleccionar el SE, en una ubicación de almacenamiento local especificada. En la realización de la presente invención, la característica de entorno es una base para que el controlador NFC en el extremo local seleccione un SE en un proceso de interacción subsiguiente.

25

Además, en la realización de la presente invención, la primera instrucción de configuración se extiende con un nuevo tipo de parámetro 0x84 (NFCC\_ENV\_STATE), donde el parámetro se usa para transportar una característica de entorno usada para seleccionar un SE, y el tipo de parámetro incluye un valor de 1 byte. Es a modo de ejemplo, pero sin limitación, que la Tabla 1 muestra una primera instrucción de configuración extendida.

30

Tabla 1 Primera instrucción de configuración

CORE_SET_CONFIG_CMD				
Campo	Longitud	Valor		
Número de parámetros	1 byte	n, que identifica el número de parámetros incluidos en el comando		
Parámetro [1...n]	3 bytes	Tipo de parámetro	1 byte	0x84
		Longitud de parámetro	1 byte	1
		Valor de parámetro	1 byte	Característica de entorno usada para seleccionar un SE

En la realización de la presente invención, el parámetro 0x84 transporta la característica de entorno usada para seleccionar un SE, donde la característica de entorno específicamente incluye un conjunto de uno o más de los siguientes atributos: un atributo de límite, un atributo de máquina POS, un atributo de tiempo, y un atributo de ubicación, y el parámetro 0x84 además transporta un atributo de apagado de DH y un atributo de apagado del extremo local, pero el atributo de apagado de DH y el atributo de apagado del extremo local ya se han establecido en la técnica anterior. Con referencia al contenido de la Tabla 1, el contenido específico del parámetro 0x84 es un

35

5 valor de una longitud de 1 byte. El controlador NFC en el extremo local configura el contenido específico del parámetro 0x84 en una ubicación de almacenamiento del controlador NFC en el extremo local. En la realización de la presente invención, el controlador NFC en el extremo local configura la característica de entorno, la cual se transporta en el parámetro 0x84 y se usa para seleccionar un SE, en un segundo byte de una característica del controlador NFC en el extremo local. Es a modo de ejemplo, pero sin limitación, que la Tabla 2 muestra una característica de entorno configurada por el controlador NFC y usada para seleccionar un SE.

Tabla 2 Característica de entorno configurada por el controlador NFC y usada para seleccionar un SE

Segundo byte de la característica del controlador NFC										Campo reservado
										Atributo de límite: establecido en 1 si el atributo se usa para seleccionar un elemento seguro
										Atributo de máquina POS: establecido en 1 si el atributo se usa para seleccionar un elemento seguro
										Atributo de tiempo: establecido en 1 si el atributo se usa para seleccionar un elemento seguro
										Atributo de ubicación: establecido en 1 si el atributo se usa para seleccionar un elemento seguro
										Apagado de DH de un extremo local: establecido en 1 si el atributo se admite
										Apagado: establecido en 1 si el atributo se admite

10 Con referencia al contenido de la Tabla 2, sobre la base de la técnica anterior que admite solo dos atributos, es decir, el atributo de apagado de DH y el atributo de apagado del extremo local, un conjunto de uno o más de cuatro atributos de características de entorno, es decir, el atributo de límite, un identificador POS, el atributo de tiempo, y el atributo de ubicación se añaden en la realización de la presente invención, y se usan como la característica de entorno usada para seleccionar un SE.

15 En un ejemplo, la característica de entorno usada para seleccionar un SE específicamente incluye el atributo de tiempo y el atributo de ubicación y, por lo tanto, los bits correspondientes del atributo de tiempo, atributo de ubicación, y atributo de apagado de DH y el atributo de apagado del extremo local se configuran en 1 para indicar la característica de entorno usada por el controlador NFC en el extremo local para seleccionar un SE.

Además, en la realización de la presente invención, cada uno del atributo de límite, identificador POS, atributo de tiempo, y atributo de ubicación, tiene tres derivaciones de selección por defecto.

20 En un ejemplo, el atributo de ubicación tiene tres derivaciones por defecto, es decir, tres tipos de condiciones para configurar tres ubicaciones diferentes A, B, C para el atributo de ubicación. En el presente caso, la característica usada por el controlador NFC para seleccionar el SE necesita extenderse con bytes para indicar las diferentes derivaciones.

25 Etapa 270: el controlador de comunicación de campo cercano recibe una segunda instrucción de configuración enviada por el ordenador principal de dispositivo.

De manera específica, después de establecer la característica de entorno usada para seleccionar el SE, el controlador NFC en el extremo local recibe la segunda instrucción de configuración enviada por el DH en el extremo local.

30 Es a modo de ejemplo, pero sin limitación, que la segunda instrucción de configuración puede ser específicamente una instrucción CORE\_SET\_CONFIG\_CMD.

Etapa 280: según la segunda instrucción de configuración, el controlador de comunicación de campo cercano configura la característica de entorno en una instrucción de respuesta de atributo para comunicarse e interactuar con un extremo par, para continuar comunicándose e interactuando con el extremo par según la instrucción de respuesta de atributo configurada y además completar la selección del elemento seguro.

5 De manera específica, según la segunda instrucción de configuración, el controlador NFC en el extremo local configura la característica de entorno, la cual se usa para seleccionar el SE, en la instrucción de respuesta de atributo para comunicarse e interactuar con el extremo par. En la realización de la presente invención, en la etapa 270 y etapa 280, el controlador NFC en el extremo local configura la instrucción para comunicarse con el extremo par, de modo que la característica de entorno usada para seleccionar el SE se transporta cuando el controlador NFC en el extremo local se comunica con el extremo par posteriormente, y además la selección del SE se completa.

10 Asimismo, en la realización de la presente invención, la segunda instrucción de configuración se extiende con un nuevo tipo de parámetro 0x5A, donde el parámetro se usa para transportar la característica de entorno usada por el controlador NFC en el extremo local para seleccionar un SE cuando la comunicación se lleva a cabo con el extremo par. El tipo de parámetro incluye un valor de 1 byte y se usa para indicar la característica de entorno usada por el controlador NFC en el extremo local para seleccionar un SE. Es a modo de ejemplo, pero sin limitación, que la Tabla 3 muestra una segunda instrucción de configuración extendida.

Tabla 3 Segunda instrucción de configuración

CORE_SET_CONFIG_CMD				
Campo	Longitud	Valor		
Número de parámetros	1 byte	n, que identifica el número de parámetros incluidos en el comando		
Parámetro er [1...n]	3 bytes	Tipo de parámetro	1 byte	0x5A
		Longitud de parámetro	1 byte	1
		Valor de parámetro	1 byte	Característica de entorno usada para seleccionar un SE.

15 Etapa 290: el controlador de comunicación de campo cercano recibe una tabla de encaminamiento enviada por el ordenador principal de dispositivo.

20 De manera específica, después de que el DH en el extremo local envía la segunda instrucción de configuración, el DH en el extremo local además genera una tabla de encaminamiento según la información de características sobre el uso del SE por el usuario. El controlador NFC en el extremo local recibe la tabla de encaminamiento, donde la tabla de encaminamiento se usa por el controlador NFC en el extremo local para seleccionar un SE según la tabla de encaminamiento en un proceso de interacción con el extremo par, donde el SE coincide con una característica de entorno admitida por el extremo par y un identificador de tipo incluido en una instrucción de selección enviada por el extremo par. Es a modo de ejemplo, pero sin limitación, que la Tabla 4 muestra una tabla de encaminamiento.

Tabla 4 Tabla de encaminamiento

1. Característica de entorno usada por el controlador NFC para seleccionar el SE									
	Apagado de DH de un extremo local	Encendido de DH de un extremo local	Apagado	Derivación de ubicación 1	Derivación de ubicación 2	Derivación de ubicación 3	Derivación de tiempo 1	Derivación de tiempo 2	Derivación de tiempo 3
2. Encaminamiento basado en AID									
AID 1	ENV	ENV	ENV	SE1'	SE2	Vacío	SE3'	SE4	Vacío

Con referencia a la Tabla 4, la tabla de encaminamiento que se muestra en la Tabla 4 muestra solamente una selección de ruta basada en AID. Según las condiciones reales, la selección de ruta basada en protocolo y la selección de ruta basada en el tipo de tecnología NFC pueden existir. La información correspondiente al apagado de DH del extremo local, encendido de DH del extremo local, y apagado es "ENV", que indica que la selección del SE se determina según una característica de entorno subsiguiente. Además, cuando el SE se selecciona según la característica de entorno, la selección puede llevarse a cabo después de llevar a cabo la determinación correspondiente según las condiciones y el número de derivaciones. Es a modo de ejemplo, pero sin limitación, que la Tabla 5 muestra una tabla de determinación de característica de entorno. La realización de la presente invención se describe usando un ejemplo en el cual cada uno del atributo de ubicación y atributo de tiempo que se muestran en la Tabla 4 tiene dos derivaciones.

Tabla 5 Tabla de determinación de característica de entorno

Atributo	Derivación	Operador para la determinación	Valor para la determinación
Ubicación	1	Igual a	Coordenadas de la ubicación A
Ubicación	2	Igual a	Coordenadas de la ubicación B
Tiempo	1	Menor que	6
Tiempo	2	Mayor que o igual a	6

Como se muestra en la Tabla 5, se determina a partir de la Tabla 4 que la característica de entorno usada por el controlador NFC en el extremo local para seleccionar un SE incluye el atributo de ubicación y el atributo de tiempo. Según el identificador de tipo en la instrucción de selección enviada por el extremo par, un registro correspondiente al identificador de tipo como, por ejemplo, un registro AID1, se selecciona de la tabla de encaminamiento. Según el registro AID1, se determina que el SE a seleccionarse se determina según la característica de entorno subsiguiente. Por lo tanto, el controlador NFC en el extremo local usa la característica de entorno admitida por el extremo par. En un ejemplo, la característica de entorno admitida por el extremo par incluye el atributo de ubicación y el atributo de tiempo, y el atributo de ubicación tiene valores de coordenadas definidos (x, y). Por lo tanto, el controlador NFC en el extremo local usa la Tabla 5 para determinar si los valores de coordenadas son iguales a las coordenadas de la ubicación A o a las coordenadas de la ubicación B. Si los valores de coordenadas son iguales a las coordenadas de la ubicación A, se determina que se selecciona la derivación de ubicación 1, y un SE correspondiente a la derivación de ubicación 1, que se selecciona con referencia a la Tabla 4, es SE1'. Después de seleccionar el SE1', el NFC en el extremo local obtiene datos de interacción en el SE1', y envía los datos de interacción al extremo par, para completar la interacción con el extremo par.

El controlador NFC en el extremo local recibe la tabla de encaminamiento enviada por el DH en el extremo local, y el controlador NFC en el extremo local selecciona el SE correspondiente según la tabla de encaminamiento recibida en el proceso de interacción con el extremo par.

Por lo tanto, mediante la aplicación de un método de configuración para implementar la selección de un elemento seguro en la comunicación de campo cercano según una realización de la presente invención, un controlador NFC en un extremo local recibe una instrucción de configuración enviada por un DH en el extremo local, donde la instrucción de configuración incluye una característica de entorno usada para seleccionar un SE; y configura la característica de entorno, la cual se usa para seleccionar el SE, en una instrucción de respuesta de atributo para comunicarse e interactuar con un extremo par. Ello resuelve el problema en la solución de la técnica anterior de que un SE puede seleccionarse solamente usando las características de la comunicación NFC que se obtienen por el controlador NFC. Además, según el método anterior, cuando la comunicación e interacción se llevan a cabo con el extremo par posteriormente, el controlador NFC en el extremo local puede seleccionar un SE según una característica de entorno configurada independientemente de si el DH en el extremo local se enciende o apaga, y así mejorar la practicalidad de la técnica anterior.

