(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 450 193**

(51) Int. CI.:

G06K 19/07 (2006.01)
G06K 19/073 (2006.01)
G06K 19/077 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **24.07.2006 E 06778905 (7)**

(97) Fecha y número de publicación de la concesión europea: **04.12.2013 EP 1907993**

(54) Título: **Entidad electrónica con medios de comunicación por contacto y a distancia**

(30) Prioridad:

25.07.2005 FR 0507887

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.03.2014

(73) Titular/es:

OBERTHUR TECHNOLOGIES (100.0%)
420, rue d'Estienne d'Orves
92700 Colombes, FR

(72) Inventor/es:

GOYET, CHRISTOPHE

(74) Agente/Representante:

PÉREZ BARQUÍN, Eliana

DESCRIPCIÓN

Entidad electrónica con medios de comunicación por contacto y a distancia

La invención se refiere a una entidad electrónica con unos medios de comunicación por contacto y unos medios de comunicación a distancia, un terminal de comunicación con una entidad electrónica de ese tipo, así como unos procedimientos de control y de personalización de esta entidad electrónica.

Una entidad electrónica, tal como por ejemplo una tarjeta de microcircuitos, que incluye en general unos circuitos electrónicos adecuados para memorizar unas informaciones, posee unos medios de comunicación con el exterior, particularmente con el fin de intercambiar unas informaciones guardadas por la entidad electrónica con unos dispositivos exteriores, del tipo lector o terminal.

Entre los medios de comunicación utilizados normalmente, se distinguen unos medios de comunicación por contacto, para los que un contacto físico entre la entidad electrónica y el terminal es una condición necesaria para el establecimiento de la comunicación, y los medios de comunicación a distancia, gracias a los que una comunicación entre la entidad electrónica y un lector es posible sin contacto físico entre estos dos elementos, con un alcance del orden de algunos centímetros en general.

Ciertas entidades electrónicas reagrupan por otro lado unos medios de comunicación de los dos tipos antes citados, en cuyo caso los modos de funcionamiento "*por contacto*" y "*sin contacto*" se pueden organizar según las funcionalidades requeridas del aparato para cada uno de los modos de comunicación, como se describe por ejemplo en las patentes US 5206495 y US 5999713.

Si la utilización de unos medios de comunicación sin contacto es conocida por su practicidad (debido al hecho de que no es necesaria ninguna colocación precisa de la entidad electrónica para el intercambio de informaciones), tiene sin embargo el inconveniente de un riesgo de intercambio intempestivo de informaciones, como por ejemplo mediante el establecimiento de una comunicación no deseada por el usuario durante su paso por la proximidad del lector. Este problema es particularmente sensible cuando la entidad electrónica guarda unas informaciones confidenciales, como por ejemplo en el caso de un pasaporte electrónico.

Se ha buscado por lo tanto ya en la técnica anterior tomar unas medidas para evitar este intercambio intempestivo de datos, a veces aludidos bajo el vocablo anglosajón de "*anti-skimming*".

En este orden de ideas, se ha propuesto en la solicitud de patente WO 99/16019 disponer un interruptor sobre la cara superior de una tarjeta de microcircuitos para hacer posible la recepción de datos por esta tarjeta solamente después de la activación del interruptor. La adición de un interruptor de ese tipo sobre la entidad electrónica posee sin embargo unos problemas de realización y de fiabilidad (por ejemplo en caso de flexión repetida de la entidad electrónica tal como se define por la norma ISO7816) e incrementa su coste de fabricación.

Esta es probablemente la razón por la que se ha propuesto en la patente US 6424029 utilizar un interruptor del tipo capacitivo, mejor adaptado a la constitución general de las entidades electrónicas portadoras de informaciones, en particular en el caso de las tarjetas de microcircuitos. Aunque esta solución reduce las dificultades a las que se acaba de aludir, no consigue evitarlas totalmente.

Además, las soluciones que acaban de ser recordadas carecen de flexibilidad y no permiten particularmente concebir una limitación del acceso al modo de comunicación sin contacto, por ejemplo mediante una palabra clave.

Se conoce igualmente por la solicitud de patente EP 1258831 una tarjeta de microcircuitos con una interfaz de contactos y con una interfaz sin contactos en la que la interfaz a utilizar se determina en función del tipo de datos a intercambiar. El preámbulo de la reivindicación 1 se conoce de este documento.

En este contexto, la invención propone una entidad electrónica según la reivindicación 1. Comprendiendo esta entidad electrónica unos medios de comunicación por contacto y unos medios de comunicación a distancia, se caracteriza por unos medios para autorizar un intercambio de ciertos datos, al menos a través de los medios de comunicación a distancia, en función de la recepción previa de una instrucción a través de los medios de comunicación por contacto.

La posibilidad de intercambiar los datos mediante los medios de comunicación a distancia puede generarse también por medio del enlace por contacto, por ejemplo por medio de un terminal.

El intercambio de datos referido por la autorización es por ejemplo la emisión de ciertos datos al menos y/o la recepción de ciertos datos al menos.

Según un primer modo de realización concebible, la entidad electrónica comprende igualmente unos medios de memorización de una información de activación controlados mediante dicha instrucción y unos medios para autorizar

el intercambio (emisión y/o recepción) de dichos datos a través de los medios de comunicación a distancia en presencia de dicha información de activación.

Se puede separar de ese modo la recepción de la instrucción y el intercambio (por ejemplo la emisión) de los datos, por ejemplo en el plano temporal.

La entidad electrónica puede comprender igualmente de manera complementaria unos medios para inhibir el intercambio de dichos datos a través de los medios de comunicación a distancia en ausencia de dicha información de activación.

Cuando los medios de comunicación a distancia comprenden una antena, dichos medios para utilizar un intercambio comprenden, según un modo de realización que puede concebirse, unos medios para controlar una conexión de la antena a un microcircuito en base a dicha instrucción. La autorización y la inhibición del intercambio (esto es por ejemplo la emisión y/o la recepción) son entonces particularmente eficaces.

La entidad electrónica es por ejemplo una tarjeta de microcircuitos de acuerdo con la norma ISO14443 y/o con la norma ISO7816.

