(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 566 669**

(51) Int. CI.:

G06Q 20/34 (2012.01)
G06Q 20/40 (2012.01)
G07C 9/00 (2006.01)
G07F 7/10 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **07.03.2005 E 05706811 (6)**

(97) Fecha y número de publicación de la concesión europea: **13.01.2016 EP 1725995**

(54) Título: **Tarjeta de crédito y sistema de activación de datos protegidos**

(30) Prioridad:

08.03.2004 EP 04075705
17.11.2004 EP 04078148
02.12.2004 US 1641

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.04.2016

(73) Titular/es:

CARDLAB APS (100.0%)
Lyskær 3 EF
2730 Herlev, DK

(72) Inventor/es:

NORDENTOFT, TORSTEN;
SKERN, BJORN y
ANDERSEN, PER BIRGER

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Tarjeta de crédito y sistema de activación de datos protegidos

La presente invención se refiere a una tarjeta de crédito que comprende un cuerpo de tarjeta, que comprende unos medios de lectura de huellas dactilares que proporcionan unas señales de huellas dactilares representativas de al menos una huella dactilar de un usuario de tarjeta, cuando al menos un dedo de dicho usuario se presiona contra dichos medios de lectura de huellas dactilares; unos medios portadores de datos que mantienen al menos unos datos de huellas dactilares de propietario de tarjeta y unos datos protegidos; una zona de lectura; unos medios de autenticación de huellas dactilares que comprenden un procesador de datos, que es capaz de autenticar dichas señales de huellas dactilares con dichos datos de huellas dactilares de propietario de tarjeta; y una fuente de alimentación eléctrica que suministra energía eléctrica a al menos dichos medios de lectura de huellas dactilares, dichos medios de autenticación de huellas dactilares y dicha zona de lectura. Una tarjeta de crédito de este tipo se desvela en la solicitud de patente internacional WO 01/52204.

Las tarjetas de crédito en los términos de la presente invención comprenden cualquier tarjeta provista de unos medios portadores de datos que transportan unos datos a protegerse destinados solo al uso del propietario de la tarjeta. Las tarjetas de crédito de este tipo incluyen tarjetas inteligentes, en las que se almacenan dichos datos protegidos en un circuito integrado, y en tarjetas de banda magnética, en las que los datos protegidos se almacenan en una banda magnética. Estas tarjetas de crédito se usan actualmente para diferentes aplicaciones, tales como tarjetas de identidad o licencias de conducción para fines de identificación y tarjetas de crédito o de transferencia de dinero para transportar los datos para su uso en las transferencias de dinero en, por ejemplo, los cajeros automáticos (ATM) como los cajeros de efectivo o las instalaciones de pago, en los que se requiere que el titular de la tarjeta de crédito deje ir la tarjeta de crédito durante un cierto tiempo de inserción de ATM, mientras que la tarjeta de crédito está leyéndose y reteniéndose, o los sistemas de pago automatizados, o fijos o móviles, por ejemplo, los dispositivos de lectura para el comercio por Internet y similares, en los que se requiere al titular de la tarjeta de crédito la retención de dicha tarjeta de crédito, mientras se realiza un movimiento de barrido de la misma en un lector de tarjetas de crédito.

Estas tarjetas de crédito, en general, llamadas tarjetas de plástico, han ganado gran popularidad en las últimas décadas como un medio por el que se paga el dinero de compra y los negocios se tratan sin necesidad de llevar dinero en efectivo o soportar un depósito en garantía a largo plazo u otros medios para transferir un título o garantizar el pago de dinero en efectivo. Con la popularidad y la aceptación inmediata de las tarjetas de crédito en el mundo de los negocios, el uso de las mismas por personas sin escrúpulos para hacer una transacción no autorizada se ha convertido en un problema grave que cuesta a los consumidores millones de dólares al año. A medida que la demanda de este tipo de tarjetas de crédito ha aumentado entre los ladrones de tarjetas, los falsificadores y otros usos ilegales, la demanda del mercado de tarjetas obtenidas indebidamente se ha disparado creando de este modo un incentivo extremadamente alto para que estos individuos sucumban a la tentación.

Ya que las tarjetas de identidad pueden transportar datos sensibles en relación con un propietario de tarjetas de crédito individual, estas tarjetas se han desarrollado también en transportar los datos para protegerse de los individuos que tienen la intención de un uso indebido de dichos datos.

Tales tarjetas de crédito con datos sensibles que requieren una identificación personal son relativamente fáciles de copiar o de hacer un mal uso, especialmente las tarjetas de crédito de banda magnética han demostrado gran facilidad para copiarse. Se han realizado muchos esfuerzos en el pasado para hacer frente al problema de proteger más dichas tarjetas de crédito, incluyendo la codificación de las mismas para comprobar en el punto de compra si la tarjeta de crédito puede ser una tarjeta de crédito robada o copiada.

