

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 663 795**

51 Int. Cl.:

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 12159987 (2)**

97 Fecha y número de publicación de la concesión europea: **27.12.2017** **EP 2490159**

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:

17.04.2018

73 Titular/es:

IDEMIA FRANCE (100.0%)
420, rue d'Estienne d'Orves
92700 Colombes, FR

72 Inventor/es:

GOYET, M. CHRISTOPHE

74 Agente/Representante:

LEHMANN NOVO, María Isabel

ES 2 663 795 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).

DESCRIPCION

Entidad electrónica con medios de comunicación por contacto y a distancia

La invención se refiere a una entidad electrónica con medios de comunicación por contacto y medios de comunicación a distancia, más precisamente a un procedimiento de personalización de esta entidad electrónica.

5 Una entidad electrónica, tal como por ejemplo una tarjeta de microcircuito, que incluye en general circuitos electrónicos aptos para memorizar informaciones, posee medios de comunicación con el exterior, con el fin particularmente de intercambiar informaciones retenidas por la entidad electrónica con los dispositivos exteriores, del tipo lector o terminal.

10 Entre los medios de comunicación corrientemente utilizados, se distinguen los medios de comunicación por contacto, para los cuales un contacto físico entre la entidad electrónica y el terminal es una condición necesaria para el establecimiento de una comunicación, y los medios de comunicación a distancia, gracias a los cuales 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.

15 Algunas entidades electrónicas reagrupan por otro lado los medios de comunicación de los dos tipos anteriormente citados, en cuyo caso los modos de funcionamiento "por contacto" y "sin contacto" pueden ser organizados según las funcionalidades requeridas del aparato para cada uno de los modos de comunicación, como se describe por ejemplo en las patentes US 5 206 495 y US 5 999 713.

20 Aunque la utilización de los medios de comunicación sin contacto es conocida por su practicidad (debido a que ningún posicionamiento preciso de la entidad electrónica es necesario para el intercambio de informaciones), la misma tiene no obstante el inconveniente de un riesgo de intercambio intempestivo de informaciones, por ejemplo, por el establecimiento de una comunicación no deseada por el usuario en su paso cerca de un lector. Este problema es particularmente sensible cuando la entidad electrónica guarda informaciones confidenciales, como por ejemplo en el caso de un pasaporte electrónico.

25 Por consiguiente, se ha buscado ya en la técnica anterior tomar medidas para evitar este intercambio intempestivo de datos, a veces aludidos bajo el vocablo anglosajón "anti-skimming".

30 En este orden de ideas, ha sido propuesto en la solicitud de patente WO 99/16019 disponer un interruptor en la superficie superior de una tarjeta de microcircuito para hacer posible la recepción de datos mediante esta tarjeta solamente después de la activación del interruptor. El aporte de un interruptor de este tipo en la entidad electrónica plantea sin embargo 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) y aumenta su coste de fabricación.

Es probablemente el motivo por el cual ha sido propuesto en la patente US 6 424 029 utilizar un interruptor del tipo capacitivo, mejor adaptado para la constitución general de las entidades electrónicas portadoras de informaciones, en particular en el caso de las tarjetas de microcircuito. Aunque esta solución reduce las dificultades que acaban de mencionarse, la misma no llega a evitarlas en su totalidad.

35 Además, las soluciones que acaban de ser recordadas carecen de flexibilidad y no permiten particularmente considerar una limitación del acceso en el modo de comunicación sin contacto, por ejemplo, mediante contraseña.

La solicitud de patente DE 199 08 285 describe la carga de datos de personalización en una tarjeta de microcircuito a través de los contactos de la tarjeta.

40 La solicitud de patente WO 98/37526 describe una tarjeta multiaplicación en la cual se consultan los datos de personalización memorizados en la tarjeta con el fin de determinar si una aplicación puede ser cargada en ella.

En este contexto, se describe a continuación un procedimiento conforme a la reivindicación 1.

La posibilidad de intercambiar los datos por los medios de comunicación a distancia puede así ser gestionada por medio de la conexión por contacto, por ejemplo, por medio de un terminal.

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

La entidad electrónica comprende igualmente medios de memorización de una información de activación controlados por la indicada instrucción y medios para permitir el intercambio (emisión y/o recepción) de los indicados datos a través de los medios de comunicación a distancia en presencia de la indicada información de activación.

50 Se pueden así separar 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 igualmente comprender de forma complementaria medios para inhibir el intercambio de los indicados datos a través de los medios de comunicación a distancia en ausencia de la indicada información de

activación.

