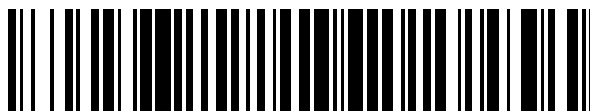


19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 719 609**

51 Int. Cl.:

**H04W 12/06** (2009.01)

**H04B 5/00** (2006.01)

**G06Q 20/32** (2012.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **21.06.2012 E 12305707 (7)**

97 Fecha y número de publicación de la concesión europea: **09.01.2019 EP 2677790**

54 Título: **Sistema de NFC que comprende una pluralidad de elementos seguros**

45 Fecha de publicación y mención en BOPI de la traducción de la patente:  
**11.07.2019**

73 Titular/es:  
**TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)**  
**(100.0%)**  
**164 83 Stockholm, SE**

72 Inventor/es:  
**GIMENO MONGE, PABLO IGNACIO y**  
**DEL PRADO PAVON, JAVIER**

74 Agente/Representante:  
**ELZABURU, S.L.P**

ES 2 719 609 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

Sistema de NFC que comprende una pluralidad de elementos seguros

### 5 CAMPO TÉCNICO

La invención se refiere al campo de la electrónica y, más particularmente, a un método, un dispositivo electrónico, un programa y un medio de almacenamiento de datos para realizar la comunicación de campo cercano (NFC).

### 10 ANTECEDENTES

10 Se espera que los sistemas de NFC se integren en los teléfonos móviles de próxima generación. La NFC típica es una tecnología de radio de corto alcance basada en el acoplamiento inductivo de dos antenas de bucle que resuenan a 13,56 MHz. Las velocidades de datos típicas están en el intervalo de 106 a 424 Kbps, y la distancia de comunicación es del orden de varios centímetros. Aplicaciones típicas incluyen transacciones seguras para el pago y la expedición de boletos. Las aplicaciones de NFC seguras requieren la adición al sistema de uno o más Elementos Seguros (SE) para contener información confidencial (por ejemplo, números de tarjeta de crédito, suscripciones del sistema de transporte).

20 Los sistemas de RFID sin contacto, los antecesores de los sistemas de NFC, comprenden una aplicación única, almacenada en un único SE, contenida en el mismo dispositivo que realiza la comunicación por radio de RFID. Los primeros dispositivos de NFC son chips de NFC independientes con al menos un SE (comprendido en el dispositivo de NFC o accesible externamente a través de una interfaz dedicada), que admite al menos una aplicación segura. Están surgiendo normas que definen interfaces y protocolos que dan acceso a los SE como dispositivos independientes (ETSI 102613/102622), restringidas por el momento a sistemas de SE individuales. Las interfaces propietarias también se utilizan para acceder a los SE.

25 El documento WO 2012/065643 A1 divulga un método para identificar una aplicación de NFC en un dispositivo habilitado para NFC que comprende una pluralidad de entornos de ejecución de NFC, en el que la aplicación de NFC está alojada por uno de la pluralidad de entornos de ejecución de NFC, comprendiendo el método: recibir, a través de una interfaz aérea, una solicitud externa para acceder a la aplicación de NFC; enviar una consulta asociada con la solicitud externa a más de uno de la pluralidad de entornos de ejecución de NFC; recibir más de una respuesta a la consulta de más de uno de la pluralidad de entornos de ejecución de NFC, respectivamente; y analizar las más de una respuestas para identificar una respuesta positiva que indique que la aplicación de NFC está alojada en una de la pluralidad de entornos de ejecución de NFC.

### 35 COMPENDIO

La invención tiene como objetivo mejorar el campo de la NFC.

40 Este objeto se logra con un método implementado por un dispositivo electrónico que comprende un sistema de NFC. El sistema comprende un extremo frontal sin contacto de NFC, una pluralidad de interfaces de elementos seguros a las que se conecta una pluralidad de elementos seguros y una unidad de procesamiento adaptada para controlar el extremo frontal sin contacto de NFC y la pluralidad de elementos seguros a través de las interfaces de los elementos seguros. El método comprende enviar una orden de inicialización a todos los elementos seguros a través de las interfaces de elementos seguros, tras la exposición del extremo frontal sin contacto de NFC a un lector de NFC.

45 Este objeto también se logra con un dispositivo electrónico que comprende un sistema de NFC. El sistema comprende un extremo frontal sin contacto de NFC, una pluralidad de interfaces de elementos seguros adaptadas para conectar una pluralidad de elementos seguros (pudiendo una pluralidad de elementos seguros estar o no conectados realmente a las interfaces de elementos seguros), y una unidad de procesamiento adaptada para controlar el extremo frontal sin contacto de NFC y la pluralidad de elementos seguros a través de las interfaces de elementos seguros. El dispositivo está adaptado para realizar el método anterior. El dispositivo puede ser un dispositivo de comunicación móvil.