La invención propone igualmente un terminal que comprende unos medios de comunicación por contacto con una entidad electrónica que comprende unos medios de comunicación a distancia, caracterizada por unos medios para emitir, a través de los medios de comunicación por contacto, una instrucción destinada a condicionar un intercambio de al menos ciertos datos a través de los medios de comunicación a distancia.

Un terminal de ese tipo puede generar la autorización de intercambio por los medios de comunicación a distancia de la entidad electrónica. El intercambio referido por la autorización puede ser una emisión y/o una recepción de datos.

Un terminal de ese tipo puede ser portátil: puede tratarse particularmente de un terminal portátil ad hoc que permite generar la autorización de intercambio por los medios de comunicación a distancia de la entidad electrónica.

La invención propone además un procedimiento de control de una entidad electrónica según la reivindicación 4. Este procedimiento que comprende unos medios de comunicación por contacto y unos medios de comunicación sin contacto, se caracteriza por las etapas siguientes:

- recepción de una instrucción de activación a través de los medios de comunicación por contacto;

- realización de una autorización de intercambio de ciertos datos al menos a través de los medios de comunicación a distancia con la recepción de dicha instrucción de activación.

La posibilidad de intercambiar los datos a través de los medios de comunicación a distancia está controlada de ese modo por la instrucción de activación, con las ventajas ya mencionadas.

En este procedimiento, una etapa de intercambio (emisión y/o recepción) de dichos datos a través de los medios de comunicación a distancia está condicionada por ejemplo por dicha autorización.

Según un modo posible de realización, la autorización se realiza mediante la puesta a un valor predeterminado de una información de activación y dicha etapa de emisión condicionada comprende las etapas siguientes:

- verificación de que el valor de la información de activación es igual al valor predeterminado;

- intercambio (por ejemplo emisión) de dichos datos a través de los medios de comunicación a distancia solamente en caso de verificación positiva.

Este procedimiento es práctico de realizar y posee las ventajas ya mencionadas en términos de separación de la autorización y del intercambio.

El intercambio puede comprender igualmente una etapa de puesta de la información de activación a un valor complementario del valor predeterminado en un instante determinado.

Según otro modo posible de realización, el procedimiento comprende una etapa de inhibición del intercambio de dichos datos en un instante determinado.

El instante determinado puede corresponder a la recepción de un control de fin de comunicación por los medios de comunicación a distancia, lo que permite a la instrucción no autorizar más que una única comunicación.

El instante determinado se puede determinar mediante una temporización, lo que permite limitar la duración de la autorización en el tiempo.

El instante determinado se pueda alcanzar después de la recepción de un número predeterminado de comandos a través de los medios de comunicación a distancia, lo que permite limitar las posibilidades de utilización de la autorización.

El instante determinado puede corresponder a la terminación de una etapa de inicialización de la comunicación.

La invención propone finalmente un procedimiento de personalización de la entidad electrónica que comprende los medios de comunicación sin contacto, caracterizado por una etapa de escritura de una información de activación destinada a condicionar el intercambio de al menos ciertos datos a través de los medios de comunicación a distancia.

Se puede determinar de ese modo durante la personalización de la entidad electrónica si la utilización de los medios de comunicación sin contacto estará autorizada por omisión.

Dicha información de activación puede modificarse por otro lado con la recepción de una instrucción a través de los medios de comunicación por contacto de la entidad electrónica. Se trata por ejemplo de una instrucción de seguridad.

Este procedimiento puede comprender además una etapa de escritura de la información de configuración representativa de las condiciones de modificación de la información de activación. Se puede configurar de ese modo a la entidad electrónica en lo que concierne a las posibilidades de utilizar los medios de comunicación a distancia durante la personalización, en función de su utilización posterior, sin que esto implique modificaciones de los circuitos utilizados.

Surgirán otras características y ventajas de la invención a la luz de la descripción que sigue, realizada con referencia a los dibujos adjuntos en los que:

- la figura 1 representa un primer ejemplo de una entidad electrónica según las enseñanzas de la invención;

- la figura 2 es un diagrama lógico que ilustra el funcionamiento general de la entidad electrónica de la figura 1;

- la figura 3 representa un segundo ejemplo de una entidad electrónica según las enseñanzas de la invención;

- la figura 4 representa un ejemplo posible de constitución física de la entidad electrónica de la figura 3;

- la figura 5 es un diagrama lógico que describe una primera parte del funcionamiento de la entidad electrónica de la figura 3;

- la figura 6 es un diagrama lógico que ilustra una segunda parte del funcionamiento de la entidad electrónica de la figura 3.

El ejemplo de entidad electrónica representado en la figura 1 comprende un microcircuito 2 (por ejemplo un microcontrolador de seguridad tal como se utiliza habitualmente en las tarjetas de chips) adecuado para comunicar con otros dispositivos electrónicos por medio, por un lado, de contactos 4, estando cada contacto unido a un borne del microcircuito y, por otro lado, por medio de una antena magnética 6, formada por ejemplo por el arrollamiento de una pluralidad de espiras.

La antena magnética 6 está conectada a dos bornes del microcircuito con interposición de un interruptor K controlado por un borne de control CMD del microcircuito 2. De ese modo, con el comando de una señal generada en el borne CMD, el microcircuito puede controlar la conexión de la antena 6 al microcircuito 2, y por ello autorizar o inhibir la utilización de los medios de comunicación a distancia de los que esta antena 6 forma parte.

Se va a describir ahora, con referencia a la figura 2, el funcionamiento general de este dispositivo.

Inicialmente se observará que, en este modo de realización, la entidad electrónica no está alimentada eléctricamente más que cuando se conecta mediante sus medios de comunicación por contacto (conjunto de contactos 4) a un dispositivo exterior del tipo terminal, lo que asegura una conexión eléctrica con cada uno de sus contactos 4 y permite de ese modo particularmente la alimentación eléctrica de la entidad electrónica.

El interruptor eléctrico K es entonces por ejemplo de tal modo que está abierto en ausencia de alimentación eléctrica (y particularmente por ejemplo en ausencia de señal en el borne CMD), aunque los medios de comunicación a distancia, que comprenden la antena 6, no pueden utilizarse mientras que la entidad electrónica no esté conectada (por medio de los contactos 4) al terminal que asegura su alimentación: en el presente modo de realización, la entidad electrónica no está prevista para funcionar sobre la única base de una tele-alimentación suministrada por la antena 6.