### Realización 3

Después de un proceso de configuración descrito en la Realización 2, se incluye además un proceso de interacción entre una terminal móvil y una máquina POS. El proceso de interacción provisto en la presente realización de la presente invención se basa en un proceso de configuración descrito en la Realización 1 anterior, y el proceso de interacción provisto en la presente realización de la presente invención es aplicable tanto a un caso en el cual un DH en un extremo local se enciende como a un caso en el cual el DH en el extremo local se apaga. Tanto en el caso en el cual el DH en el extremo local se enciende como el caso en el cual el DH en el extremo local se apaga, un

controlador NFC en el extremo local puede seleccionar un SE correspondiente según una tabla de encaminamiento, y así compensar las limitaciones de la solución en la técnica anterior y mejorar también la practicalidad de la técnica anterior. Como se muestra en la Figura 3, se incluyen las siguientes etapas.

5 En la realización de la presente invención, un método de interacción para implementar la selección de un elemento seguro en la comunicación de campo cercano se describe usando un ejemplo en el cual una terminal móvil funciona como un extremo local y una máquina POS funciona como un extremo par.

Etapas 310: un controlador de comunicación de campo cercano recibe una instrucción de solicitud de atributo enviada por el extremo par, donde la instrucción de solicitud de atributo incluye una primera característica de entorno admitida por el extremo par.

10 De manera específica, el controlador NFC en el extremo local recibe la instrucción de solicitud de atributo enviada por el extremo par, donde la instrucción de solicitud de atributo incluye la primera característica de entorno admitida por el controlador NFC en el extremo par.

Es a modo de ejemplo, pero sin limitación, que la instrucción de solicitud de atributo puede ser específicamente una instrucción ATTRBIT REQUEST.

15 Etapas 320: según la instrucción de solicitud de atributo, el controlador de comunicación de campo cercano envía una instrucción de respuesta de atributo al extremo par, donde la instrucción de respuesta de atributo incluye una segunda característica de entorno usada por el controlador de comunicación de campo cercano para seleccionar el elemento seguro.

20 De manera específica, después de recibir la instrucción de solicitud de atributo, el controlador NFC en el extremo local analiza la instrucción de solicitud de atributo y extrae la primera característica de entorno incluida en la instrucción, y descubre que el extremo par ha enviado la característica de entorno admitida. El controlador NFC en el extremo local envía la instrucción de respuesta de atributo al extremo par, donde la instrucción de respuesta de atributo incluye la segunda característica de entorno usada por el controlador NFC local para seleccionar el SE. En la realización de la presente invención, la instrucción de respuesta de atributo es la instrucción de respuesta de atributo que se configura por el controlador NFC en el extremo local en la Realización 1.

25 Es a modo de ejemplo, pero sin limitación, que la instrucción de respuesta de atributo puede ser específicamente una instrucción ATTRBIT RESPONSE.

30 Etapas 330: el controlador de comunicación de campo cercano recibe una instrucción de selección enviada por el extremo par, donde la instrucción de selección incluye un identificador de tipo de un elemento seguro requerido por el extremo par.

De manera específica, el controlador NFC en el extremo local recibe la instrucción de selección enviada por el extremo par, donde la instrucción de selección incluye el identificador de tipo del SE requerido por el extremo par.

35 Además, el identificador de tipo del SE es específicamente un identificador de tipo usado para distinguir los datos de interacción en el SE. Por ejemplo, un SE almacena datos de interacción relacionados con una tarjeta bancaria y, por lo tanto, el identificador de tipo del SE es D156000001ED/EP; y otro SE almacena datos de interacción relacionados con una tarjeta de transporte público y, por lo tanto, el identificador de tipo del SE es D1560XXXX0XGONGJIAO.

Es a modo de ejemplo, pero sin limitación, que la instrucción de selección puede ser específicamente una instrucción SELECT.

40 Etapas 340: el controlador de comunicación de campo cercano selecciona, según la instrucción de selección, un elemento seguro correspondiente a la primera característica de entorno y al identificador de tipo, para completar la interacción con el extremo par.

45 De manera específica, después de recibir la instrucción de selección, el controlador NFC en el extremo local analiza y extrae contenido transportado en la instrucción de selección, selecciona un SE correspondiente a la primera característica de entorno y al identificador de tipo de múltiples SE en el extremo local, y envía una instrucción de selección al SE seleccionado. Después de recibir la instrucción de selección, el SE seleccionado realimenta los datos de interacción almacenados en el SE seleccionado al controlador NFC en el extremo local. El controlador NFC en el extremo local obtiene los datos de interacción en el SE.

50 Después de obtener los datos de interacción en el SE seleccionado, la NFC en el extremo local envía los datos de interacción al controlador NFC en el extremo par. Después de recibir los datos de interacción, la NFC en el extremo par usa los datos de interacción para completar la interacción correspondiente.

Por lo tanto, mediante la aplicación de un método de interacción para implementar la selección de un elemento seguro en la comunicación de campo cercano según una realización de la presente invención, dado que un

controlador NFC en una terminal móvil ha completado la configuración correspondiente previamente, un problema en la solución de la técnica anterior se resuelve en la interacción subsiguiente con una máquina POS, donde el problema es que un SE puede seleccionarse solo usando características de comunicación NFC que se obtienen por el controlador NFC en la terminal móvil. Además, según el método anterior, cuando la comunicación e interacción se llevan a cabo con el extremo par posteriormente, el controlador NFC en la terminal móvil puede seleccionar un SE según una característica de entorno configurada independientemente de si el DH en la terminal móvil se enciende o apaga, y así mejorar la practicalidad de la técnica anterior.

#### Realización 4

En el proceso de interacción descrito en la realización previa, un método de interacción para implementar la selección de un elemento seguro en la comunicación de campo cercano se describe usando un ejemplo en el cual una terminal móvil funciona como un extremo local y una máquina POS funciona como un extremo par. En la presente realización de la presente invención, un método de interacción para implementar la selección de un elemento seguro en la comunicación de campo cercano se describe usando un controlador NFC en la máquina POS como una entidad de implementación. Como se muestra en la Figura 4, se incluyen las siguientes etapas.

En la realización de la presente invención, el método de interacción para implementar la selección de un elemento seguro en la comunicación de campo cercano se describe usando un ejemplo en el cual una máquina POS funciona como un extremo local y una terminal móvil funciona como un extremo par.

Etapas 410: enviar una primera instrucción de solicitud de atributo, donde la primera instrucción de solicitud de atributo incluye una primera característica de entorno admitida por el extremo local.

De manera específica, un controlador NFC en el extremo local envía la primera instrucción de solicitud de atributo al extremo par, donde la primera instrucción de solicitud de atributo incluye la primera característica de entorno admitida por el controlador NFC en el extremo local.

Es a modo de ejemplo, pero sin limitación, que la primera instrucción de solicitud de atributo puede ser específicamente una instrucción ATTRBIT REQUEST.

Etapas 420: recibir una primera instrucción de respuesta de atributo, donde la primera instrucción de respuesta de atributo incluye una segunda característica de entorno usada por el extremo par para seleccionar el elemento seguro.

De manera específica, después de recibir la primera instrucción de solicitud de atributo, el extremo par determina que el controlador NFC en el extremo local ha enviado la característica de entorno admitida. El extremo par envía la primera instrucción de respuesta de atributo al controlador NFC en el extremo local, donde la primera instrucción de respuesta de atributo incluye la segunda característica de entorno usada por el extremo par para seleccionar el SE.

Es a modo de ejemplo, pero sin limitación, que la primera instrucción de respuesta de atributo puede ser específicamente una instrucción ATTRBIT RESPONSE.

Etapas 430: determinar si un conjunto de atributos de la primera característica de entorno incluye un conjunto de atributos de la segunda característica de entorno.

De manera específica, después de recibir la primera instrucción de respuesta de atributo, el controlador NFC en el extremo local analiza la primera instrucción de respuesta de atributo y extrae la segunda característica de entorno transportada, y analiza la segunda característica de entorno y extrae contenido transportado, y el controlador NFC en el extremo local determina si el conjunto de atributos de la primera característica de entorno incluye el conjunto de atributos de la segunda característica de entorno.

Etapas 440: enviar una instrucción de selección si el conjunto de atributos de la primera característica de entorno incluye el conjunto de atributos de la segunda característica de entorno, donde la instrucción de selección incluye un identificador de tipo de un elemento seguro requerido por el extremo local.

De manera específica, el controlador NFC en el extremo local determina si el conjunto de atributos de la primera característica de entorno incluye el conjunto de atributos de la segunda característica de entorno. Si el conjunto de atributos de la primera característica de entorno incluye el conjunto de atributos de la segunda característica de entorno, el controlador NFC en el extremo local envía la instrucción de selección al extremo par, donde la instrucción de selección incluye el identificador de tipo del SE requerido por el controlador NFC en el extremo local, y el identificador de tipo del SE se usa por el extremo par para seleccionar un SE correspondiente a la primera característica de entorno y al identificador de tipo y obtener datos de interacción del SE, para completar un proceso de interacción con el controlador NFC en el extremo local.

En la realización de la presente invención, que el conjunto de atributos de la primera característica de entorno incluye el conjunto de atributos de la segunda característica de entorno es, específicamente, que el conjunto de atributos de la primera característica de entorno es mayor que o igual al conjunto de atributos de la segunda característica de entorno. Si el conjunto de atributos de la primera característica de entorno es mayor que o igual al conjunto de atributos de la segunda característica de entorno, el controlador NFC en el extremo local envía la instrucción de selección al extremo par.

Es a modo de ejemplo, pero sin limitación, que la instrucción de selección puede ser específicamente una instrucción SELECT.

Por lo tanto, mediante la aplicación de un método de interacción para implementar la selección de un elemento seguro en la comunicación de campo cercano según una realización de la presente invención, dado que un controlador NFC en una terminal móvil ha completado la configuración correspondiente previamente, el controlador NFC en la terminal móvil puede seleccionar un SE según la configuración correspondiente previa en un proceso de interacción entre un controlador NFC en una máquina POS y la terminal móvil, para completar la interacción subsiguiente. Además, según el método anterior, cuando la comunicación e interacción se llevan a cabo con el extremo par posteriormente, el controlador NFC en la terminal móvil puede seleccionar un SE según una característica de entorno configurada independientemente de si el DH en la terminal móvil se enciende o apaga, y así mejorar la practicalidad de la técnica anterior.

Realización 5

Con el fin de aclarar aún más los objetivos, las soluciones técnicas y las ventajas de la presente invención, a continuación se describen las realizaciones de la presente invención en detalle con referencia a los dibujos anexos.

Mediante el uso de la Figura 5 a modo de ejemplo, a continuación se describe un método de interacción para implementar la selección de un elemento seguro en la comunicación de campo cercano según una realización de la presente invención. La Figura 5 es un diagrama de señalización de un método de interacción para implementar la selección de un elemento seguro en la comunicación de campo cercano según la Realización 5 de la presente invención. La realización de la presente invención describe un proceso de interacción entre una terminal móvil y una máquina POS usando un ejemplo en el cual un DH en la terminal móvil se apaga. Como se muestra en la Figura 5, la terminal móvil y la máquina POS también forman un sistema para implementar la selección de un elemento seguro en la comunicación de campo cercano. La presente realización incluye las siguientes etapas:

Eta 501: un usuario coloca la terminal móvil cerca de la máquina POS.

De manera específica, el usuario espera llevar a cabo la comunicación e interacción con la máquina POS usando la terminal móvil, y el usuario coloca la terminal móvil cerca de la máquina POS.