50 Este objeto también se logra con un programa de ordenador que comprende instrucciones para realizar el método anterior.

55 Este objeto también se logra con un medio de almacenamiento de datos que tiene registrado en el mismo el programa anterior.

60 La invención ofrece muchas ventajas, que incluyen las siguientes:

- Gracias al sistema de NFC, el dispositivo electrónico puede usarse convenientemente para realizar la NFC.
- El dispositivo puede tener una pluralidad de elementos seguros conectados gracias a la pluralidad de interfaces, lo que hace que el dispositivo sea más cómodo que otros dispositivos que comprenden una sola interfaz de elemento seguro.
- 65 - Debido a que el método comprende, al exponerse el extremo frontal sin contacto de NFC a un lector de NFC, enviar la orden de inicialización a todos los elementos seguros en lugar de a uno solo, el acceso a la

aplicación solicitada se realiza de manera relativamente rápida, aunque el dispositivo comprenda una pluralidad de elementos seguros, y sin necesidad de una pluralidad de extremos frontales sin contacto de NFC (por ejemplo, uno por elemento seguro).

- 5 Otras características y ventajas de la invención aparecerán a partir de la siguiente descripción de realizaciones de la invención, dadas como ejemplos no limitativos, con referencia a los dibujos adjuntos mencionados a continuación.

#### BREVE DESCRIPCIÓN DE LOS DIBUJOS

- 10 La figura 1 muestra una representación esquemática de un ejemplo del dispositivo electrónico,  
La figura 2 muestra una representación esquemática de un ejemplo de un sistema de NFC,  
La figura 3 muestra un diagrama de flujo de un ejemplo del método, y  
La figura 4 muestra una representación esquemática de ejemplos del paso de inicialización del método.

#### DESCRIPCIÓN DETALLADA

- 15 El método se puede realizar en base a un programa de ordenador que comprenda instrucciones para realizar el método, por ejemplo leyendo las instrucciones por medio de una unidad de procesamiento (es decir, un procesador). El programa puede ser ejecutable en un dispositivo programable (es decir, el dispositivo electrónico). El programa de aplicación puede implementarse en un lenguaje de programación orientado a objetos o de procedimiento de alto nivel, o en lenguaje ensamblador o de máquina, si se desea. En cualquier caso, el lenguaje puede ser un lenguaje compilado o interpretado. El programa puede ser un programa de instalación completo o un programa de actualización. En este último caso, el programa es un programa de actualización que actualiza un dispositivo programable, previamente programado para realizar partes del método, a un estado en el que el dispositivo es adecuado para realizar todo el método.

- 25 El programa puede estar grabado en un medio de almacenamiento de datos. El medio de almacenamiento de datos puede ser cualquier memoria adaptada para grabar instrucciones de ordenador. El medio de almacenamiento de datos puede ser, por lo tanto, cualquier forma de memoria no volátil, incluyendo a modo de ejemplo dispositivos de memoria de semiconductores, tales como EPROM, EEPROM y dispositivos de memoria flash; discos magnéticos tales como discos duros internos y discos extraíbles, discos magneto-ópticos y discos de CD-ROM.

- 30 Un dispositivo adecuado para realizar el método puede ser un dispositivo electrónico que comprenda una memoria de hardware, que incluya una memoria volátil y/o no volátil, y que haya grabado en el mismo el programa. La memoria puede almacenar cualquier otra información utilizada por el método. La memoria es accesible por al menos un procesador, por ejemplo una unidad central de procesamiento (CPU) del dispositivo. El procesador puede ejecutar el programa y, por lo tanto, puede realizar el método, sin programación adicional del dispositivo.

- 35 El dispositivo comprende un sistema de NFC adecuado para realizar NFC con el dispositivo. El sistema comprende un extremo frontal sin contacto de NFC, que es una interfaz para realizar NFC con otro dispositivo, tal como un lector de NFC. El extremo frontal sin contacto de NFC puede comprender un módulo de radio para recibir y/o emitir una señal de NFC. El extremo frontal sin contacto de NFC puede comprender (o estar acoplado a) una unidad de procesamiento, posiblemente la CPU mencionada anteriormente. El sistema puede comprender un único extremo frontal sin contacto de NFC. Por lo tanto, el dispositivo puede ser fácil y barato de construir y ocupar menos espacio.