El esquema general del funcionamiento de la entidad electrónica de la figura 1 comienza entonces durante la conexión de esta entidad electrónica a un terminal (a través de los contactos 4), lo que provoca la inicialización de la comunicación entre la entidad electrónica (es decir el microcircuito 2) y el terminal (por ejemplo unos medios del tipo microcircuito en este terminal), como se ha representado en la etapa E2 de la figura 2.

Durante la etapa de inicialización, se efectúa particularmente un comando del interruptor K de manera que éste esté en la posición abierta, lo que permite inhibir la comunicación sin contacto como se ha explicado anteriormente. El control de la apertura del interruptor K se efectúa mediante el microcircuito 2 colocando el borne CMD al potencial que provoca la apertura del interruptor K, por ejemplo un potencial que represente un nivel lógico 0.

La entidad electrónica puede tener entonces un funcionamiento normal en el modo “contactos”, en el curso de la que se procede por ejemplo a un intercambio de datos entre la entidad electrónica y el terminal al que está conectada (etapa E4).

En el curso de estos intercambios de datos, la entidad electrónica puede recibir particularmente una instrucción que autorice la comunicación en el modo sin contacto, como se ha representado en la etapa E6.

Una instrucción de este tipo es por ejemplo un código de operación particular cuando el microcircuito 2 de la entidad electrónica está controlado en su funcionamiento por dichos códigos recibidos desde el terminal. Como variante, podrá tratarse de un dato (tal como por ejemplo un código secreto introducido por el usuario en el terminal) cuya exactitud será interpretada por el microcircuito 2 como una instrucción que autoriza la comunicación en modo “*sin contacto*”.

Con la recepción de esta instrucción durante la etapa E6, el microcircuito controla en la etapa E8 el cierre del interruptor K (por ejemplo haciendo pasar al borne CMD a un potencial que corresponde al nivel lógico 1); de ese modo, la antena 6 se conecta en sus dos extremos al microcircuito 2, lo que hace posible la comunicación de la entidad electrónica con un dispositivo exterior a través de esta antena 6, es decir a través de los medios de comunicación sin contacto.

En el presente modo de realización, como se describe más adelante, el cierre del interruptor K durará hasta el fin de una comunicación a través de los medios de comunicación sin contacto. Como variante, la comunicación sin contacto podría no autorizarse más que para una duración predeterminada (temporización al fin de la que el potencial sobre el borne CMD vuelve a pasar al nivel lógico 0). Se pueden concebir igualmente otras variantes como se explica a propósito del segundo modo de realización.

Una vez cerrado el interruptor K, la entidad electrónica es apta para establecer una comunicación sin contacto con un lector destinado a este fin (asociado o no al terminal de comunicación por contacto), como se representa en la etapa E10, lo que permite el intercambio de datos en modo “*sin contacto*” entre la entidad electrónica y el lector, como se indica en la figura 2 por la etapa E12.

Al final del diálogo en el modo sin contacto entre la entidad electrónica y el lector, es decir cuando estos dos dispositivos han procedido a los intercambios de datos previstos, la entidad electrónica recibe una instrucción “*fin de transacción*”, tal como por ejemplo una instrucción “*DESELECT*” definida según la norma ISO1443-4, como se ha representado en la etapa E14.

Con la recepción de una instrucción de este tipo, el microcircuito 2 controla la apertura del interruptor K (poniendo, en el ejemplo descrito en este caso, a un nivel lógico 0 al borne CMD), lo que provoca la inhibición de la comunicación sin contacto debido al hecho de que la antena 6 no está ya conectada al microcircuito 2, como se ha representado en la etapa E16.

Como se ha indicado ya, la inhibición de la comunicación sin contacto (en este caso por medio de la apertura del interruptor K) podría como variante intervenir bajo otras condiciones, tal como una cierta duración a partir de la autorización de esta comunicación, la salida de la entidad electrónica del campo del lector, u otra, como se menciona igualmente más adelante.

El funcionamiento se reinicia entonces en la etapa E4 mediante la gestión del modo “*contacto*”.

Se observa que el modo de realización que acaba de ser descrito es particularmente ventajoso cuando un lector que funciona a distancia debe comunicar con la entidad electrónica incluso aunque ésta esté igualmente conectada a un terminal que funcione por contacto. Se puede tratar por ejemplo de una tarjeta de microcircuitos insertada en un terminal adaptado de un vehículo durante el paso de éste sobre un pórtico provisto con un lector que funciona a distancia. El intercambio de datos entre la entidad electrónica y el lector a distancia (por ejemplo para la apertura de una barrera y/o el pago de un peaje) puede estar sometido de ese modo a unas condiciones particulares generadas por el terminal en contactos colocados en el vehículo, tal como por ejemplo la introducción de un código secreto por el usuario en este terminal o un interruptor de control en el volante.

Se describirá ahora un segundo modo de realización de la invención con referencia a las figuras 3 a 6.

La figura 3 representa los elementos principales de la entidad electrónica según este modo de realización: esta entidad electrónica comprende un microcircuito 12 (por ejemplo un microprocesador) que puede estar conectado a un dispositivo exterior del tipo terminal por medio de contactos 14, con el fin de establecer una comunicación del tipo "*por contacto*" entre la entidad electrónica y este terminal.

La entidad electrónica comprende igualmente una antena 16 conectada en cada uno de sus extremos a un borne correspondiente del microcircuito 12 (sin que esté previsto interrumpir las conexiones entre la antena 16 y el microcircuito 12, contrariamente al primer modo de realización descrito anteriormente).

La antena 16 forma parte de los medios de comunicación a distancia de la entidad electrónica.

Se conecta igualmente una memoria que pueda reescribirse 18 (por ejemplo una memoria no volátil del tipo memoria que puede borrarse y programarse electrónicamente, generalmente denominada mediante el acrónimo anglosajón EEPROM) al microcircuito 12.