Antes de que el usuario coloque la terminal móvil cerca de la máquina POS, un primer controlador NFC también lleva a cabo la configuración correspondiente de modo que el primer controlador NFC determina una característica de entorno admitida.

El primer controlador NFC recibe una instrucción de configuración enviada por un DH en la máquina POS, donde la instrucción de configuración incluye la característica de entorno admitida por el primer controlador NFC. El primer controlador NFC configura la característica de entorno en una instrucción de llevar a cabo la comunicación e interacción con un segundo controlador NFC.

Además, un formato de la instrucción de configuración en la realización de la presente invención es igual a un formato de la segunda instrucción de configuración que se muestra en la Tabla 3, pero los valores de parámetros en la instrucción de configuración usan los valores de atributos que se muestran en la Tabla 6. Los valores de atributos que se muestran en la Tabla 6 son a modo de ejemplo pero no se interpretan como una limitación.

Tabla 6 Valores de atributos

Tipo	Longitud	Valor de atributo
1 (representa un atributo de ubicación)	x bytes	Valores de coordenadas de ubicación (x, y)
2 (representa un atributo de tiempo)	x bytes	Valor de tiempo (hora; minuto)
3 (representa un atributo de máquina POS)	1 byte	Atributo de máquina POS

4 (representa un atributo de límite)	1 byte	Límite de interacción actual
--------------------------------------	--------	------------------------------

Etapa 502: un primer controlador NFC en la máquina POS descubre un segundo controlador NFC en la terminal móvil.

5 De manera específica, la máquina POS se encuentra en un estado encendido, el primer controlador NFC en la máquina POS transmite un campo de radiofrecuencia, y el usuario coloca la terminal móvil cerca de la máquina POS. Cuando está preparado para realizar un pago, el primer controlador NFC detecta que el segundo controlador NFC en la terminal móvil entra en un rango de campo de radiofrecuencia del primer controlador NFC. Cuando un DH en la terminal móvil se apaga, el campo de radiofrecuencia transmitido por el primer controlador NFC puede proveer energía eléctrica al segundo controlador NFC, de modo que la segunda NFC puede funcionar normalmente. La comunicación por radiofrecuencia se permite tanto en el primer controlador NFC como en el segundo controlador NFC.

Etapa 503: el primer controlador NFC envía una primera instrucción de solicitud de atributo al segundo controlador NFC, donde la primera instrucción de solicitud de atributo incluye una primera característica de entorno admitida por el primer controlador NFC.

15 De manera específica, dado que el campo de radiofrecuencia transmitido por el primer controlador NFC puede proveer energía eléctrica al segundo controlador NFC, el segundo controlador NFC puede funcionar normalmente. El primer controlador NFC envía la primera instrucción de solicitud de atributo al segundo controlador NFC, donde la primera instrucción de solicitud de atributo incluye la primera característica de entorno admitida por el primer controlador NFC.

20 La primera característica de entorno transporta una combinación de uno o más de los siguientes atributos: un atributo de ubicación, un atributo de límite, un atributo de tiempo, y un identificador de máquina POS. Por ejemplo, en la realización de la presente invención, la primera característica de entorno admitida por el primer controlador NFC es, específicamente, el atributo de ubicación y el atributo de tiempo. Además, el atributo de ubicación y el atributo de tiempo corresponden a valores de atributos específicos. Por ejemplo, el valor de atributo correspondiente al atributo de ubicación son valores de coordenadas (x, y) de la máquina POS, y el valor de atributo correspondiente al atributo de tiempo es el tiempo actual (horas y minutos específicos).

Es a modo de ejemplo, pero sin limitación, que la primera instrucción de solicitud de atributo puede ser específicamente una instrucción ATTRBIT REQUEST.

30 Etapa 504: el segundo controlador NFC envía una primera instrucción de respuesta de atributo al primer controlador NFC, donde la primera instrucción de respuesta de atributo incluye una segunda característica de entorno usada por el segundo controlador NFC para seleccionar el elemento seguro.

35 De manera específica, después de recibir la primera instrucción de solicitud de atributo, el segundo controlador NFC determina que el segundo controlador NFC ha enviado la característica de entorno admitida. El segundo controlador NFC envía la primera instrucción de respuesta de atributo al primer controlador NFC, donde la primera instrucción de respuesta de atributo incluye la segunda característica de entorno usada por el segundo controlador NFC para seleccionar el SE. En la realización de la presente invención, la primera instrucción de respuesta de atributo es la instrucción de respuesta de atributo que se configura por el segundo controlador NFC en la Realización 1.

40 La segunda característica de entorno transporta una combinación de uno o más de los siguientes atributos: el atributo de ubicación, el atributo de límite, el atributo de tiempo, y un atributo de máquina POS. Por ejemplo, en la realización de la presente invención, la segunda característica de entorno usada por el segundo controlador NFC para seleccionar el SE es el atributo de ubicación y el atributo de tiempo.

Es a modo de ejemplo, pero sin limitación, que la primera instrucción de respuesta de atributo puede ser específicamente una instrucción ATTRBIT RESPONSE.

45 Etapa 505: el segundo controlador NFC determina si un conjunto de atributos de la primera característica de entorno incluye un conjunto de atributos de la segunda característica de entorno.

50 De manera específica, después de recibir la primera instrucción de respuesta de atributo, el primer controlador NFC analiza la primera instrucción de respuesta de atributo y extrae la segunda característica de entorno transportada, y analiza la segunda característica de entorno y extrae contenido transportado, y el primer controlador NFC determina si el conjunto de atributos de la primera característica de entorno incluye el conjunto de atributos de la segunda característica de entorno.

Además, en la realización de la presente invención, que el conjunto de atributos de la primera característica de entorno incluye el conjunto de atributos de la segunda característica de entorno es, específicamente, que el conjunto

de atributos de la primera característica de entorno es mayor que o igual al conjunto de atributos de la segunda característica de entorno. Si el conjunto de atributos de la primera característica de entorno incluye el conjunto de atributos de la segunda característica de entorno, se lleva a cabo la etapa 506; de lo contrario, se lleva a cabo la etapa 511.

- 5 En un ejemplo, como se describe en el ejemplo previo, el conjunto de atributos de la primera característica de entorno es el atributo de ubicación y el atributo de tiempo, y el conjunto de atributos de la segunda característica de entorno es el atributo de ubicación y el atributo de tiempo. Por lo tanto, el primer controlador NFC determina que el conjunto de atributos de la primera característica de entorno incluye el conjunto de atributos de la segunda característica de entorno, y se lleva a cabo la etapa 506.
- 10 En otro ejemplo, el conjunto de atributos de la primera característica de entorno es el atributo de ubicación, el atributo de tiempo, y el atributo de límite, y el conjunto de atributos de la segunda característica de entorno es el atributo de ubicación y el atributo de tiempo. Por lo tanto, el primer controlador NFC determina que el conjunto de atributos de la primera característica de entorno incluye el conjunto de atributos de la segunda característica de entorno, y se lleva a cabo la etapa 506.
- 15 En otro ejemplo, el conjunto de atributos de la primera característica de entorno es el atributo de ubicación, y el conjunto de atributos de la segunda característica de entorno es el atributo de ubicación y el atributo de tiempo. Por lo tanto, el primer controlador NFC determina que el conjunto de atributos de la primera característica de entorno excluye (es decir, es menor que) el conjunto de atributos de la segunda característica de entorno, y se lleva a cabo la etapa 511.
- 20 Etapa 506: el primer controlador NFC envía una instrucción de selección si el conjunto de atributos de la primera característica de entorno incluye el conjunto de atributos de la segunda característica de entorno, donde la instrucción de selección incluye un identificador de tipo de un elemento seguro requerido por el primer controlador NFC.
- De manera específica, si el conjunto de atributos de la primera característica de entorno incluye el conjunto de atributos de la segunda característica de entorno, el primer controlador NFC envía la instrucción de selección al segundo controlador NFC, donde la instrucción de selección incluye el identificador de tipo del SE requerido por el primer controlador NFC, y se usa por el segundo controlador NFC para seleccionar un SE correspondiente a la primera característica de entorno y al identificador de tipo en una etapa subsiguiente.
- 25 El identificador de tipo del SE es específicamente un identificador de tipo usado para distinguir los datos de interacción en el SE. Por ejemplo, un SE almacena datos de interacción relacionados con una tarjeta bancaria y, por lo tanto, el identificador de tipo del SE es D156000001ED/EP; otro SE almacena datos de interacción relacionados con una tarjeta de transporte público y, por lo tanto, el identificador de tipo del SE es D1560XXXX0XGONGJIAO.
- Es a modo de ejemplo, pero sin limitación, que la instrucción de selección puede ser específicamente una instrucción SELECT.
- 30 Etapa 507: el segundo controlador NFC selecciona un elemento seguro correspondiente a la primera característica de entorno y al identificador de tipo según la instrucción de selección.
- De manera específica, después de recibir la instrucción de selección, el primer controlador NFC analiza y extrae contenido transportado en la instrucción de selección, y selecciona el SE correspondiente a la primera característica de entorno y al identificador de tipo de múltiples SE en un extremo local según una tabla de encaminamiento.
- 40 Etapa 508: el segundo controlador NFC obtiene datos de interacción del elemento seguro seleccionado.
- De manera específica, después de seleccionar el SE correspondiente a la primera característica de entorno y al identificador de tipo de los múltiples SE según la tabla de encaminamiento, el segundo controlador NFC envía una instrucción de selección al SE seleccionado. Después de recibir la instrucción de selección, el SE seleccionado realimenta los datos de interacción almacenados en el SE seleccionado al segundo controlador NFC. El segundo controlador NFC obtiene los datos de interacción en el SE.
- 45 Etapa 509: el segundo controlador NFC envía los datos de interacción obtenidos al primer controlador NFC.
- De manera específica, después de obtener los datos de interacción en el SE seleccionado, el segundo controlador NFC envía los datos de interacción al primer controlador NFC.
- Etapa 510: el primer controlador NFC completa la interacción según los datos de interacción.
- 50 De manera específica, después de recibir los datos de interacción, el primer controlador NFC completa la interacción correspondiente usando los datos de interacción.

Etapa 511: si el conjunto de atributos de la primera característica de entorno excluye el conjunto de atributos de la segunda característica de entorno, el primer controlador NFC obtiene una tercera característica de entorno, donde la tercera característica de entorno incluye un conjunto de atributos que no se incluye en la primera característica de entorno pero se incluye en la segunda característica de entorno.

- 5 De manera específica, si el conjunto de atributos de la primera característica de entorno excluye el conjunto de atributos de la segunda característica de entorno, el primer controlador NFC obtiene la tercera característica de entorno, donde la tercera característica de entorno incluye un conjunto de atributos que no se incluye de la primera característica de entorno pero se incluye en la segunda característica de entorno.

10 En un ejemplo, el conjunto de atributos de la primera característica de entorno es el atributo de ubicación, y el conjunto de atributos de la segunda característica de entorno es el atributo de ubicación y el atributo de tiempo. Por lo tanto, el primer controlador NFC determina que el conjunto de atributos de la primera característica de entorno excluye (es decir, es menor que) el conjunto de atributos de la segunda característica de entorno, y el primer controlador NFC obtiene contenido que no se incluye (es decir, el primer controlador NFC obtiene el atributo de tiempo).

- 15 El primer controlador NFC puede obtener el atributo de tiempo usando su propio sensor.

Etapa 512: el primer controlador NFC envía una segunda instrucción de solicitud de atributo, donde la segunda instrucción de solicitud de atributo incluye la tercera característica de entorno.