- 45 El sistema comprende una pluralidad de (es decir, al menos dos) interfaces de elementos seguros adaptadas para conectar una pluralidad de elementos seguros (es decir, un elemento seguro por interfaz). Como es sabido en sí, los elementos seguros son piezas de hardware conectables al sistema y que contienen datos (por ejemplo, en una memoria) que pueden comunicarse a través de NFC de manera segura (por ejemplo, respetando cualquier requisito de seguridad estándar). Un elemento seguro puede comprender un procesador y una memoria, así como una aplicación, es decir, una pieza de software que se ejecuta dentro del elemento seguro, siendo accesible la aplicación mediante un lector de NFC a través de NFC de una manera segura. Elementos seguros típicos son las tarjetas SIM y las tarjetas SD. Las interfaces comprenden una parte de hardware y una parte de software, que pueden ser las conocidas en la técnica, por ejemplo; de acuerdo con las normas ETSI 102613 y/o ETSI 102622. Tener al menos una o al menos ambas de las normas anteriores es particularmente convenientes para conectar una pluralidad de elementos seguros al dispositivo.

- 55 El sistema de NFC comprende además una unidad de procesamiento adaptada para controlar el extremo frontal sin contacto de NFC y la pluralidad de elementos seguros a través de las interfaces de elementos seguros. En otras palabras, la unidad de procesamiento está en comunicación con el extremo frontal sin contacto de NFC, por ejemplo, para recibir señales entrantes de un lector de NFC y canalizadas por el extremo frontal sin contacto, y con los elementos seguros que están conectados a las interfaces, por ejemplo para hacer que los elementos seguros realicen acciones tales como el intercambio de datos.

- 65 En un ejemplo, el dispositivo puede comprender además convertidores de audio y transductores, tales como convertidor de digital en analógico (DAC) y un altavoz. En tal caso, el dispositivo puede reproducir la señal de audio numérica. El dispositivo puede comprender además una interfaz gráfica de usuario, tal como una pantalla sensible o una pantalla y un teclado.

5 El dispositivo puede ser un dispositivo de comunicación. El dispositivo puede comprender así un emisor de señal y un receptor de señal. Por ejemplo, el dispositivo puede ser un teléfono. El dispositivo puede ser un dispositivo de comunicación inalámbrica. El dispositivo puede ser móvil (es decir, transportable). El dispositivo puede ser, por ejemplo, un teléfono móvil (por ejemplo, un teléfono celular).

Se hace referencia a la figura 1, que muestra un diagrama de bloques que representa un ejemplo de un dispositivo 30 electrónico móvil, que puede ser un teléfono móvil, adecuado para implementar el método.

10 En el ejemplo, el dispositivo 30 se puede usar para capturar datos de audio e imagen. Para esto, el dispositivo 30 comprende la cámara 32 y el micrófono 34 para capturar respectivamente datos de imagen y audio. El dispositivo 30 también comprende la memoria 36, que puede consistir en memoria volátil y no volátil (no se distingue en la figura). La memoria 36 se puede dividir en varios compartimentos, posiblemente separados físicamente en el dispositivo 30. La memoria 36 almacena, grabadas en ella, las instrucciones para realizar el método, posiblemente ya compiladas o precompiladas. El dispositivo 30 también comprende procesadores que incluyen la CPU 38, el procesador 46 de señal de imagen (ISP) y el procesador 48 de señal de audio (ASP). Estos procesadores acceden a los datos a través del bus 44, procesan los datos y hacen circular los datos a través del bus 44. Por supuesto, se pueden incorporar físicamente menos de tres procesadores, por ejemplo si un procesador realiza todos los cálculos. Por otro lado, se pueden incorporar físicamente más de tres procesadores, por ejemplo, en el caso de procesamiento paralelo. El dispositivo 30 también comprende una pantalla 50 y un altavoz 52 para emitir datos, es decir, para mostrar respectivamente datos de imagen y reproducir datos de audio. El dispositivo 30 también comprende el receptor 40 y el emisor 42, que están destinados a comunicarse con el exterior, por ejemplo con otros dispositivos, por ejemplo si el dispositivo 30 es un teléfono celular.

25 El dispositivo 30 también comprende el sistema 49 de NFC. Por ejemplo, el dispositivo 30 puede estar expuesto a un lector de NFC (no representado). Tras dicha exposición, el procesador del sistema 49 de NFC (no representado en la figura) envía una orden de inicialización a todos los elementos seguros a través de las interfaces de elementos seguros (tampoco representadas).