Se observará que, en este modo de realización, el microcircuito 12 se puede alimentar a través de la conexión por contactos (a través de al menos uno de los contactos 14) o, independientemente de esta primera posibilidad de alimentación, mediante una tele-alimentación que utilice la antena magnética 16 (y esto contrariamente al primer modo de realización). La utilización del modo de comunicación "sin contacto" no estará en este caso condicionada por lo tanto por la utilización simultánea de la conexión por contacto (a través de los contactos 14).

La entidad electrónica podrá por lo tanto ser alimentada o bien mediante la conexión por contacto, o bien por la tele-alimentación, lo que da lugar a dos modos principales de funcionamiento descritos respectivamente en las figuras 5 y 6; una alimentación simultánea mediante la alimentación por contacto y la tele-alimentación es posible naturalmente sin cuestionar los principios de funcionamiento de los dos modos descritos anteriormente.

Durante una comunicación de la entidad electrónica con un terminal a través de los contactos 14, el procedimiento ilustrado en la figura 5 se realiza bajo el control del microcircuito 12 (por ejemplo programado por medio de instrucciones almacenadas en la memoria).

Previamente, por ejemplo durante una etapa de inicialización de los datos almacenados en la entidad electrónica (tal como por ejemplo la etapa de personalización clásicamente utilizada en la fabricación de las tarjetas de microcircuitos antes de su envío al mercado), se pone a 0 un bit de activación almacenado por ejemplo en la memoria que puede reescribirse 18, lo que permite indicar que, por omisión, está inhibida una comunicación a distancia (como se describirá en detalle más adelante).

Durante la etapa de personalización, se puede prever igualmente la escritura de la información de configuración que indica (por ejemplo en la forma de derechos de acceso al archivo en el que se memoriza el bit de activación) en qué medida la utilización de los medios de comunicación a distancia de la entidad electrónica se podrá autorizar a través de la conexión por contacto, a saber, por ejemplo:

- en todo momento, por ejemplo dejando acceso libre al archivo que contiene el bit de activación (el programa de control de la entidad electrónica puede en este caso condicionar sin embargo la emisión a la entrada de un código secreto como se describe más adelante);

- después de una autentificación del lector (o del portador de la tarjeta que coincida eventualmente con un código en el lector), lo que constituye una variante del modo de realización descrito después para no autorizar la utilización de los medios de comunicación a distancia más que a los usuarios autentificados;

- jamás, por ejemplo prohibiendo el acceso al fichero que contiene el bit de activación, lo que hace imposible la modificación de éste para autorizar eventualmente la utilización de los medios de comunicación sin contacto.

Se sitúa a continuación el caso en el que el acceso al bit de activación es libre con respecto al programa de control de la entidad electrónica.

En un cierto punto de funcionamiento del modo "*contactos*" (en el que el microcircuito 12 está alimentado por el terminal e intercambia los datos con éste por medio de los contactos 14), el microcircuito podrá recibir del terminal una instrucción de activación de la comunicación sin contacto, es decir un dato (o más generalmente una información) que trate de controlar la autorización de un funcionamiento en modo "*sin contacto*" a través de la antena 16, como se ha explicado con referencia a la figura 6 (etapa E20).

En el ejemplo descrito en este caso, un código suministrado por el usuario (por ejemplo por medio de un teclado) al terminal se transmite en asociación con la instrucción de activación de manera que la autorización del

funcionamiento del modo sin contacto no sea efectiva más que en presencia del código correcto suministrado por el usuario, es decir de un código predeterminado y almacenado (eventualmente en una forma protegida) en la memoria que pueda reescribirse 18 asociada al microcircuito 12 (o en otra memoria, del tipo memoria no volátil, asociada a este microcircuito 12).

Después de haber recibido la instrucción de activación acompañada del código suministrado por el usuario, el microcircuito 12 procede a una etapa E22 de verificación de la exactitud del código suministrado, es decir en la práctica la comparación del código suministrado con el código memorizado en la entidad electrónica, como ya se ha mencionado.

Si el código suministrado corresponde correctamente al código secreto memorizado en la entidad electrónica, la autorización de una comunicación sin contacto se hace efectiva mediante la colocación a 1 en la etapa E24 del bit de activación mencionado anteriormente, lo que significa que la entidad electrónica ha recibido efectivamente una información de activación de la comunicación sin contacto correcta.

Al contrario, si el código suministrado por el usuario, que se transmite a la entidad electrónica con la instrucción de activación en la etapa E20, no es el código memorizado por ésta, se procede en la etapa E26 a la puesta a 0 del bit de activación en la memoria que puede reescribirse 18, lo que significa que entonces se considera que ninguna información de activación correcta ha sido recibida.

En los dos casos, el bit de activación se modifica por ejemplo mediante una instrucción del tipo "*UPDATE BINARY*" (definida por la norma ISO7816-4) después de la selección del archivo que contiene este bit de activación mediante un comando del tipo "*SELECT*".

Se puede remarcar que, en el caso anteriormente mencionado en el que el bit de activación se pone a 0 durante una etapa de inicialización, no es necesaria la etapa E26 puesto que no cambia *a priori* el valor del bit de activación. Sin embargo puede desearse utilizarla, por ejemplo para asegurar que cualquier utilización de un código correcto conduce a la puesta a 0 del bit de activación incluso si el código correcto se ha suministrado en una fase precedente. Por otro lado, en presencia o no de la etapa E26, la recepción de un código incorrecto podría conducir a otras consecuencias, como por ejemplo la emisión de un mensaje de error de la tarjeta, con destino en el terminal a través de los contactos 14.

Además, aunque con un objetivo de concisión se haya descrito una única etapa de verificación de la exactitud del código sin precisar si era posible repetir o no esta etapa, por supuesto se puede concebir la posibilidad de dejar al usuario un número limitado de tentativas de introducción del código secreto correcto, con la consecuencia por ejemplo del bloqueo de la entidad electrónica cuando el número limitado de tentativas se ha agotado y el código siempre es erróneo.

El modo de funcionamiento "*sin contacto*" se describirá ahora con referencia a la figura 6. Como se indica a continuación, este modo de funcionamiento se desencadena mediante la introducción de la entidad electrónica en el alcance de un lector a distancia, tanto si se ha procedido o no previamente a las etapas de la figura 5 dirigidas a activar el enlace sin contacto.