20 De manera específica, después de obtener el atributo de tiempo, el primer controlador NFC envía la segunda instrucción de solicitud de atributo al segundo controlador NFC. Según la segunda instrucción de solicitud de atributo, el segundo controlador NFC envía una segunda instrucción de respuesta de atributo al primer controlador NFC, donde la segunda instrucción de respuesta de atributo incluye la segunda característica de entorno usada por el segundo controlador NFC para seleccionar el SE. El primer controlador NFC determina si el conjunto de atributos de la primera característica de entorno y la tercera característica de entorno incluye el conjunto de atributos de la segunda característica de entorno.

- 25 Cuando el conjunto de atributos de la primera característica de entorno y la tercera característica de entorno incluye el conjunto de atributos de la segunda característica de entorno, el segundo controlador NFC recibe la instrucción de selección enviada por el primer controlador NFC.

30 Cuando el conjunto de atributos de la primera característica de entorno y la tercera característica de entorno excluye el conjunto de atributos de la segunda característica de entorno, el segundo controlador NFC aún recibe una instrucción de selección enviada por el primer controlador NFC.

Debe notarse que la Figura 5 no muestra la etapa 511 y la etapa 512.

35 Por lo tanto, mediante la aplicación de un método de interacción para implementar la selección de un elemento seguro en la comunicación de campo cercano según una realización de la presente invención, dado que un controlador NFC en una terminal móvil ha completado la configuración correspondiente previamente, un problema en la solución de la técnica anterior se resuelve en la interacción subsiguiente con una máquina POS, donde el problema es que un SE puede seleccionarse solo usando características de comunicación NFC que se obtienen por el controlador NFC en la terminal móvil, y existen algunos riesgos de seguridad cuando el SE seleccionado por el controlador NFC en la terminal móvil realiza un pago con la máquina POS correspondiente. Además, según el método anterior, cuando la comunicación e interacción se llevan a cabo con el extremo par posteriormente, el controlador NFC en la terminal móvil puede seleccionar un SE según una característica de entorno configurada independientemente de si un DH en la terminal móvil se enciende o apaga, y así mejorar la practicalidad de la técnica anterior.

#### Realización 6

45 Por consiguiente, la Realización 6 de la presente invención además provee una terminal móvil para implementar la selección de un elemento seguro en la comunicación de campo cercano para implementar el método en la realización anterior. Como se muestra en la Figura 6, la terminal móvil incluye una unidad de recepción 610 y una unidad de configuración 620.

50 La unidad de recepción 610 en el aparato se configura para recibir una primera instrucción de configuración enviada por un ordenador principal de dispositivo en un extremo local, donde la primera instrucción de configuración incluye una característica de entorno usada para seleccionar el elemento seguro.

La unidad de configuración 620 se configura para configurar la característica de entorno en un controlador de comunicación de campo cercano según la primera instrucción de configuración.

La unidad de recepción 610 se configura además para recibir una segunda instrucción de configuración enviada por el ordenador principal de dispositivo.

5 La unidad de configuración 620 se configura además para: según la segunda instrucción de configuración, configurar la característica de entorno en una instrucción de respuesta de atributo para comunicarse e interactuar con un extremo par, para continuar comunicándose e interactuando con el extremo par según la instrucción de respuesta de atributo configurada y además completar la selección del elemento seguro.

La unidad de recepción 610 se configura además para recibir una tabla de encaminamiento generada por el ordenador principal de dispositivo según la característica de entorno.

10 La unidad de recepción 610 y la unidad de configuración 620 se pueden usar para implementar el método descrito en la Realización 1. Para más detalles, es preciso remitirse a la descripción del método en la Realización 1, y los detalles no se describen nuevamente en la presente memoria descriptiva.

La característica de entorno recibida por la unidad de recepción 610 específicamente incluye un conjunto de uno o más de los siguientes atributos: un atributo de ubicación, un atributo de límite, un atributo de tiempo, y un atributo de máquina POS.

15 Cuando la característica de entorno incluye el atributo de límite, después de que el ordenador principal de dispositivo ordena a un primer elemento seguro correspondiente al atributo de límite que separe un segundo elemento seguro del primer elemento seguro,

la unidad de recepción 610 se configura además para recibir un comando de registro enviado por el segundo elemento seguro.

20 Por lo tanto, mediante la aplicación de una terminal móvil para implementar la selección de un elemento seguro en la comunicación de campo cercano según una realización de la presente invención, un controlador NFC en un extremo local recibe una instrucción de configuración enviada por un DH en el extremo local, donde la instrucción de configuración incluye una característica de entorno usada para seleccionar un SE; y configura la característica de entorno, la cual se usa para seleccionar el SE, en una instrucción de respuesta de atributo para comunicarse e interactuar con un extremo par. Ello resuelve el problema en la solución de la técnica anterior de que un SE puede seleccionarse solamente usando características de la comunicación NFC que se obtienen por el controlador NFC. Además, según el método anterior, cuando la comunicación e interacción se llevan a cabo con el extremo par posteriormente, el controlador NFC en el extremo local puede seleccionar un SE según una característica de entorno configurada independientemente de si el DH en el extremo local se enciende o apaga, y así mejorar la practicidad de la técnica anterior.

25

30

#### Realización 7

Además, una terminal móvil para implementar la selección de un elemento seguro en la comunicación de campo cercano según la Realización 7 de la presente invención puede implementarse también de la siguiente manera, para implementar el método en la realización anterior. Como se muestra en la Figura 7, la terminal móvil incluye una interfaz de red 710, un procesador 720 y una memoria 730. Un bus de sistema 740 se configura para conectar la interfaz de red 710, el procesador 720 y la memoria 730.

35

La interfaz de red 710 se configura para comunicarse con un controlador NFC en una máquina POS.

40 La memoria 730 puede ser una memoria permanente como, por ejemplo, una unidad de disco duro y una memoria flash, y la memoria 730 incluye un módulo de software y un controlador de dispositivos. El módulo de software puede ser cualquier tipo de módulo de función que pueda implementar el método anterior de la presente invención, y el controlador de dispositivos puede ser un controlador de red e interfaz.

Cuando se encienden, dichos componentes de software se cargan a la memoria 730, y luego se accede a ellos por el procesador 720 para ejecutar las siguientes instrucciones:

45 recibir una primera instrucción de configuración enviada por un ordenador principal de dispositivo en un extremo local, donde la primera instrucción de configuración incluye una característica de entorno usada para seleccionar el elemento seguro;

configurar la característica de entorno en sí misma según la primera instrucción de configuración;

recibir una segunda instrucción de configuración enviada por el ordenador principal de dispositivo; y

50 configurar, según la segunda instrucción de configuración, la característica de entorno en una instrucción de respuesta de atributo para comunicarse e interactuar con un extremo par, para continuar comunicándose e

interactuando con el extremo par según la instrucción de respuesta de atributo configurada y además completar la selección del elemento seguro.

5 La interfaz de red 710, el procesador 720, la memoria 730 y el bus de sistema 740 pueden usarse para implementar el método descrito en la Realización 1. Para más detalles, es preciso remitirse a la descripción del método en la Realización 1, y los detalles no se describen nuevamente en la presente memoria descriptiva.

Además, después de acceder a los componentes de software de la memoria 730, el procesador ejecuta instrucciones en el siguiente proceso:

recibir una tabla de encaminamiento generada por el ordenador principal de dispositivo según la característica de entorno.

10 Además, la característica de entorno específicamente incluye un conjunto de uno o más de los siguientes atributos: un atributo de ubicación, un atributo de límite, un atributo de tiempo, y un identificador de máquina POS.

Además, después de acceder a los componentes de software de la memoria 730, el procesador ejecuta instrucciones en el siguiente proceso:

15 ordenar, por el ordenador principal de dispositivo, a un primer elemento seguro correspondiente al atributo de límite que separe un segundo elemento seguro del primer elemento seguro; y

recibir un comando de registro enviado por el segundo elemento seguro.

20 Por lo tanto, mediante la aplicación de una terminal móvil de configuración para implementar la selección de un elemento seguro en la comunicación de campo cercano según una realización de la presente invención, un controlador NFC en un extremo local recibe una instrucción de configuración enviada por un DH en el extremo local, donde la instrucción de configuración incluye una característica de entorno usada para seleccionar un SE; y configura la característica de entorno, la cual se usa para seleccionar el SE, en una instrucción de respuesta de atributo para comunicarse e interactuar con un extremo par. Ello resuelve el problema en la solución de la técnica anterior de que un SE puede seleccionarse solamente usando características de la comunicación NFC que se obtienen por el controlador NFC. Además, según el método anterior, cuando la comunicación e interacción se llevan a cabo con el extremo par posteriormente, el controlador NFC en el extremo local puede seleccionar un SE según una característica de entorno configurada independientemente de si el DH en el extremo local se enciende o apaga, y así mejorar la practicalidad de la técnica anterior.

#### Realización 8

30 Por consiguiente, la Realización 8 de la presente invención además provee una terminal móvil para implementar la selección de un elemento seguro en la comunicación de campo cercano para implementar el método en la realización anterior. Como se muestra en la Figura 8, la terminal móvil incluye una unidad de recepción 810, una unidad de envío 820 y una unidad de selección 830.

35 La unidad de recepción 810 en la terminal móvil se configura para recibir una instrucción de solicitud de atributo enviada por un extremo par, donde la instrucción de solicitud de atributo incluye una primera característica de entorno admitida por el extremo par.

La unidad de envío 820 se configura para: según la instrucción de solicitud de atributo, enviar una instrucción de respuesta de atributo al extremo par, donde la instrucción de respuesta de atributo incluye una segunda característica de entorno usada por la terminal móvil para seleccionar el elemento seguro.

40 La unidad de recepción 810 se configura además para recibir una instrucción de selección enviada por el extremo par, donde la instrucción de selección incluye un identificador de tipo del elemento seguro requerido por el extremo par.

La unidad de selección 830 se configura para seleccionar, según la instrucción de selección, un elemento seguro correspondiente a la primera característica de entorno y al identificador de tipo, para completar la interacción con el extremo par.

45 La unidad de recepción 810, la unidad de envío 820 y la unidad de selección 830 se pueden usar para implementar el método descrito en la Realización 3. Para más detalles, es preciso remitirse a la descripción del método en la Realización 3, y los detalles no se describen nuevamente en la presente memoria descriptiva.

La unidad de selección 830 se configura específicamente para seleccionar, según una tabla de encaminamiento, el elemento seguro correspondiente a la primera característica de entorno y al identificador de tipo.

Por lo tanto, mediante la aplicación de una terminal móvil para implementar la selección de un elemento seguro en la comunicación de campo cercano según una realización de la presente invención, dado que un controlador NFC en la terminal móvil ha completado la configuración correspondiente previamente, un problema en la solución de la técnica anterior se resuelve en la interacción subsiguiente con una máquina POS, donde el problema es que un SE puede seleccionarse solo usando características de comunicación NFC que se obtienen por el controlador NFC en la terminal móvil. Además, según el método anterior, cuando la comunicación e interacción se llevan a cabo con el extremo par posteriormente, el controlador NFC en la terminal móvil puede seleccionar un SE según una característica de entorno configurada independientemente de si un DH en la terminal móvil se enciende o apaga, y así mejorar la practicalidad de la técnica anterior.

10 Realización 9

Además, la terminal móvil para implementar la selección de un elemento seguro en la comunicación de campo cercano según la Realización 8 de la presente invención puede implementarse también de la siguiente manera, para implementar el método en la realización anterior. Como se muestra en la Figura 9, la terminal móvil incluye una interfaz de red 910, un procesador 920 y una memoria 930. Un bus de sistema 940 se configura para conectar la interfaz de red 910, el procesador 920 y la memoria 930.