30 La figura 2 muestra una representación esquemática de un ejemplo del sistema 49 de NFC de la figura 1, que puede ser utilizado en cualquier otro dispositivo electrónico.

El sistema 49 de NFC comprende un extremo frontal 62 sin contacto de NFC, incluido en la estación 60 de radio en el ejemplo, para realizar una comunicación de tipo NFC representada por líneas 61 de puntos con el lector 63 de NFC que también tiene una estación 65 de radio. El sistema 49 de NFC también comprende la pluralidad 70 de interfaces SE1\_IF y SE2\_IF de elementos seguros conectadas a la pluralidad 72 de elementos seguros SE1 y SE2 (que se representan tanto como conectados a las interfaces 70 como en una vista separada y ampliada, respectivamente, en los círculos de líneas de puntos pequeños y más grandes). La pluralidad de elementos seguros puede comprender elementos seguros que sean elementos extraíbles y/o elementos seguros que estén montados permanentemente en el sistema (por ejemplo, soldados). El sistema de NFC también comprende la unidad 66 de procesamiento que puede ser una unidad de procesamiento dedicada o, preferiblemente para ahorrar recursos, una CPU del dispositivo electrónico. Como se puede ver en la figura, la unidad 66 de procesamiento está acoplada al extremo frontal 62 sin contacto de NFC y a la pluralidad 72 de elementos seguros (a través de las interfaces 70), y por lo tanto está adaptada para controlar estos elementos.

45 La figura 2 representa una situación en la que el extremo frontal 62 sin contacto del sistema 49 de NFC está expuesto al lector 63 de NFC, que intenta acceder a la aplicación  $A^2_1$ . Tras dicha exposición, según el método implementado por el dispositivo electrónico que comprende el sistema 49 de NFC, el extremo frontal 62 sin contacto indica a la unidad de procesamiento 66 que está cerca de un lector de NFC, que es el lector 63 de NFC en esta situación, y, opcionalmente, que un intento de acceso a una aplicación está siendo realizado por dicho lector 63 de NFC (en esta etapa, con o sin la precisión de que es específicamente la aplicación  $A^2_1$ ). Tras dicha indicación, la unidad 66 de procesamiento envía (o asegura el envío de) una orden de inicialización a todos los elementos 70 seguros (SE1 y SE2 en el ejemplo) a través de las interfaces 70 (SE1\_IF y SE2\_IF en el ejemplo) de elementos seguros. La orden de inicialización notifica a los elementos seguros que se llevará a cabo alguna actividad de NFC, de modo que se puedan inicializar los elementos seguros. La inicialización de los elementos seguros consiste en una serie de operaciones realizadas por los elementos seguros para permitir la comunicación entre ellos y la unidad de procesamiento (por ejemplo, el lector de NFC a través de la unidad de procesamiento). En particular, la inicialización de los elementos seguros puede hacer que los elementos seguros salgan de un estado inactivo (en el que se encontraban antes de la exposición al lector de NFC) y activar los elementos seguros. Por lo tanto, con un solo extremo frontal 62 sin contacto, el sistema de NFC garantiza la inicialización de todos los elementos seguros (tanto SE1 como SE2), de modo que el lector 63 de NFC puede acceder a la aplicación  $A^2_1$  de manera rápida y robusta, con poca complejidad y bajo consumo de recursos.

65 Para los elementos seguros, la inicialización puede ser, como se conoce *per se*, un proceso de dos pasos dependiente de la interfaz: una solicitud de inicialización, seguida de un reconocimiento o una disponibilidad predefinida en tiempo. El sistema de NFC puede entonces enviar al lector de NFC un mensaje que indique su

disponibilidad para la ejecución de una aplicación a través de NFC (es decir, también llamado "mensaje de respuesta inicial").

5 La figura 3 muestra un diagrama de flujo de un ejemplo del método, por ejemplo realizado por cualquier dispositivo electrónico que comprenda un sistema de NFC adaptado al mismo, por ejemplo, el sistema 49 de NFC de la figura 2, por ejemplo el dispositivo 30 de la figura 1. El método del ejemplo permite la ejecución de una aplicación alojada por uno de los elementos seguros de una manera eficiente.

10 El método del ejemplo comprende exponer (S5) el extremo frontal sin contacto al lector de NFC. Tras dicha acción, los elementos seguros son inicializados (S20), mientras que los elementos seguros se desactivan de lo contrario (excepto si se expusieron previamente al lector de NFC o a otro lector de NFC).