La entidad electrónica es por ejemplo una tarjeta de microcircuito conforme a la norma ISO14443 y/o a la norma ISO7816.

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

Según un modo posible de realización, puede existir una etapa de inhibición del intercambio de los indicados datos en un momento determinado.

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

10 El momento determinado puede estar determinado por una temporización, lo cual permite limitar la duración de la autorización en el tiempo.

El momento determinado puede ser alcanzado después de la recepción de un número predeterminado de controles por los medios de comunicación a distancia, lo cual permite limitar las posibilidades de utilización de la autorización.

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

15 Se trata por ejemplo de una instrucción de seguridad.

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

20 Otras características y ventajas de la invención aparecerán a la luz de la descripción que sigue, realizadas con referencia a los dibujos adjuntos en los cuales:

- la figura 1 representa un ejemplo de una entidad electrónica según las enseñanzas de la invención;
- la figura 2 representa un ejemplo posible de constitución física de la entidad electrónica de la figura 1;
- la figura 3 es un ordinograma que describe una primera parte del funcionamiento de la entidad electrónica de la figura 1;
- la figura 4 es un diagrama lógico que ilustra una segunda parte del funcionamiento de la entidad electrónica de la figura 1.

La figura 1 representa los elementos principales de una entidad electrónica: esta entidad electrónica comprende un microcircuito 12 (por ejemplo, un microprocesador) que puede ser conectado con 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 con un borne correspondiente del microcircuito 12.

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

35 Una memoria reescribible 18 (por ejemplo, una memoria no volátil del tipo de memoria borrable y programable electrónicamente, generalmente denominada por el acrónimo anglosajón EEPROM) está igualmente conectada al microcircuito 12.

Se apreciará que, en este modo de realización, el microcircuito 12 puede ser alimentado a través de la conexión por contactos (por medio al menos uno de los contactos 14) o, independientemente de esta primera posibilidad de alimentación, por una alimentación a distancia utilizando la antena magnética 16. La utilización del modo de comunicación "sin contacto" no estará por consiguiente condicionada por la utilización simultánea de la conexión por contacto (a través de los contactos 14).

La entidad electrónica podrá por consiguiente ser alimentada bien sea por la conexión mediante contacto, o por alimentación a distancia, lo cual da lugar a dos modos principales de funcionamiento descritos respectivamente en las figuras 3 y 4; una alimentación simultánea mediante la alimentación por contacto y la alimentación a distancia es naturalmente posible sin cuestionar de nuevo los principios de funcionamiento de los dos modos descritos anteriormente.

En una comunicación de la entidad electrónica con un terminal a través de los contactos 14, el procedimiento ilustrado en la figura 3 es puesto en práctica bajo el control del microcircuito 12 (por ejemplo, programado por medio de instrucciones almacenadas en memoria).

Previamente, en una etapa de inicialización de los datos almacenados en la entidad electrónica, a saber, la etapa de

personalización utilizada en la fabricación de tarjetas con microcircuito antes de su puesta en el mercado, se pone a 0 un bitio de activación almacenado por ejemplo en la memoria reescribible 18, lo cual permite indicar que, por omisión, una comunicación a distancia ha sido inhibida (como se describirá en detalle más adelante).

En la etapa de personalización, se puede igualmente prever la escritura de una información de configuración que indica (por ejemplo, bajo la forma de derechos de acceso al archivo en el cual está memorizado el bitio de activación) en qué medida la utilización de los medios de comunicación a distancia de la entidad electrónica podrá ser autorizada por medio de la conexión por contacto, a saber, por ejemplo:

- en cualquier momento, por ejemplo, dejando libre acceso al archivo que contiene el bitio de activación (el programa de control de la entidad electrónica que puede no obstante en este caso condicionar la emisión a la introducción de un código secreto como se ha descrito más adelante);
- después de una autenticación del lector (o del portador de la tarjeta que introduce eventualmente un código en el lector), lo cual constituye una variante del modo de realización descrito a continuación para permitir solo la utilización de los medios de comunicación a distancia a los usuarios autenticados;
- nunca, por ejemplo, impidiendo el acceso al archivo que contiene el bitio de activación, lo cual hace imposible la modificación de éste para permitir eventualmente la utilización de los medios de comunicación sin contacto.

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

En un cierto punto del funcionamiento en modo “*contactos*” (en el cual el microcircuito 12 es alimentado por el terminal e intercambia datos con éste por medio de los contactos 14), el microcircuito puede recibir del terminal una instrucción de activación de la comunicación sin contacto, es decir, un dato (o más generalmente una información) que trata 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 4 (etapa E20).