Durante la entrada de la entidad electrónica en el campo del lector (etapa E30), la entidad electrónica se tele-alimenta (lo que puede ser visto como una detección del lector por parte de la entidad electrónica) y el microcircuito 12 comienza su funcionamiento en el modo "*sin contacto*".

Al comienzo de este funcionamiento (preferentemente durante unas primeras etapas del programa ejecutado por el microcircuito 13, por ejemplo durante la realización de los programas de inicialización y de anticolisión, tales como los definidos en la norma ISO14443-3), el microcircuito 12 procede a la lectura en la memoria que puede reescribirse 18 del bit de activación (etapa E32).

Se puede proceder entonces en la etapa E34 a una verificación del valor del bit de activación (que, como ya se ha indicado, es indicativo de una información de activación de la comunicación sin contacto).

Si el bit de activación está a 0 (o bien porque este valor ha sido inscrito durante la inicialización de la entidad electrónica y no ha sido modificado por la recepción de una instrucción de activación correcta, o bien porque este bit ha sido repuesto a 0 a continuación de la introducción de un código erróneo o de la realización previamente del intercambio de datos autorizados sin que se haya suministrado una nueva autorización), se pone fin en la etapa E36 a la comunicación sin contacto, en la que sólo las primeras etapas habrían sido realizadas sin que esto implique un intercambio de datos.

Al contrario, si se verifica por parte del microcircuito 12 que el bit de activación memorizado en la memoria que puede reescribirse 18 está en el valor 1 (es decir que se está en presencia de una información de activación), se procede a proseguir con la realización de la comunicación sin contacto, a saber inicialmente a una inicialización del protocolo de enlace sin contacto en la etapa E38 (por ejemplo según la norma ISO14443-4 con el fin de llegar a un

nivel de ejecución del protocolo “*Half-Duplex Block Transmission Protocol*”).

Una vez establecida la comunicación sin contacto (por ejemplo después de la etapa E38), se procede a la puesta a 0 del bit de activación en la memoria que puede rescribirse 18, como se representa por la etapa E40 en la figura 6. La realización de la etapa E40 después de la inicialización del protocolo permite asegurar que la entidad electrónica no será autorizada a establecer una nueva comunicación sin contacto después de haber salido del campo del lector (salvo que reciba una nueva instrucción de activación por medio del enlace por contacto).

Sin embargo, como ya se ha aludido, la puesta a 0 del bit de activación (es decir la inhibición del establecimiento de una nueva comunicación sin contacto) podría intervenir bajo otras condiciones, tales como por ejemplo una temporización con relación al momento de la recepción de la instrucción de activación (o eventualmente con relación al establecimiento del enlace sin contacto), la ejecución de un número predeterminado de instrucciones por el microcircuito 12 (o de comandos APDU “*Application Protocol Data Unit*”) o la recepción del mensaje de fin de transacción (como era el caso en el primer modo de realización).

Según otra variante, se puede concebir que el bit de activación no sea repuesto a 0 durante su funcionamiento en el modo sin contacto, sino más bien con la recepción de una instrucción de desactivación en el modo “contactos”. Una instrucción de ese tipo de desactivación podría preverse por otro lado incluso para el caso en el que el bit de activación sea repuesto a 0 durante el funcionamiento sin contacto (como por ejemplo se describe en la figura 6).

En el ejemplo descrito, una vez inicializado el protocolo en la etapa E38, y aunque el bit de activación sea repuesto a 0 en la etapa E40, se procede a continuación a un intercambio de datos según el protocolo sin contacto en una etapa E42. Se observará sin embargo que, cuando el intercambio de datos de la etapa E42 haya terminado, por ejemplo mediante la salida de la entidad electrónica del campo del lector, o como variante con la recepción de éste de un comando que pone fin a la comunicación sin contacto, habiendo sido repuesto a 0 el bit de activación por la etapa E40, una nueva interacción de las etapas E30 a E34 mediante el retorno de la entidad electrónica en el campo del lector conducirá a un fracaso de la comunicación sin contacto por el paso a la etapa E36.

En el modo de realización que acaba de ser descrito, el bit de activación (utilizado como indicador de la recepción previa de una instrucción de activación correcta) condiciona el conjunto de los intercambios de datos en el modo sin contacto. Como variante, se podría prever que este bit de activación no condicione más que el intercambio de ciertos datos particulares de la entidad electrónica, mientras que otros datos podrían comunicarse libremente por la entidad electrónica durante su paso cerca de un lector a distancia, incluso si no se ha recibido ninguna instrucción específica previamente mediante el enlace por contacto.

De ese modo, cuando la entidad electrónica es un documento de identificación electrónico, se puede prever que ciertos datos presentes en el documento (como el nombre de la persona relacionada) se comuniquen sin necesitar previamente la activación de la autorización particular, mientras que la emisión de otros datos (por ejemplo las informaciones confidenciales de tipos de datos biométricos - huellas digitales, iris o imagen facial) no podrían ser emitidas por la entidad electrónica a través del enlace sin contactos más que a condición de que la entidad electrónica haya recibido previamente una instrucción válida de activación en este sentido por medio del enlace por contacto.

En este caso, la presencia de la información de activación (es decir el valor 1 del bit de activación) no condicionará el establecimiento del enlace sin contacto propiamente dicho, sino de ciertas etapas de emisión de los datos confidenciales.

Se puede prever entonces por ejemplo que la instrucción de activación no corresponda a la autorización de emitir más que una sola vez estos datos, es decir que el bit de activación sería entonces repuesto a 0 inmediatamente después de la emisión de los datos confidenciales.

Según una variante, se puede prever que la información de activación condicione la recepción de datos a través del enlace sin contacto. Se puede evitar así por ejemplo que un código de identificación se presente a la entidad electrónica a través del enlace sin contacto por un tercero malintencionado, a espaldas del portador autorizado de la entidad electrónica, con el riesgo por ejemplo de bloquear la entidad electrónica a continuación de la presentación de varios códigos falsos por este tercero.

Por otro lado, los datos relacionados con la autorización de intercambio no están necesariamente limitados a los datos de aplicación de la entidad electrónica (es decir, particularmente a los datos transportados por la entidad electrónica en su función de soporte de información), sino que pueden incluir igualmente unos datos de otro tipo, tales como los datos que permitan el establecimiento de un protocolo de comunicación.