15 Una vez que todos los elementos seguros se inicializan (es decir, en el "estado listo"), el método puede comprender recibir (S20) del lector de NFC una solicitud para acceder a una aplicación. El método puede entonces determinar el elemento seguro que aloja la aplicación. Luego, el sistema puede activar el elemento seguro que aloja la aplicación a través de su interfaz de elemento seguro (excepto si el elemento seguro ya estaba activado previamente). En paralelo, el método envía (S25) al lector de NFC una respuesta a la solicitud de activación.

20 Una vez que el elemento seguro que aloja la aplicación está activado (es decir, listo para la ejecución de una aplicación en él), el lector de NFC en el método del ejemplo envía (S30) una orden para seleccionar la aplicación al elemento seguro que aloja la aplicación. La aplicación puede ser entonces ejecutada.

25 El dispositivo y el método proponen así un marco de acceso unificado de SE que es agnóstico de la interfaz de SE, de modo que varias instancias de SE se pueden integrar de manera eficiente en un sistema de NFC, permitiendo la inicialización simultánea de SE independientemente de la interfaz y el protocolo soportados. El sistema de NFC inicializa todos los elementos seguros antes de lanzar la selección de una aplicación (por ejemplo, antes de enviar el mensaje de respuesta inicial al lector de la NFC). La inicialización debe llevarse a cabo y luego se alcanza un estado de activación, definiéndose la activación como el estado en el que un elemento seguro está listo para enviar (recibir) datos a (desde) las aplicaciones cargadas dentro. El dispositivo y el método proporcionan un marco flexible que da acceso a todas las aplicaciones alojadas en varios elementos seguros conectados a un sistema de NFC. Esta es una mejora significativa en comparación con los sistemas ya existentes.

35 Ahora, refiriéndose a la figura 4, que puede aplicarse al ejemplo de la figura 2 (es decir, un dispositivo electrónico que comprende un sistema de NFC que tiene dos elementos seguros SE1 y SE2 conectados a través de las interfaces SE1\_IF y SE2\_IF), posiblemente en combinación con el ejemplo de la FIG.1 y/o el ejemplo de la figura 3, enviando una de inicialización a todos los elementos seguros, puede realizarse simultáneamente o de manera intercalada (la figura 4 representa las dos opciones, junto con la inicialización del extremo frontal sin contacto). De hecho, la secuencia para la inicialización del elemento seguro puede diseñarse de diferentes maneras, por ejemplo, todos los elementos seguros podrían inicializarse simultáneamente (lo que lleva a un rápido tiempo de inicialización combinado), intercalado uno por uno (lo que lleva a una baja demanda de potencia), o con una mezcla simultánea e intercalada. En todos los casos, el objetivo es el mismo, es decir, poner todos los elementos seguros en un estado inicializado, y eso independientemente de la interfaz y los protocolos utilizados para comunicarse con el elemento seguro, e independientemente de la(las) aplicación(es) cargada(s) dentro del(de los) elemento(s) seguro(s).

**REIVINDICACIONES**

- 5 1. Un método ejecutado por un dispositivo electrónico (30) que comprende un sistema (49) de comunicación de campo cercano (NFC) , en el que:
- el sistema comprende:
- 10 - un extremo frontal (62) sin contacto de NFC,  
- una pluralidad (70) de interfaces (SE1\_IF, SE2\_IF) de elementos seguros a las que están conectados una pluralidad (72) de elementos (SE1, SE2) seguros, y  
- una unidad (66) de procesamiento adaptada para controlar el extremo frontal sin contacto de NFC y la pluralidad de elementos seguros a través de las interfaces de elementos seguros,
- 15 y el método comprende:  
enviar (S10) una orden de inicialización a todos los elementos seguros a través de las interfaces de elementos seguros, tras la exposición del extremo frontal sin contacto de la NFC a un lector de NFC.
- 20 2. El método de la reivindicación 1, en el que el envío de una orden de inicialización a todos los elementos seguros se realiza de manera simultánea o intercalada.
3. El método de la reivindicación 1 ó 2, en el que el método comprende además, una vez que están inicializados todos los elementos seguros:
- 25 - recibir (S20) del lector de NFC una solicitud para acceder a una aplicación, y luego  
- determinar y activar el elemento seguro que aloja la aplicación,  
- enviar (S25) al lector de NFC una respuesta a la solicitud para acceder a una aplicación.
- 30 4. El método de la reivindicación 3, en el que el método comprende además, una vez que se activa el elemento seguro que aloja la aplicación, recibir (S30) una orden del Lector de NFC para seleccionar la aplicación por el elemento seguro que aloja la aplicación.
- 35 5. Un dispositivo electrónico (30) que comprende un sistema (49) de comunicación de campo cercano (NFC), en el que el sistema comprende:
- 40 - un extremo frontal (62) sin contacto de NFC,  
- una pluralidad (70) de interfaces (SE1\_IF, SE2\_IF) del elementos seguros adaptadas para conectar una pluralidad de elementos seguros, y  
- una unidad (66) de procesamiento adaptada para controlar el extremo frontal sin contacto de NFC y la pluralidad de elementos seguros a través de las interfaces de elementos seguros,
- estando el sistema adaptado para realizar el método de cualquiera de las reivindicaciones 1-4.
- 45 6. El dispositivo de la reivindicación 5, en el que las interfaces de elementos seguros comprenden al menos una o dos interfaces de ETSI.
7. El dispositivo de la reivindicación 5 ó 6, en el que el dispositivo comprende además una pluralidad (70) de elementos seguros (SE1, SE2) conectados a las interfaces de elementos seguros.
- 50 8. El dispositivo de cualquiera de las reivindicaciones 5-7, en el que el dispositivo es un dispositivo de comunicación móvil.
9. Un programa informático que comprende instrucciones para realizar el método de cualquiera de las reivindicaciones 1-4.
- 55 10. Un medio de almacenamiento de datos que tiene registrado en el mismo el programa de la reivindicación 9.