En el ejemplo descrito aquí, un código proporcionado por el usuario (por ejemplo por medio de un teclado) al terminal es transmitido en asociación con la instrucción de activación de forma que la autorización del funcionamiento en modo “*sin contacto*” solo sea efectiva en presencia del código correcto proporcionado por el usuario, es decir por un código predeterminado y almacenado (eventualmente en forma protegida) en la memoria reescribible 18 asociada con el microcircuito 12 (o en otra memoria, del tipo de almacenamiento de solo lectura, asociada con este microcircuito 12).

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

Si el código proporcionado corresponde con el código secreto memorizado en la entidad electrónica, la autorización de una comunicación sin contacto se hace efectiva por la puesta en 1 en la etapa E24 del bitio de activación anteriormente mencionado, lo cual significa que la entidad electrónica ha recibido efectivamente una información de activación de la comunicación sin contacto correcta.

Al contrario, si el código proporcionado por el usuario es transmitido 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 bitio de activación en la memoria reescribible 18, lo que significa que se considera entonces que ninguna información de activación correcta ha sido recibida.

En los dos casos, el bitio de activación es por ejemplo modificado por una instrucción del tipo “*UPDATE BINARY*” (definida por la norma ISO7816-4) después de la selección del archivo que contiene este bitio de activación por un comando del tipo “*SELECT*”.

Se puede observar que, puesto que el bitio de activación es puesto a 0 en la etapa de inicialización, la etapa E26 no es necesaria, ya que no cambia a priori el valor del bitio de activación. Se puede sin embargo desear utilizarla, por ejemplo, para asegurarse que toda utilización de un código incorrecto conduce a la puesta a 0 del bitio de activación incluso si el código correcto ha sido indicado en una fase anterior. 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 destinado al terminal por medio de los contactos 14.

Además, aunque con un fin de concisión haya sido descrita una sola etapa de comprobación de la exactitud del código sin precisar si era posible repetir o no esta etapa, se puede desde luego considerar de dejar al usuario un número limitado de intentos de introducción del código secreto correcto, teniendo por consecuencia por ejemplo el bloqueo de la entidad electrónica cuando el número limitado de intentos se ha agotado y el código todavía es erróneo.

El modo de funcionamiento “*sin contacto*” se describirá ahora en referencia a la figura 4. Como se indica en lo que sigue, este modo de funcionamiento se activa por la introducción de la entidad electrónica en el soporte de un lector

a distancia, que haya sido precedido o no antes a las etapas de la figura 3 que tratan de activar la conexión sin contacto.

En la introducción de la entidad electrónica en el campo del lector (etapa E30), la entidad electrónica es alimentada a distancia (lo cual puede ser visto como una detección del lector por la entidad electrónica) y el microcircuito 12 comienza su funcionamiento en modo "sin contacto".

Al comienzo de este funcionamiento (de preferencia en las primeras etapas del programa ejecutado por el microcircuito 13, por ejemplo, en la puesta en práctica de los programas de inicialización y de anti-colisión, tales como los definidos en la norma ISO14443-3), el microcircuito 12 procede a la lectura en la memoria reescribible 18 del bitio de activación (etapa E32).

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

Si el bitio de activación se encuentra en 0 (bien sea porque este valor haya sido inscrito en la inicialización de la entidad electrónica y no haya sido modificado por la recepción de una instrucción de activación correcta, o bien porque este bitio ha sido repuesto a 0 como consecuencia de la introducción de un código erróneo o en la realización previa de un intercambio de datos autorizado sin que una nueva autorización haya sido proporcionada), se pone fin a la etapa E36 a la comunicación sin contacto, en las que solo las primeras etapas habrían sido así realizadas sin que eso implique un intercambio de datos.

Al contrario, si se ha comprobado por el microcircuito 12 que el bitio de activación memorizado en la memoria reescribible 18 está en el valor 1 (es decir que se está en presencia de una información de activación), se procede a la continuación de la realización de la comunicación sin contacto, a saber primeramente a una inicialización del protocolo de conexión sin contacto en la etapa E38 (por ejemplo según la norma ISO14443-4 con el fin de llegar al nivel de la ejecución del protocolo "*Half-Duplex Block Transmission Protocol*").