La interfaz de red 910 se configura para comunicarse con un controlador NFC en una máquina POS.

La memoria 930 puede ser una memoria permanente como, por ejemplo, una unidad de disco duro y una memoria flash, y la memoria 930 incluye un módulo de software y un controlador de dispositivos. El módulo de software puede ser cualquier tipo de módulo de función que pueda implementar el método anterior de la presente invención, y el controlador de dispositivos puede ser un controlador de red e interfaz.

Cuando se encienden, dichos componentes de software se cargan a la memoria 930, y luego se accede a ellos por el procesador 920 para ejecutar las siguientes instrucciones:

recibir una instrucción de solicitud de atributo enviada por un extremo par, donde la instrucción de solicitud de atributo incluye una primera característica de entorno admitida por el extremo par;

25 enviar, según la instrucción de solicitud de atributo, una instrucción de respuesta de atributo al extremo par, donde la instrucción de respuesta de atributo incluye una segunda característica de entorno usada por la terminal móvil para seleccionar el elemento seguro;

recibir una instrucción de selección enviada por el extremo par, donde la instrucción de selección incluye un identificador de tipo del elemento seguro requerido por el extremo par; y

30 seleccionar, según la instrucción de selección, un elemento seguro correspondiente a la primera característica de entorno y al identificador de tipo, para completar la interacción con el extremo par.

La interfaz de red 910, el procesador 920, la memoria 930 y el bus de sistema 940 pueden usarse para implementar el método descrito en la Realización 3. Para más detalles, es preciso remitirse a la descripción del método en la Realización 3, y los detalles no se describen nuevamente en la presente memoria descriptiva.

35 Además, después de acceder a los componentes de software de la memoria 930, el procesador ejecuta instrucciones en el siguiente proceso:

seleccionar, según una tabla de encaminamiento, el elemento seguro correspondiente a la primera característica de entorno y al identificador de tipo.

40 Por lo tanto, mediante la aplicación de una terminal móvil para implementar la selección de un elemento seguro en la comunicación de campo cercano según una realización de la presente invención, dado que un controlador NFC en la terminal móvil ha completado la configuración correspondiente previamente, un problema en la solución de la técnica anterior se resuelve en la interacción subsiguiente con una máquina POS, donde el problema es que un SE puede seleccionarse solo usando características de comunicación NFC que se obtienen por el controlador NFC en la terminal móvil. Además, según el método anterior, cuando la comunicación e interacción se llevan a cabo con el extremo par posteriormente, el controlador NFC en la terminal móvil puede seleccionar un SE según una característica de entorno configurada independientemente de si un DH en la terminal móvil se enciende o apaga, y así mejorar la practicalidad de la técnica anterior.

Realización 10

50 Por consiguiente, la Realización 10 de la presente invención además provee una máquina POS para implementar la selección de un elemento seguro en la comunicación de campo cercano para implementar el método en la realización anterior. Como se muestra en la Figura 10, la máquina POS incluye una unidad de envío 1010, una unidad de recepción 1020 y una unidad de determinación 1030.

La unidad de envío 1010 en la máquina POS se configura para enviar una primera instrucción de solicitud de atributo, donde la primera instrucción de solicitud de atributo incluye una primera característica de entorno admitida por un extremo local.

5 La unidad de recepción 1020 se configura para recibir una primera instrucción de respuesta de atributo, donde la primera instrucción de respuesta de atributo incluye una segunda característica de entorno usada por un extremo par para seleccionar el elemento seguro.

La unidad de determinación 1030 se configura para determinar si un conjunto de atributos de la primera característica de entorno incluye un conjunto de atributos de la segunda característica de entorno.

10 La unidad de envío 1010 se configura además para enviar una instrucción de selección si el conjunto de atributos de la primera característica de entorno incluye el conjunto de atributos de la segunda característica de entorno, donde la instrucción de selección incluye un identificador de tipo del elemento seguro requerido por la máquina POS.

La unidad de envío 1010, la unidad de recepción 1020 y la unidad de determinación 1030 pueden usarse para implementar el método descrito en la Realización 4. Para más detalles, es preciso remitirse a la descripción del método en la Realización 4, y los detalles no se describen nuevamente en la presente memoria descriptiva.

15 La máquina POS además incluye una unidad de obtención 1040, configurada para obtener una tercera característica de entorno si el conjunto de atributos de la primera característica de entorno excluye el conjunto de atributos de la segunda característica de entorno, donde la tercera característica de entorno incluye un conjunto de atributos que no se incluye en la primera característica de entorno y se incluye en la segunda característica de entorno.

20 La unidad de envío 1010 se configura además para enviar una segunda instrucción de solicitud de atributo, donde la segunda instrucción de solicitud de atributo incluye la tercera característica de entorno.

25 Por lo tanto, mediante la aplicación de una máquina POS para implementar la selección de un elemento seguro en la comunicación de campo cercano según una realización de la presente invención, dado que un controlador NFC en una terminal móvil ha completado la configuración correspondiente previamente, el controlador NFC en la terminal móvil puede seleccionar un SE según la configuración correspondiente previa en un proceso de interacción entre un controlador NFC en la máquina POS y la terminal móvil, para completar la interacción subsiguiente. Además, según el método anterior, cuando la comunicación e interacción se llevan a cabo con el extremo par posteriormente, el controlador NFC en la terminal móvil puede seleccionar un SE según una característica de entorno configurada independientemente de si un DH en la terminal móvil se enciende o apaga, y así mejorar la practicalidad de la técnica anterior.

30 Realización 11

Además, la máquina POS para implementar la selección de un elemento seguro en la comunicación de campo cercano según la Realización 10 de la presente invención puede implementarse también de la siguiente manera, para implementar el método en la realización anterior. Como se muestra en la Figura 11, la máquina POS incluye una interfaz de red 1110, un procesador 1120 y una memoria 1130. Un bus de sistema 1140 se configura para conectar la interfaz de red 1110, el procesador 1120 y la memoria 1130.

35 La interfaz de red 1110 se configura para comunicarse con un controlador NFC en una terminal móvil.

40 La memoria 1130 puede ser una memoria permanente como, por ejemplo, una unidad de disco duro y una memoria flash, y la memoria 1130 incluye un módulo de software y un controlador de dispositivos. El módulo de software puede ser cualquier tipo de módulo de función que pueda implementar el método anterior de la presente invención, y el controlador de dispositivos puede ser un controlador de red e interfaz.

Cuando se encienden, dichos componentes de software se cargan a la memoria 1130, y luego se accede a ellos por el procesador 1120 para ejecutar las siguientes instrucciones:

enviar una primera instrucción de solicitud de atributo, donde la primera instrucción de solicitud de atributo incluye una primera característica de entorno admitida por un extremo local;

45 recibir una primera instrucción de respuesta de atributo, donde la primera instrucción de respuesta de atributo incluye una segunda característica de entorno usada por un extremo par para seleccionar el elemento seguro;

determinar si un conjunto de atributos de la primera característica de entorno incluye un conjunto de atributos de la segunda característica de entorno; y

50 enviar una instrucción de selección si el conjunto de atributos de la primera característica de entorno incluye el conjunto de atributos de la segunda característica de entorno, donde la instrucción de selección incluye un identificador de tipo del elemento seguro requerido por la máquina POS.

La interfaz de red 1110, el procesador 1120, la memoria 1130 y el bus de sistema 1140 pueden usarse para implementar el método descrito en la Realización 4. Para más detalles, es preciso remitirse a la descripción del método en la Realización 4, y los detalles no se describen nuevamente en la presente memoria descriptiva.

5 Además, después de acceder a los componentes de software de la memoria 1130, el procesador ejecuta instrucciones en el siguiente proceso:

obtener una tercera característica de entorno si el conjunto de atributos de la primera característica de entorno excluye el conjunto de atributos de la segunda característica de entorno, donde la tercera característica de entorno incluye un conjunto de atributos que no se incluye en la primera característica de entorno y se incluye en la segunda característica de entorno; y

10 enviar una segunda instrucción de solicitud de atributo, donde la segunda instrucción de solicitud de atributo incluye la tercera característica de entorno.

Por lo tanto, mediante la aplicación de una máquina POS para implementar la selección de un elemento seguro en la comunicación de campo cercano según una realización de la presente invención, dado que un controlador NFC en una terminal móvil ha completado la configuración correspondiente previamente, el controlador NFC en la terminal móvil puede seleccionar un SE según la configuración correspondiente previa en un proceso de interacción entre un controlador NFC en la máquina POS y la terminal móvil, para completar la interacción subsiguiente. Además, según el método anterior, cuando la comunicación e interacción se llevan a cabo con el extremo par posteriormente, el controlador NFC en la terminal móvil puede seleccionar un SE según una característica de entorno configurada independientemente de si un DH en la terminal móvil se enciende o apaga, y así mejorar la practicalidad de la técnica anterior.

#### Realización 12

25 Además, la terminal móvil para implementar la selección de un elemento seguro en la comunicación de campo cercano según la Realización 7 de la presente invención puede implementarse también de la siguiente manera, para implementar el método en la realización anterior. Como se muestra en la Figura 12, la terminal móvil incluye un controlador de comunicación de campo cercano 1210 y un ordenador principal de dispositivo 1220.

El ordenador principal de dispositivo 1220 se configura para enviar una primera instrucción de configuración, donde la primera instrucción de configuración incluye una característica de entorno usada para seleccionar el elemento seguro.

30 El controlador de comunicación de campo cercano 1210 se configura para recibir la primera instrucción de configuración y configurar la característica de entorno según la primera instrucción de configuración.

El ordenador principal de dispositivo 1220 se configura además para enviar una segunda instrucción de configuración.

35 El controlador de comunicación de campo cercano 1210 se configura además para recibir la segunda instrucción de configuración, y configurar, según la segunda instrucción de configuración, la característica de entorno en una instrucción de respuesta de atributo para comunicarse e interactuar con un extremo par, para continuar comunicándose e interactuando con el extremo par según la instrucción de respuesta de atributo configurada y además completar la selección del elemento seguro.

40 El controlador de comunicación de campo cercano 1210 y el ordenador principal de dispositivo 1220 pueden usarse para implementar el método descrito en la Realización 1. Para más detalles, es preciso remitirse a la descripción del método en la Realización 1, y los detalles no se describen nuevamente en la presente memoria descriptiva. Por lo tanto, mediante la aplicación de una terminal móvil para implementar la selección de un elemento seguro en la comunicación de campo cercano según una realización de la presente invención, un controlador NFC en un extremo local recibe una instrucción de configuración enviada por un DH en el extremo local, donde la instrucción de configuración incluye una característica de entorno usada para seleccionar un SE; y configura la característica de entorno, la cual se usa para seleccionar el SE, en una instrucción de respuesta de atributo para comunicarse e interactuar con un extremo par. Ello resuelve el problema en la solución de la técnica anterior de que un SE puede seleccionarse solamente usando características de la comunicación NFC que se obtienen por el controlador NFC. Además, según el método anterior, cuando la comunicación e interacción se llevan a cabo con el extremo par posteriormente, el controlador NFC en el extremo local puede seleccionar un SE según una característica de entorno configurada independientemente de si el DH en el extremo local se enciende o apaga, y así mejorar la practicalidad de la técnica anterior.

Una persona con experiencia en la técnica puede darse cuenta además de que, en combinación con los ejemplos descritos en las realizaciones descritas en la presente memoria descriptiva, las etapas de las unidades y algoritmos pueden implementarse por hardware electrónico, software de ordenador o una combinación de ellos. Con el fin de

5 describir, de manera clara, la intercambiabilidad entre hardware y software, lo anterior ha descrito, de forma general, las etapas y composiciones de cada ejemplo según las funciones. Si las funciones se llevan a cabo por hardware o software depende de las aplicaciones particulares y de las condiciones de limitaciones de diseño de las soluciones técnicas. Una persona con experiencia en la técnica puede usar diferentes métodos para implementar las funciones descritas para cada aplicación particular, pero no se considerará que la implementación va más allá del alcance de la presente invención.