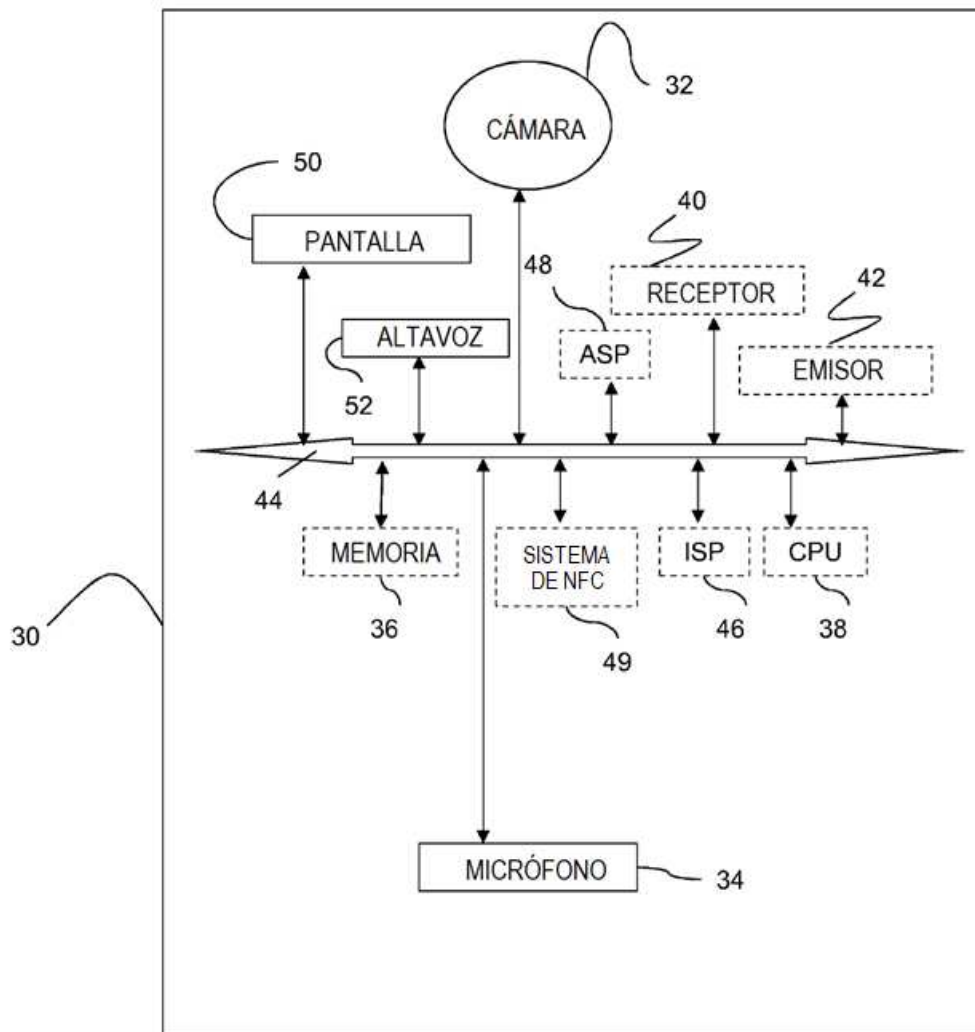


FIG. 1