Una vez la comunicación sin contacto establecida (por ejemplo, después de la etapa E38), se procede a la puesta a 0 del bitio de activación en la memoria reescribible 18, como se ha representado por la etapa E40 en la figura 4. 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 sido retirada del campo del lector (salvo para recibir una nueva instrucción de activación por medio de la conexión por contacto).

Sin embargo, como ya se ha mencionado, la puesta a 0 del bitio de activación (es decir, la inhibición del establecimiento de una nueva comunicación sin contacto) podría producirse en 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 de la conexión sin contacto), la ejecución de un número predeterminado de instrucciones por el microcircuito 12 (o de controles APDU "*Application Protocol Data Unit*" o la recepción de un mensaje de fin de transacción (como era el caso en el primer modo de realización).

Según otra variante, se puede considerar que el bitio de activación no sea repuesto a 0 en el funcionamiento en modo sin contacto, sino más bien en recepción de una instrucción de desactivación en modo "*contactos*". Una instrucción de desactivación de este tipo podría por otro lado estar prevista incluso para el caso en que el bitio de activación sea repuesto a 0 en el funcionamiento sin contacto (como por ejemplo se ha descrito en la figura 4).

En el ejemplo descrito, una vez inicializado el protocolo en la etapa E38 y aunque el bitio de activación sea repuesto a 0 en la etapa E40, se procede seguidamente a un intercambio de datos según el protocolo sin contacto en una etapa E42. Se observará no obstante que, cuando el intercambio de datos de la etapa E42 se haya terminado, por ejemplo por la extracción de la entidad electrónica del campo del lector, o en variante con la recepción de éste de un comando que pone fin a la comunicación sin contacto, el bitio de activación que ha sido repuesto a 0 por la etapa E40, una nueva iteración de las etapas E30 a E34 por el retorno de la entidad electrónica al 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 describirse, el bitio de activación (utilizado como indicador de la recepción previa de una instrucción de activación correcta) condiciona el conjunto de los intercambios de datos en modo sin contacto. En variante, se podría prever que este bitio de activación condicione solo el intercambio de algunos datos particulares de la entidad electrónica, mientras que otros datos podrían ser libremente comunicados por la entidad electrónica en su paso por un lector a distancia, incluso si ninguna instrucción específica ha sido recibida por la conexión por contacto antes.

Así, cuando la entidad electrónica es un documento de identificación electrónico, se puede prever que algunos datos presentes en el documento (como el nombre de la persona relacionada) sean comunicados sin necesitar antes la activación de una autorización particular, mientras que la emisión de otros datos (por ejemplo las informaciones confidenciales del tipo de datos biométricos – huellas digitales, iris o imagen facial) no podrán ser emitidas por la entidad electrónica por medio de la conexión sin contacto más que con la condición de que la entidad electrónica haya antes recibido una instrucción válida de activación en este sentido por medio de la conexión por contacto.

En este caso, la presencia de una información de activación (es decir el valor 1 del bitio de activación) no

condicionará el establecimiento de la conexión sin contacto propiamente dicha, sino algunas etapas de emisión de los datos confidenciales.

5 Puede entonces estar previsto por ejemplo que la instrucción de activación no corresponda con la autorización de emitir una sola vez estos datos, es decir que el bitio de activación sería entonces repuesto a 0 inmediatamente después de la emisión de los datos confidenciales.

10 Según una variante (que puede ser eventualmente combinada con el modo de realización que acaba de describirse), se puede prever que la información de activación condicione la recepción de datos por medio de la conexión sin contacto. Se puede así evitar por ejemplo que un código de identificación sea presentado a la entidad electrónica por medio de la conexión 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 como consecuencia de la presentación de varios códigos falsos por este tercero.

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

Los modos de realización que acaban de darse, con las variantes consideradas, solo constituyen ejemplos posibles de realización de la invención que no se limita a los mismos.