Los modos de realización que se acaban de dar, con las variantes concebidas, no constituyen más que unos ejemplos posibles de realización de la invención que no se limita por ello.

REIVINDICACIONES

1. Entidad electrónica que comprende:

- unos medios de comunicación por contacto (4; 14);

- unos medios de comunicación sin contacto (6; 16);

- una memoria no volátil que puede reescribirse adecuada para memorizar una información de activación;

caracterizada por:

- unos medios de puesta a un valor predeterminado de la información de activación con la recepción de la instrucción a través de los medios de comunicación por contacto;

- unos medios (12) para autorizar un intercambio de ciertos datos al menos a través de los medios de comunicación sin contacto solamente en presencia del valor predeterminado de dicha información de activación.

2. Entidad electrónica según la reivindicación 1, caracterizada por unos medios para inhibir el intercambio de dichos datos a través de los medios de comunicación sin contacto en ausencia del valor predeterminado de dicha información de activación.

3. Entidad electrónica según la reivindicación 1 o 2, caracterizada por que es una tarjeta de microcircuitos.

4. Procedimiento de control de una entidad electrónica que comprende unos medios de comunicación por contacto y unos medios de comunicación sin contacto, caracterizada por una memoria no volátil que puede reescribirse adecuada para memorizar una información de activación y por las etapas siguientes:

- recepción de una instrucción de activación (E20) a través de los medios de comunicación por contacto;

- realización de una autorización de intercambio (E24) de ciertos datos al menos a través de los medios de comunicación sin contacto, mediante la puesta a un valor predeterminado (E24) de dicha información de activación, con la recepción de dicha instrucción de activación;

- verificación (E34) de que el valor de la información de activación es igual al valor predeterminado;

- intercambio de dichos datos (E38, E42) a través de los medios de comunicación sin contacto solamente en caso de verificación de la igualdad.

5. Procedimiento según la reivindicación 4, caracterizado por una etapa de puesta de la información de activación a un valor complementario (E40) del valor predeterminado en un instante determinado.

6. Procedimiento según la reivindicación 5, caracterizado por que el instante determinado corresponde a la recepción de un comando de fin de comunicación (E14) por los medios de comunicación sin contacto.

7. Procedimiento según la reivindicación 5, caracterizado por que el instante determinado se determina mediante una temporización.

8. Procedimiento según la reivindicación 5, caracterizado por que el instante determinado se alcanza después de la recepción de un número predeterminado de comandos a través de los medios de comunicación sin contacto.

9. Procedimiento según la reivindicación 5, caracterizado por que el instante determinado corresponde a la terminación de una tapa de inicialización (E38) de la comunicación.

10. Procedimiento según una de las reivindicaciones 4 a 9, en el que se transmite un código a través de los medios de comunicación por contacto y en el que dicha autorización de intercambio es efectiva si el código transmitido corresponde al código memorizado en la entidad electrónica.

11. Procedimiento según la reivindicación 10, en el que la instrucción de activación se recibe acompañada del código transmitido.