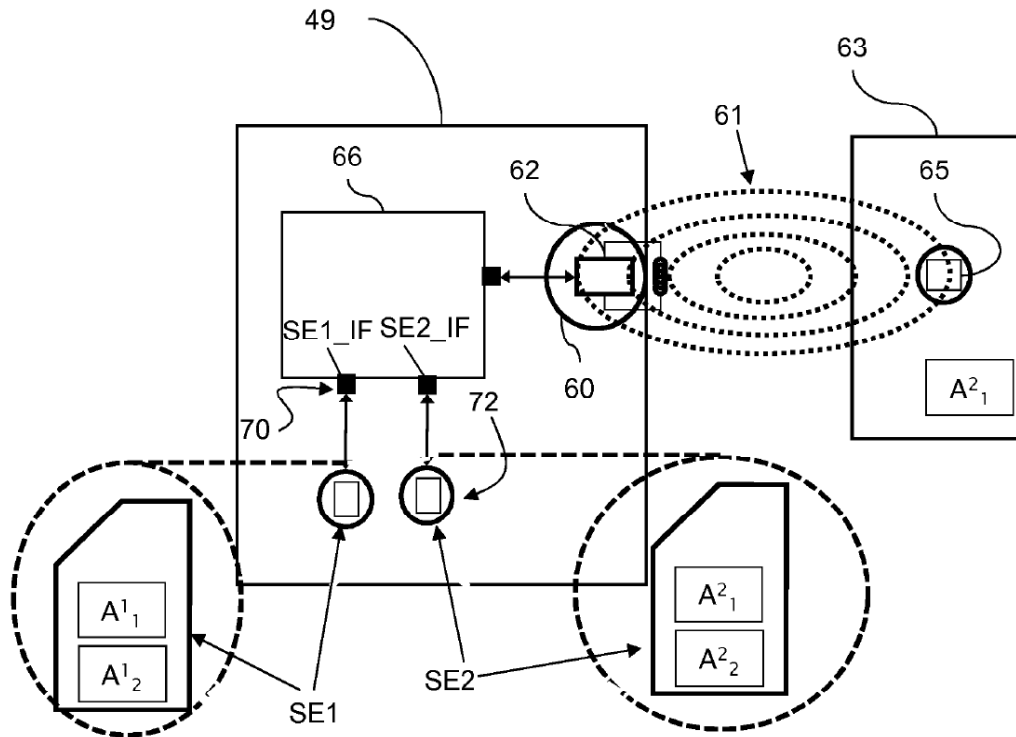


FIG. 2



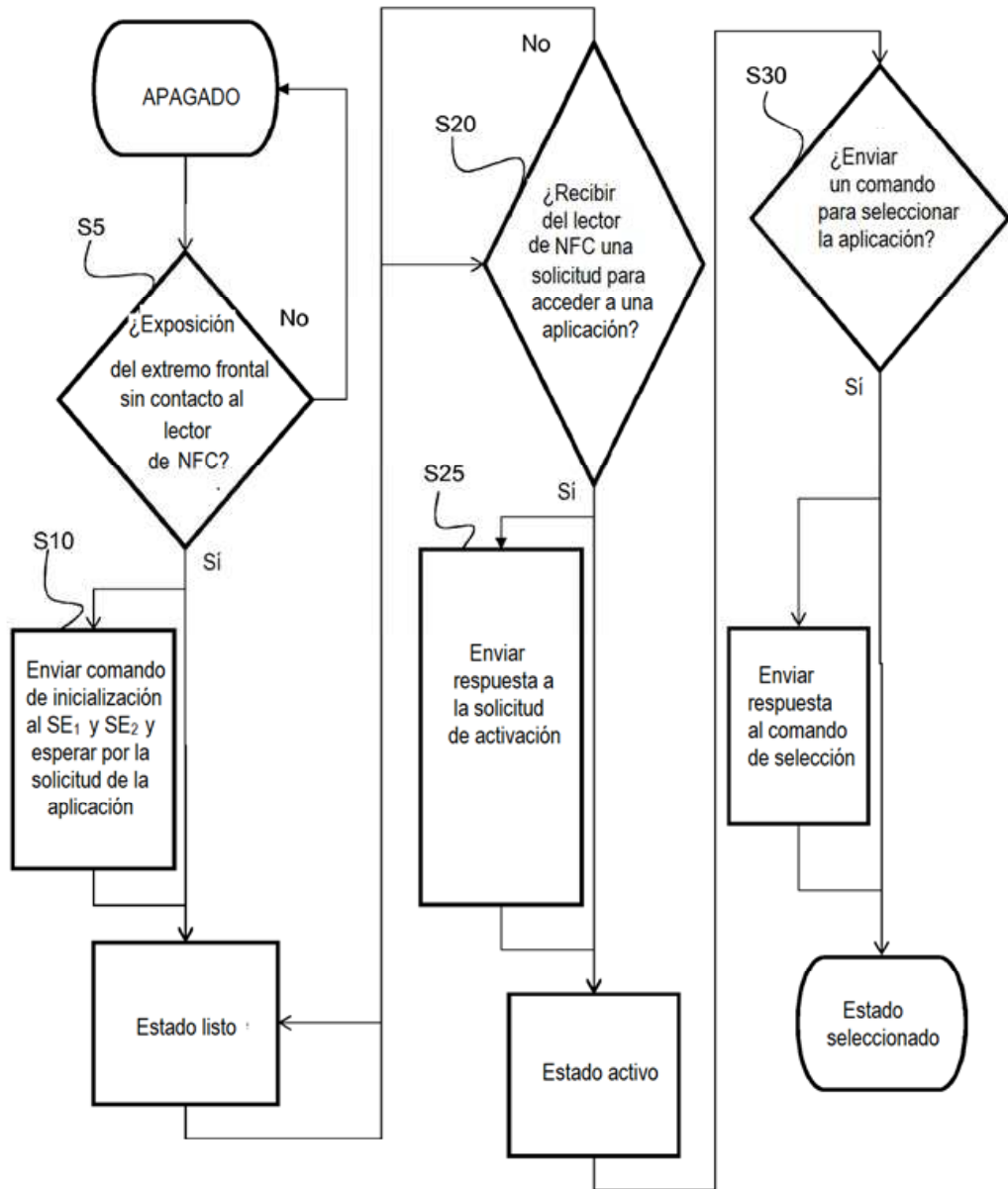