REIVINDICACIONES

1. Procedimiento de personalización de una entidad electrónica que comprende medios de comunicación sin contacto (16) y medios de comunicación por contacto (14), caracterizado por una etapa de escritura en esta entidad electrónica de una información de activación destinada a condicionar el intercambio de algunos datos al menos a través de los medios de comunicación sin contacto (16) con un valor que inhibe dicho intercambio, siendo la indicada información de activación apta para ser modificada a la recepción de al menos una instrucción de activación a través de los medios de comunicación por contacto (14), no pudiendo los indicados datos ser intercambiados por los medios de comunicación sin contacto más que con la condición de que la indicada instrucción de activación haya sido recibida por medio de los medios de comunicación por contacto.
- 5 2. Procedimiento según la reivindicación 1, que comprende una etapa de escritura de una información de configuración representativa de las condiciones de modificación de la información de activación.
3. Procedimiento según la reivindicación 1 o 2, en el cual la información de activación es apta para ser modificada si un código recibido con la indicada instrucción de activación corresponde con un código memorizado en la entidad electrónica.
- 15 4. Procedimiento según la reivindicación 3, en el cual la entidad electrónica se bloquea si el código recibido es todavía erróneo después de un número predeterminado de intentos.
5. Procedimiento según la reivindicación 1 o 2, en el cual la entidad electrónica comprende un programa de control apto para modificar la información de activación si un código recibido con la indicada instrucción de activación corresponde con un código memorizado en la entidad electrónica.
- 20 6. Procedimiento según la reivindicación 5, en el cual el programa es apto para bloquear la entidad electrónica si el código recibido es todavía erróneo después de un número predeterminado de intentos.
7. Procedimiento según una de las reivindicaciones 1 a 6, en el cual la información de activación es apta para ser modificada después de la autenticación de un lector en comunicación con la entidad electrónica.
8. Procedimiento según una de las reivindicaciones 1 a 6, caracterizado por que la entidad electrónica es una tarjeta de microcircuito.
- 25 9. Procedimiento según la reivindicación 8, en el cual la información de activación es apta para ser modificada después de la autenticación del portador de la tarjeta de microcircuito.
10. Procedimiento según una de las reivindicaciones 1 a 9, caracterizado por que la información de activación modificada es apta para permitir la comunicación sin contacto.
- 30 11. Procedimiento según una de las reivindicaciones 1 a 10, caracterizado por que la entidad electrónica es una tarjeta de microcircuito conforme a la norma ISO14443
12. Procedimiento según una de las reivindicaciones 1 a 11, caracterizado por que la entidad electrónica es una tarjeta de microcircuito conforme a la norma ISO7816.

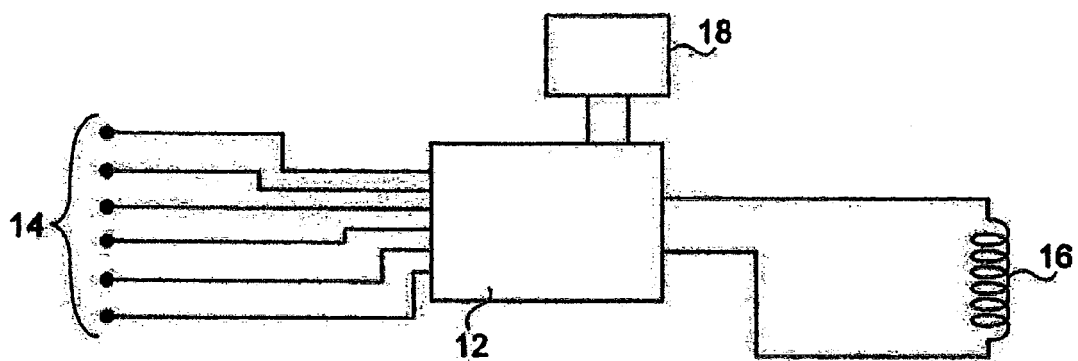


Fig. 1

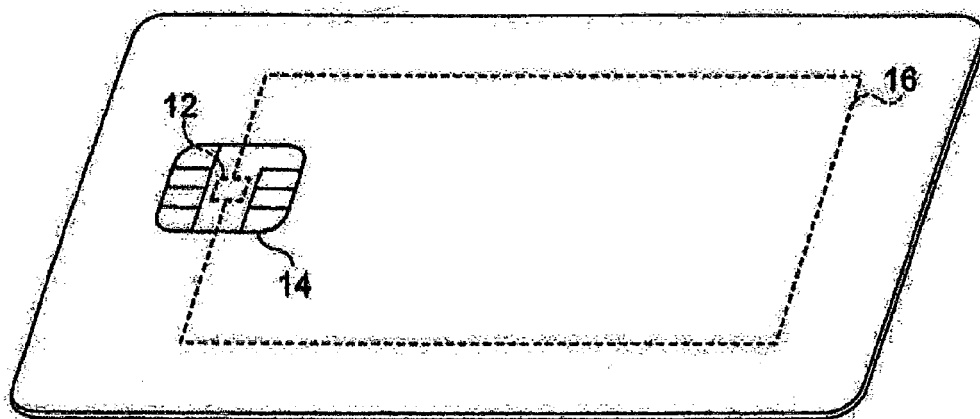


Fig. 2