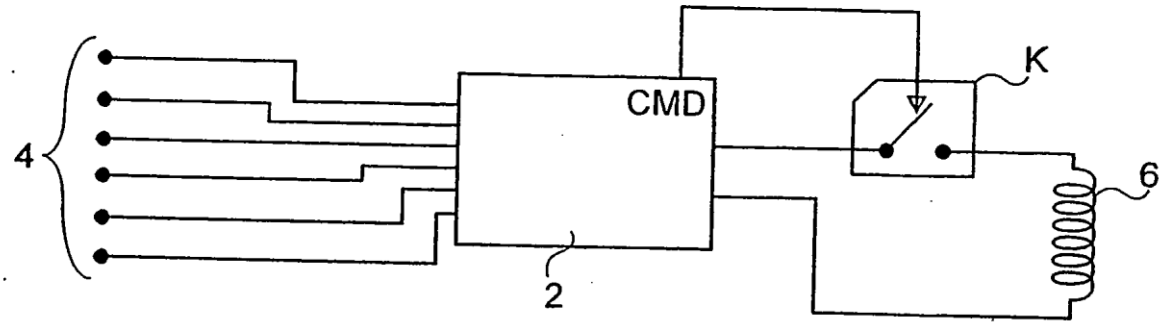

Fig. 1

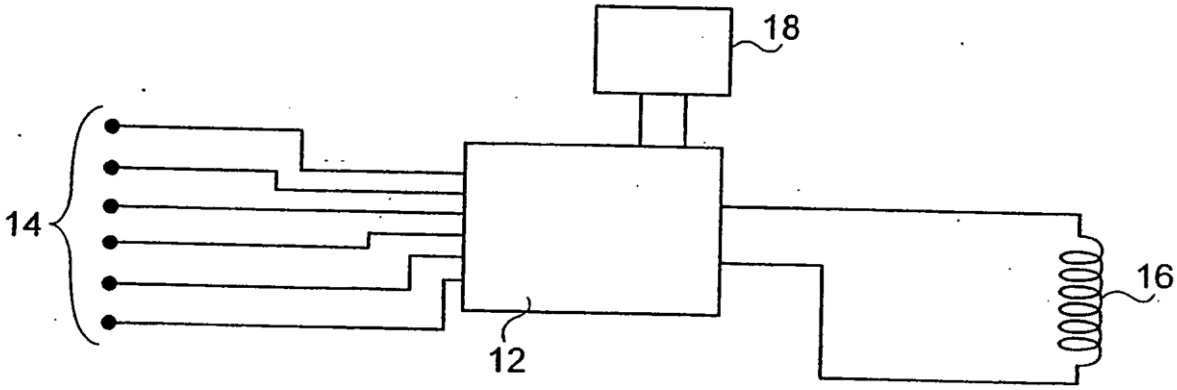

Fig. 3

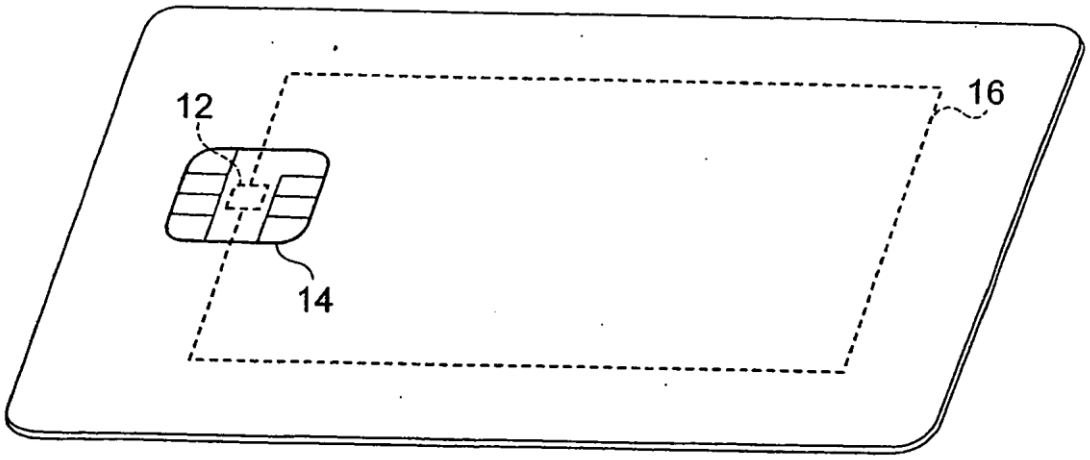

Fig. 4

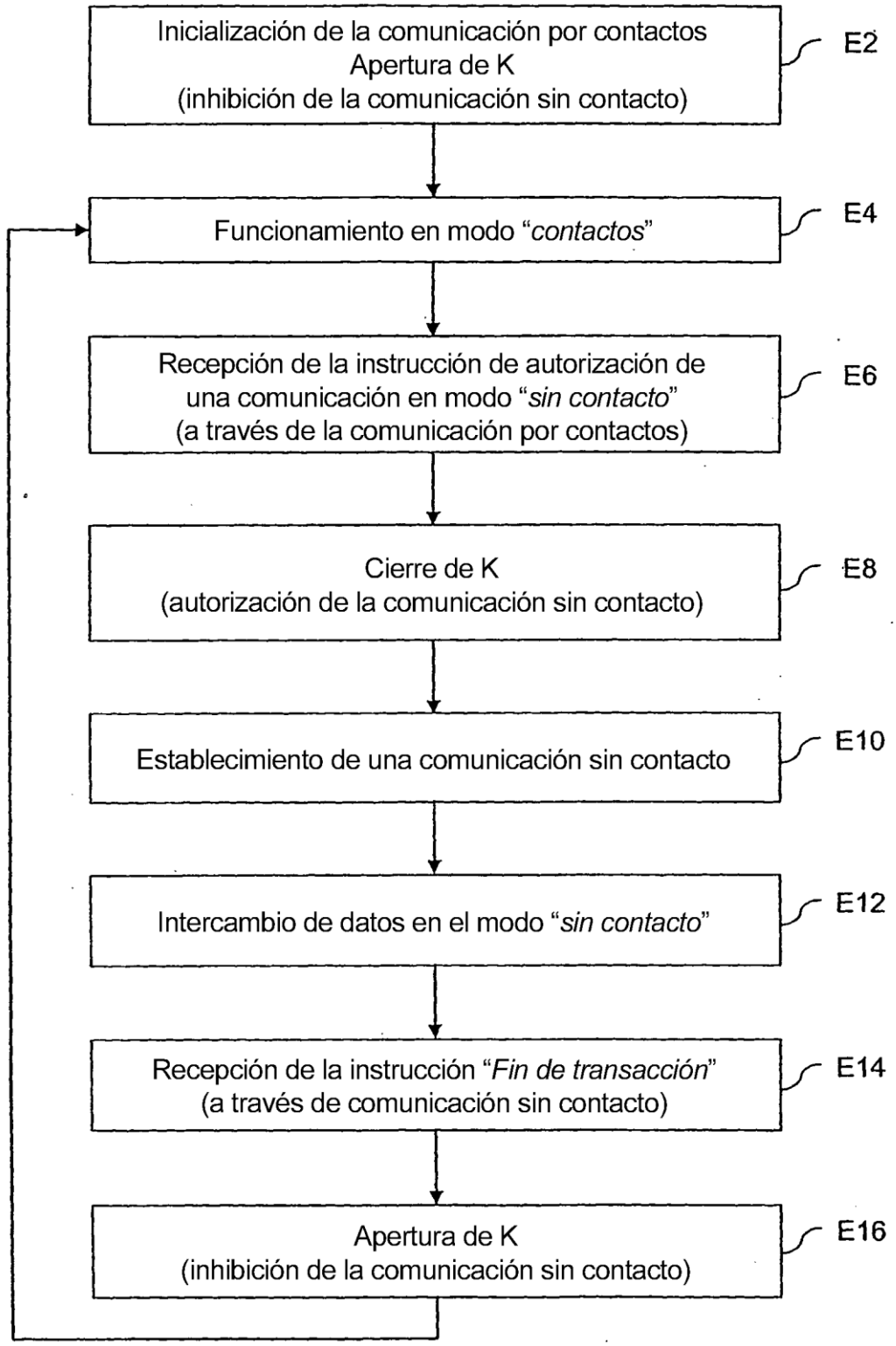
Inicialización de la comunicación por contactos
Apertura de K
(inhibición de la comunicación sin contacto)
E2
Funcionamiento en modo "*contactos*"
E4
Recepción de la instrucción de autorización de una comunicación en modo "*sin contacto*" (a través de la comunicación por contactos)
E6
Cierre de K
(autorización de la comunicación sin contacto)
E8
Establecimiento de una comunicación sin contacto
E10
Intercambio de datos en el modo "*sin contacto*"
E12
Recepción de la instrucción "*Fin de transacción*" (a través de comunicación sin contacto)
E14
Apertura de K
(inhibición de la comunicación sin contacto)
E16