10 Las etapas de los métodos o algoritmos descritas en las realizaciones descritas en la presente memoria descriptiva pueden implementarse mediante hardware, un módulo de software ejecutado por un procesador, o una combinación de ellos. El módulo de software puede residir en una memoria de acceso aleatorio (RAM, por sus siglas en inglés), una memoria, una memoria de solo lectura (ROM, por sus siglas en inglés), una ROM programable eléctricamente, una ROM eléctricamente programable y borrrable, un registro, un disco duro, un disco extraíble, un CD-ROM, o cualquier otra forma de medio de almacenamiento conocida en la técnica.

15 En las anteriores maneras de implementación específicas, el objetivo, las soluciones técnicas y los beneficios de la presente invención se describen en detalle. Debe comprenderse que las anteriores descripciones son meramente maneras específicas de implementación de la presente invención, pero no pretenden limitar el alcance de protección de la presente invención.

**REIVINDICACIONES**

1. Un método de configuración para implementar la selección de un elemento seguro en la comunicación de campo cercano, en donde el método de configuración comprende:
- 5 recibir (110, 250), por un controlador de comunicación de campo cercano ubicado en una terminal móvil en un extremo local, una primera instrucción de configuración enviada por un ordenador principal de dispositivo en el extremo local, en donde la primera instrucción de configuración comprende una característica de entorno usada para seleccionar el elemento seguro;
- configurar (120, 260), por el controlador de comunicación de campo cercano, la característica de entorno en el controlador de comunicación de campo cercano según la primera instrucción de configuración; y,
- 10 recibir (130, 270), por el controlador de comunicación de campo cercano, una segunda instrucción de configuración enviada por el ordenador principal de dispositivo, caracterizado por que el método además comprende:
- configurar (140, 280), por el controlador de comunicación de campo cercano según la segunda instrucción de configuración, la característica de entorno en una instrucción de respuesta de atributo para comunicarse e interactuar con un extremo par, para continuar comunicándose e interactuando con el extremo par según la
- 15 instrucción de respuesta de atributo configurada y además completar la selección del elemento seguro; y,
- seleccionar, por el controlador de comunicación de campo cercano, un elemento seguro según la característica de entorno configurada para la subsiguiente comunicación e interacción con el extremo par.
2. El método de configuración según la reivindicación 1, en donde después de la configuración (140), por el controlador de comunicación de campo cercano según la segunda instrucción de configuración, la característica de
- 20 entorno en una instrucción de respuesta de atributo para comunicarse e interactuar con un extremo par, el método además comprende:
- recibir (290), por el controlador de comunicación de campo cercano, una tabla de encaminamiento generada por el ordenador principal de dispositivo según la característica de entorno.
3. El método de configuración según la reivindicación 1 o 2, en donde:
- 25 la característica de entorno específicamente comprende un conjunto de uno o más de los siguientes atributos: un atributo de ubicación, un atributo de límite, un atributo de tiempo, y un atributo de máquina POS.
4. El método de configuración según la reivindicación 3, en donde la característica de entorno comprende el atributo de límite, y antes de recibir, por un controlador de comunicación de campo cercano en un extremo local, una primera instrucción de configuración enviada por un ordenador principal de dispositivo en el extremo local, el método de
- 30 configuración además comprende:
- ordenar (220), por el ordenador principal de dispositivo, a un primer elemento seguro correspondiente al atributo de límite que separe un segundo elemento seguro del primer elemento seguro; y
- recibir (240), por el controlador de comunicación de campo cercano, un comando de registro enviado por el segundo elemento seguro.
- 35 5. Una terminal móvil para implementar la selección de un elemento seguro en la comunicación de campo cercano, en donde la terminal móvil comprende un controlador de comunicación de campo cercano en un extremo local que comprende:
- una unidad de recepción (610), configurada para recibir una primera instrucción de configuración enviada por un ordenador principal de dispositivo en el extremo local, en donde la primera instrucción de configuración comprende
- 40 una característica de entorno usada para seleccionar el elemento seguro; y
- una unidad de configuración (620), configurada para configurar la característica de entorno en un controlador de comunicación de campo cercano según la primera instrucción de configuración;
- en donde la unidad de recepción (610) se configura además para recibir una segunda instrucción de configuración enviada por el ordenador principal de dispositivo;
- 45 caracterizado por que la unidad de configuración (620) se configura además para:
- según la segunda instrucción de configuración, configurar la característica de entorno en una instrucción de respuesta de atributo para comunicarse e interactuar con un extremo par, para continuar comunicándose e

interactuando con el extremo par según la instrucción de respuesta de atributo configurada y además completar la selección del elemento seguro; y,

seleccionar un elemento seguro según la característica de entorno configurada para la subsiguiente comunicación e interacción con el extremo par.

- 5 6. La terminal móvil según la reivindicación 5, en donde la unidad de recepción se configura además para recibir una tabla de encaminamiento generada por el ordenador principal de dispositivo según la característica de entorno.