FIG. 3

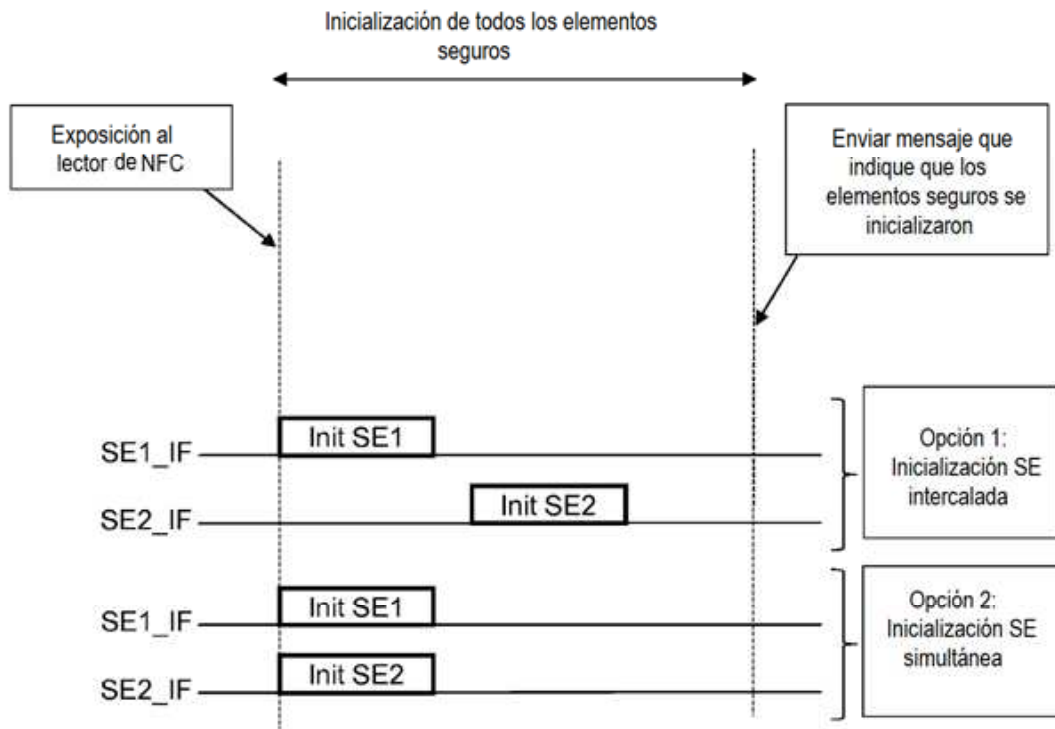


FIG. 4