Fig.2

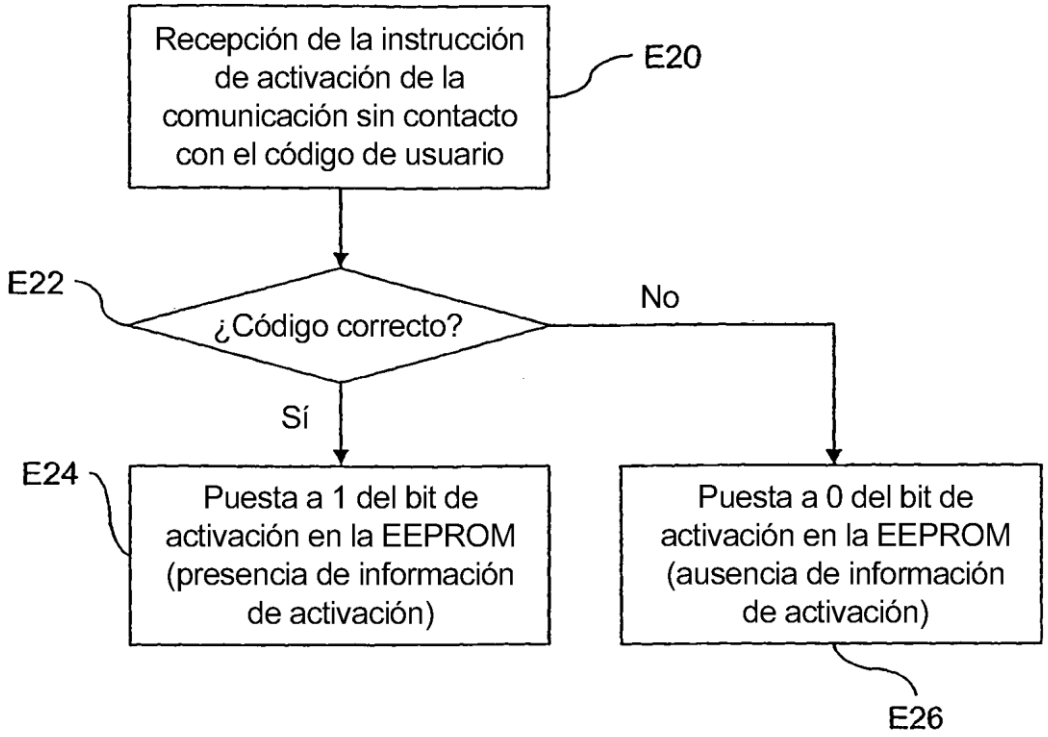
Recepción de la instrucción de activación de la comunicación sin contacto con el código de usuario
E20
E22
¿Código correcto?
No
Sí
E24
Puesta a 1 del bit de activación en la EEPROM (presencia de información de activación)
Puesta a 0 del bit de activación en la EEPROM (ausencia de información de activación)
E26

Fig.5

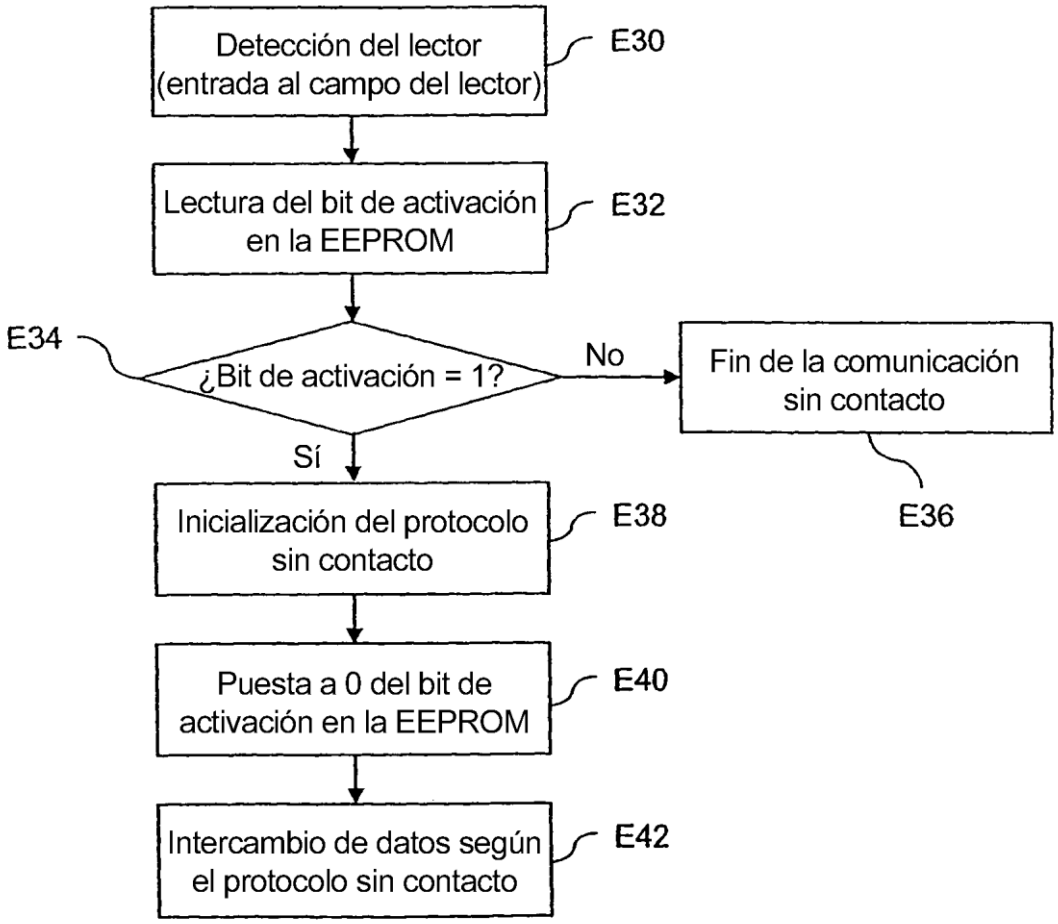
Detección del lector (entrada al campo del lector)
E30
Lectura del bit de activación en la EEPROM
E32
E34
¿Bit de activación = 1?
No
Fin de la comunicación sin contacto
E36
Sí
Inicialización del protocolo sin contacto
E38
Puesta a 0 del bit de activación en la EEPROM
E40
Intercambio de datos según el protocolo sin contacto
E42

Fig.6