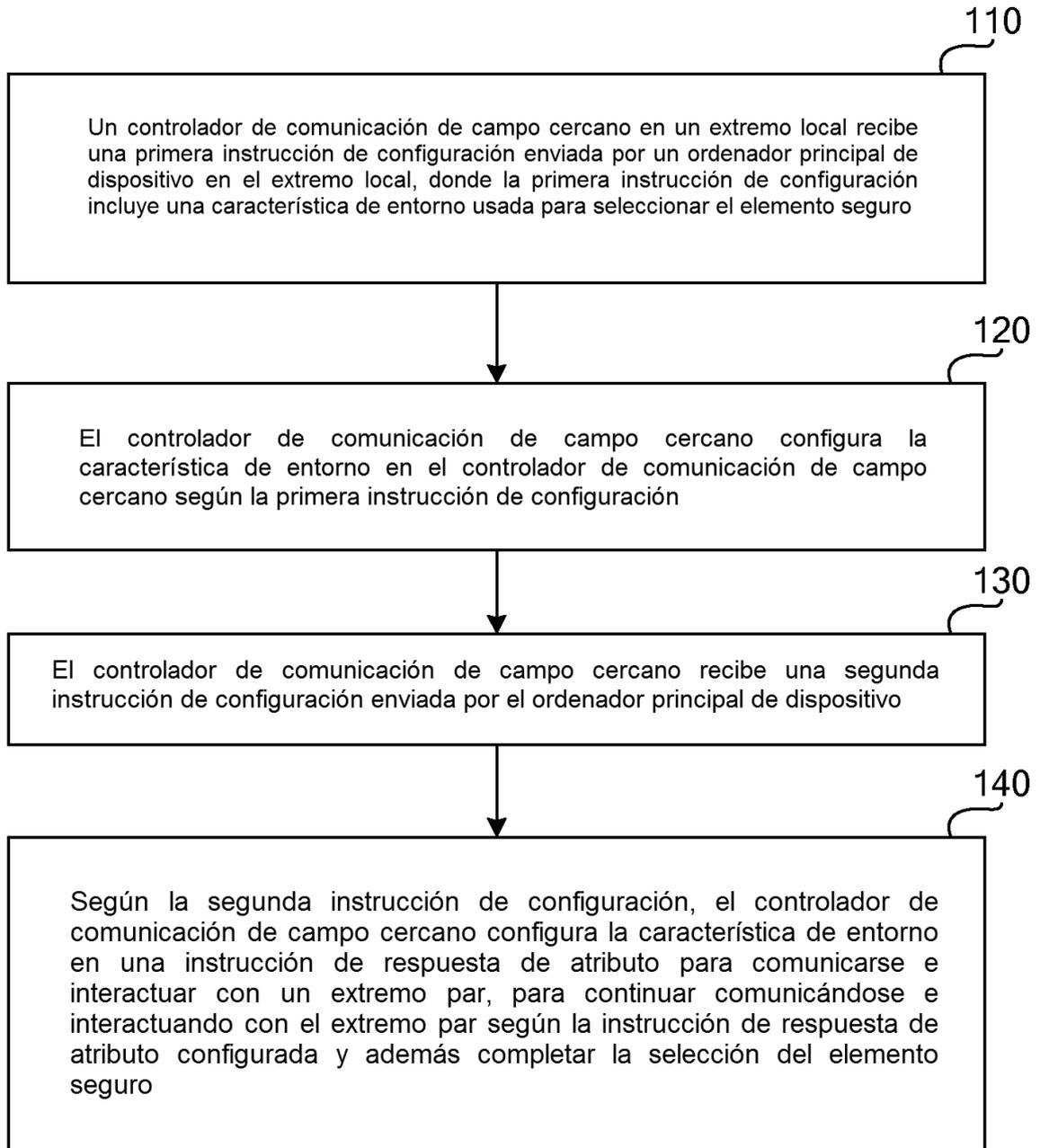


FIG. 1

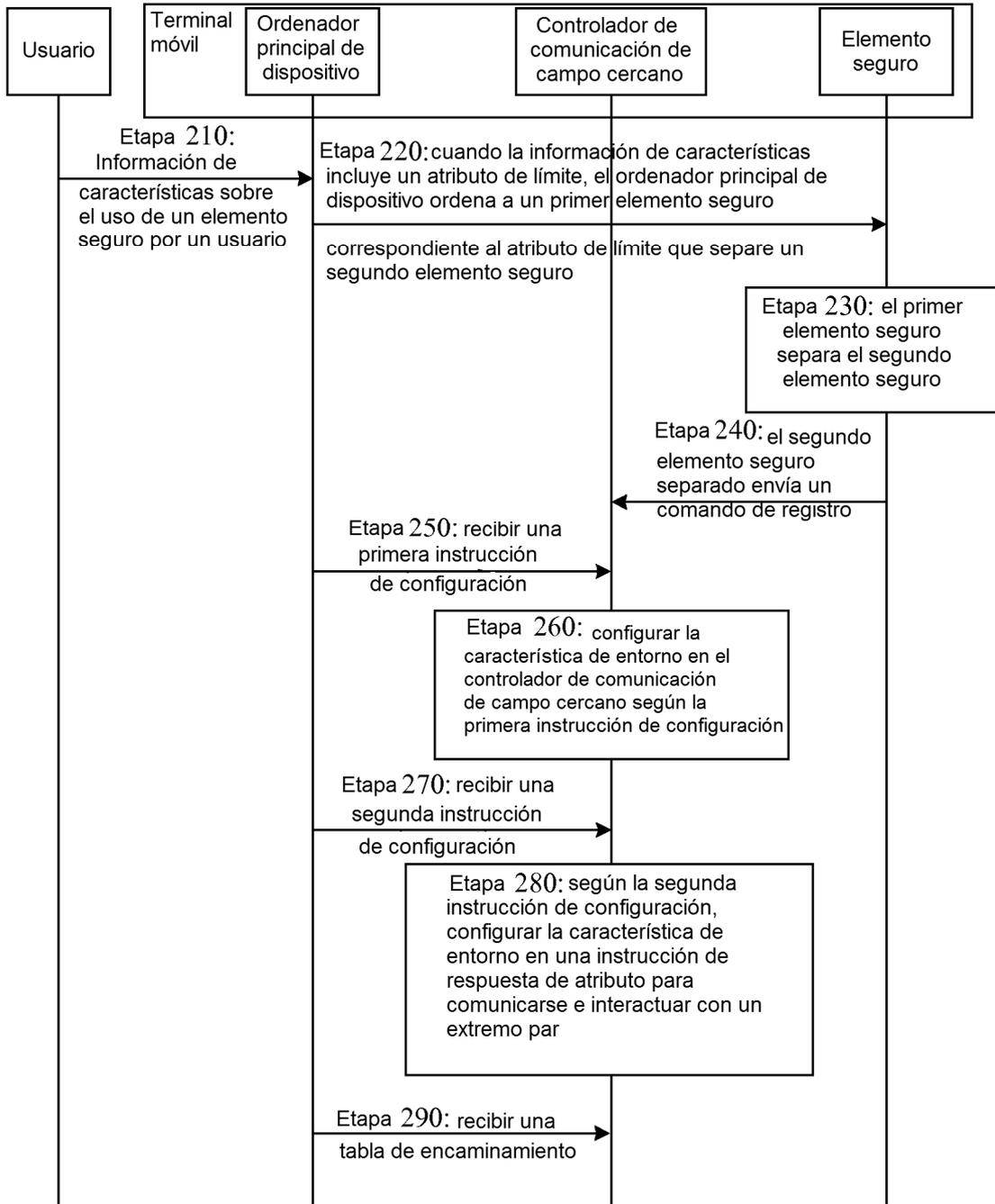


FIG. 2

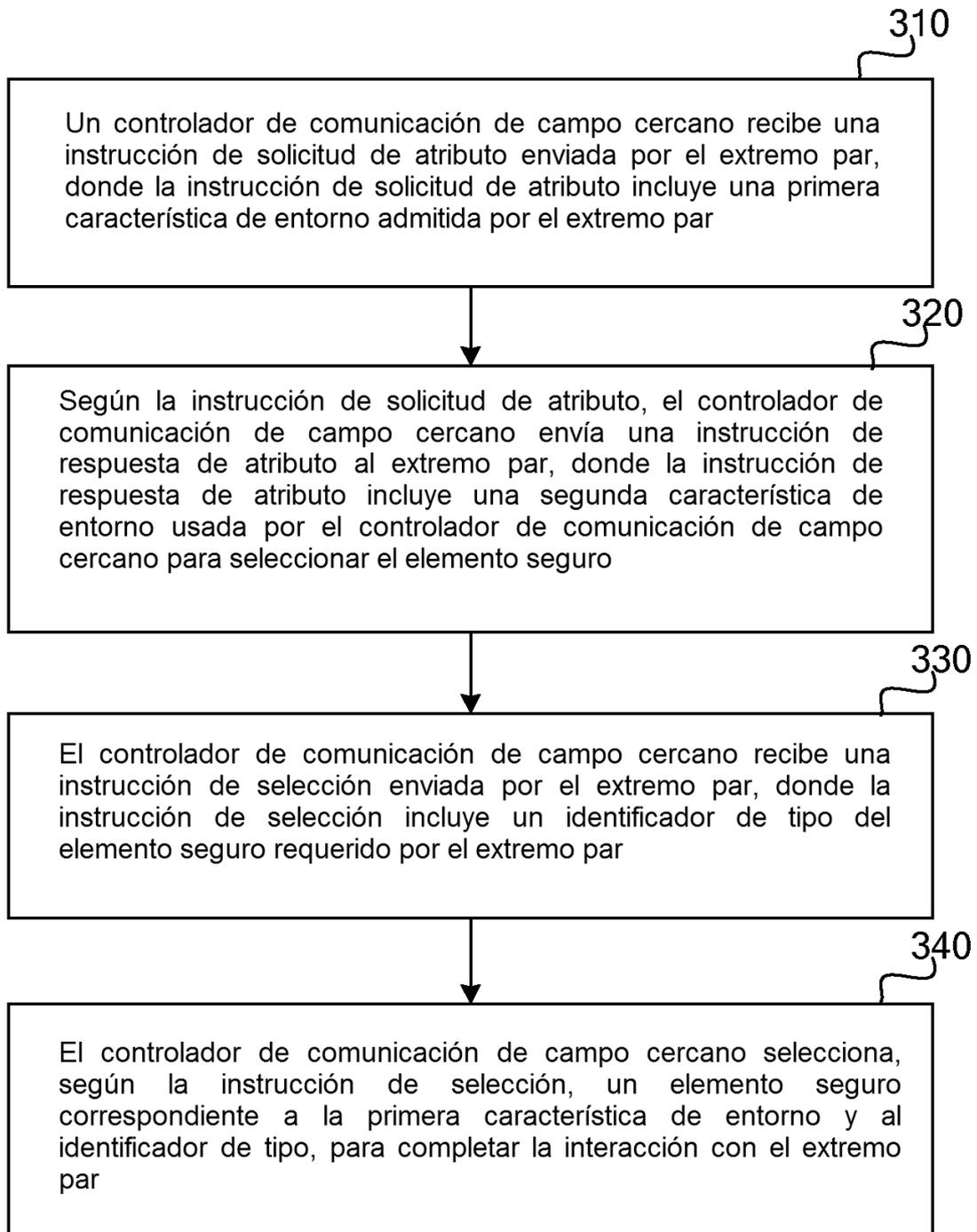


FIG. 3

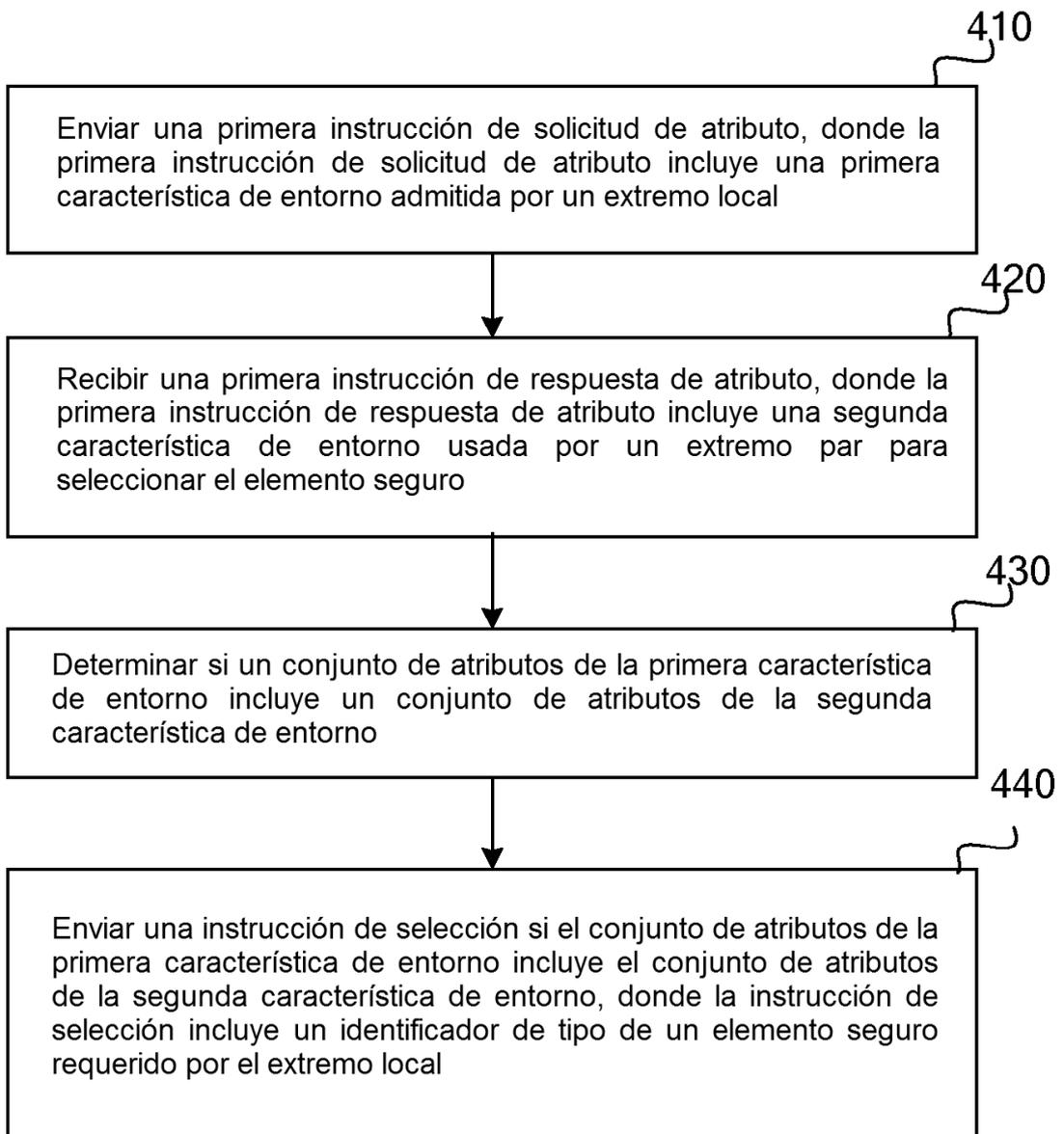


FIG. 4

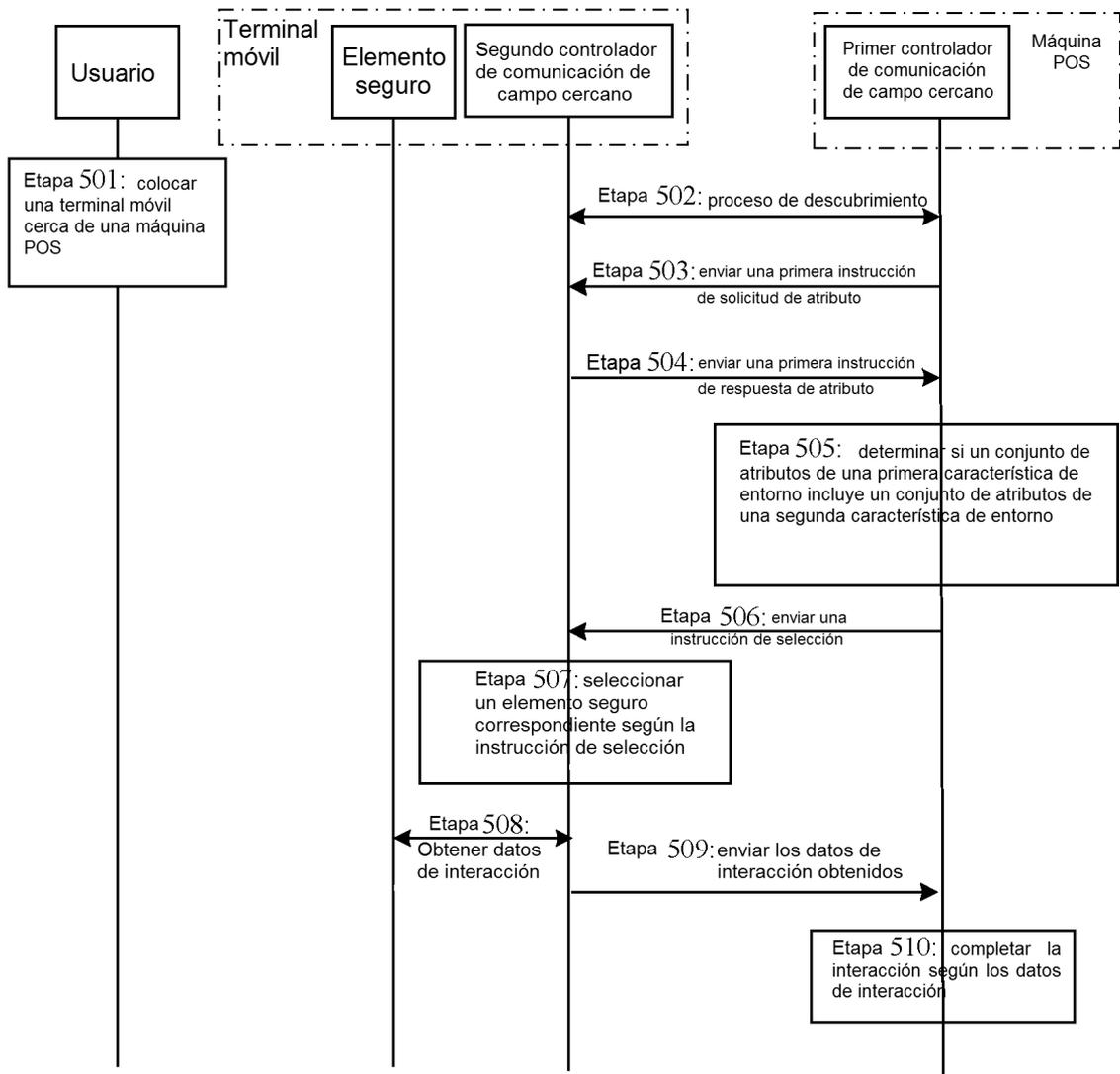


FIG. 5

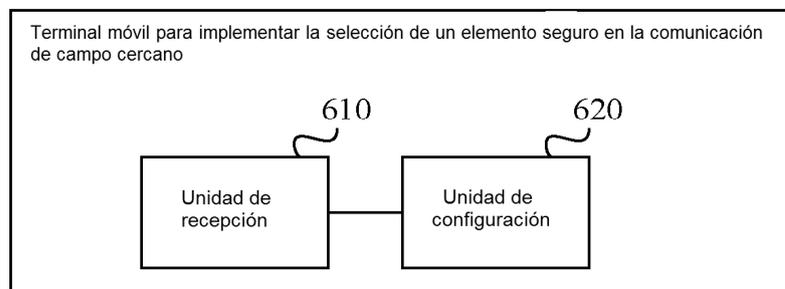


FIG. 6

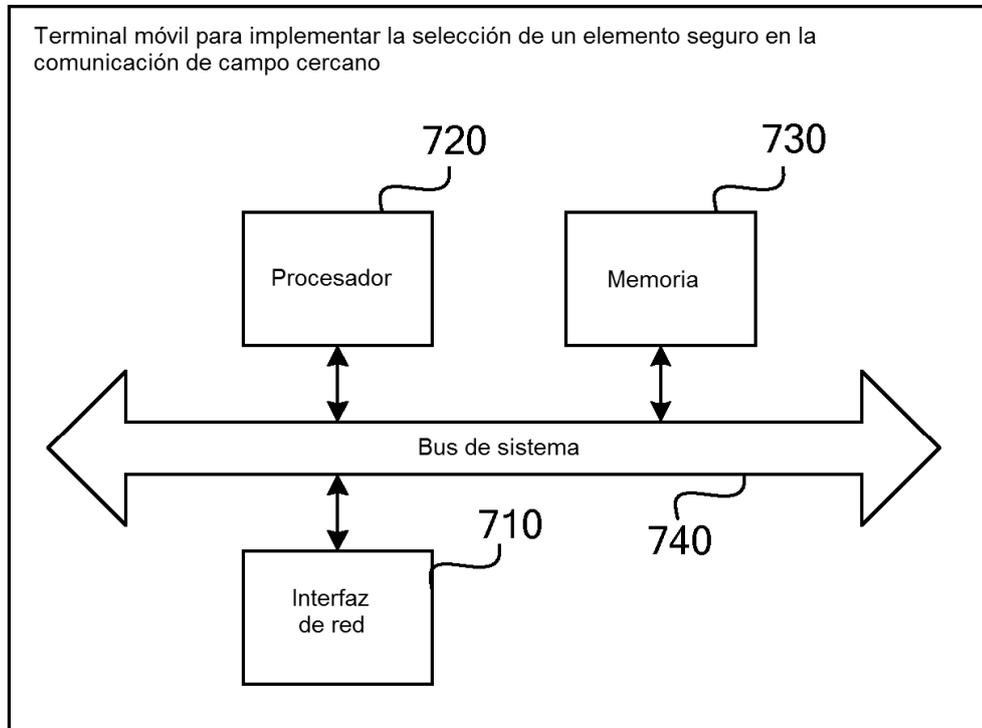


FIG. 7

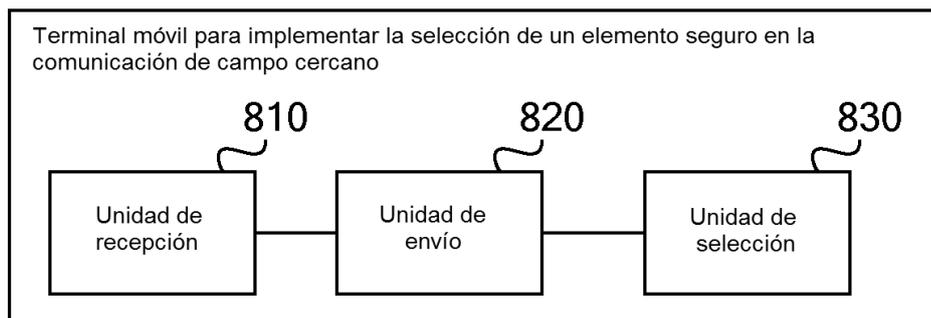


FIG. 8

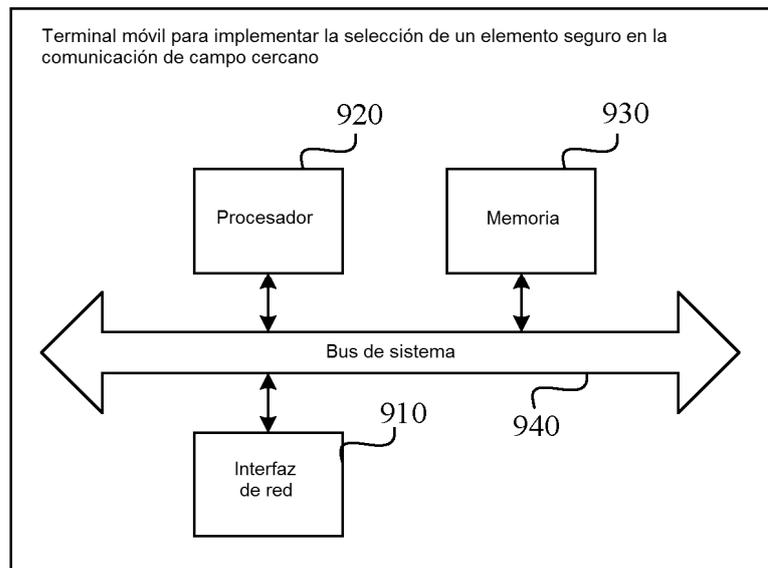


FIG. 9

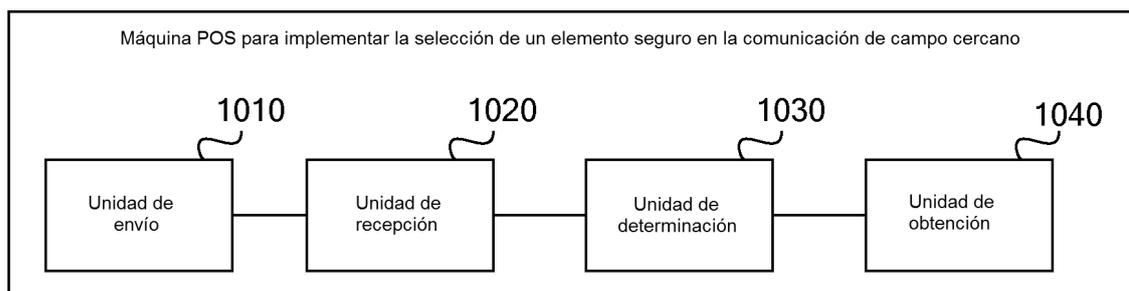


FIG. 10

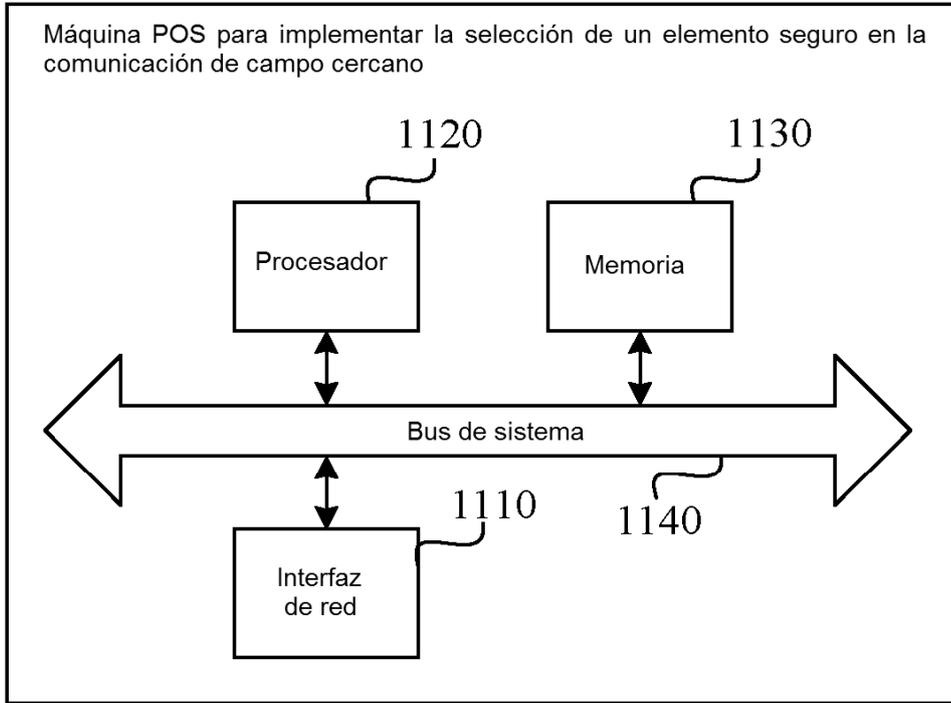


FIG. 11

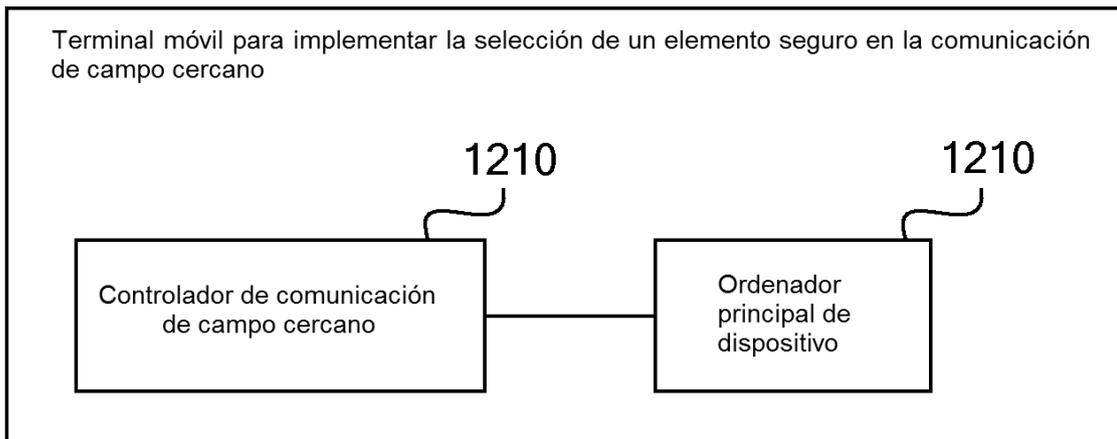


FIG. 12