Una forma de proteger dichos datos se ha concentrado en la asignación de tarjetas de crédito con números de código de identificación multi-digito individuales, por ejemplo, los números de identificación personal o PIN, que el usuario de la tarjeta de crédito debe mantener en secreto y usar en el número de código de identificación que comprueba el ATM. Un usuario de tarjeta de crédito que transporta varias tarjetas de crédito de diferentes proveedores de tarjetas de crédito tendrá que recordar y aprender de memoria, en estos casos, diversos números de código de identificación, lo que es a menudo difícil, especialmente si el usuario está transportando muchas de estas tarjetas de crédito. En consecuencia, y en contra del asesoramiento del proveedor de la tarjeta de crédito, algunos usuarios anotan sus números de código de identificación en las proximidades de sus tarjetas de crédito, a menudo transportándose en los bolsillos o en la billetera que transporta las tarjetas de crédito.

Si un ladrón de tarjetas de crédito ha tenido acceso tanto a una tarjeta de crédito como al número de código de identificación correspondiente, por ejemplo, robando una cartera que contiene tales efectos, éstos proporcionan un fácil acceso al dinero en efectivo en un ATM o a las mercancías en almacenamientos y tiendas, a menudo, incluso antes de que el propietario de la tarjeta de crédito tenga tiempo de cancelar sus tarjetas de crédito, o pueden proporcionar al ladrón el acceso a la información personal y a los servicios no destinados al mismo.

En otro esfuerzo, el documento EP 1 326 196 A1 desvela una tarjeta inteligente para su uso junto con un portal de seguridad, tal como un portal de tránsito o una instalación de estacionamiento para realizar la comprobación de

autenticación para el paso autorizado. Los sensores de patrones de huellas dactilares en la tarjeta generan unas señales de patrón de impresión, que se compara con las versiones auténticas almacenadas en una memoria en la tarjeta, usando un procesador localizado en la tarjeta, y el resultado de esto se comunica con el portal de seguridad externo asociado.

La patente de Estados Unidos N.º 6.325.285 desvela una tarjeta inteligente con un lector de huellas dactilares integrado, una CPU y una memoria con el fin de realizar la verificación del usuario de tarjeta y basándose en esta verificación permitir el acceso a los datos protegidos en dicha tarjeta.

Un inconveniente es que este tipo de tarjetas de crédito requiere un sistema externo, un ATM o similares, que esté especialmente adaptado para comunicarse con una tarjeta de crédito de este tipo con el fin de activarla en el ATM. Por otra parte, estas tarjetas de crédito biométricas con datos protegidos almacenados en una banda magnética no son adecuados para los sistemas de pago automático que requieren una rápida transferencia de la tarjeta de crédito a través de un lector de tarjetas, por ejemplo, los dispositivos móviles, ya que no hay suficiente tiempo para una autenticación de la tarjeta de crédito durante la comunicación con el lector de tarjetas.

Por lo tanto, es un objeto de la presente invención proporcionar una tarjeta de crédito por autenticación de huellas dactilares, que mejore la seguridad de los datos protegidos que se transportan por dicha tarjeta realizando una de cualquier autenticación de huellas dactilares independiente del sistema externo y que la tarjeta de crédito no requiera ningún cambio en los dispositivos de lectura de tarjetas existentes, tales como los ATM y similares, y como tales puedan usarse directamente con las mismas.

En la solicitud de patente internacional WO 01/52204 se desvela una tarjeta de crédito que comprende una unidad de comunicación para comunicarse con una unidad externa y que pueda activarse por un lector de huellas dactilares y un procesador. En una realización, el procesador puede instruirse para generar la información de señal magnética apropiada para una banda magnética, de manera que la tarjeta puede leerse después de la activación, pero no se desvela información relativa a cómo generar tal información de señal magnética apropiada para la banda magnética, lo que hace difícil proporcionar un campo magnético homogéneo para una comunicación eficaz de los datos protegidos a un lector de tarjetas de crédito.

Otras referencias relevantes son los documentos WO 01/31577, US 2002/032657, WO 00/49561, EP 0994439, US 2004/133787, EP 1231562 y US 7278025.

En consecuencia, por lo tanto, es otro objeto de la presente invención proporcionar una tarjeta de crédito que mejore la seguridad de dichos datos protegidos mejorando la comunicación de datos entre dicha tarjeta de crédito y un lector de tarjetas de crédito.

Estos objetos se logran en un primer aspecto de la invención por una tarjeta de crédito de acuerdo con la reivindicación 1.

En consecuencia, se logra un tiempo controlable, fiable y por lo tanto una comunicación de datos eficaz mediante la emisión electromagnética de señales de datos protegidos por dicha tarjeta de crédito, en la que el procesador de datos provoca la emisión de dichas señales de datos protegidos desde dicha al menos una bobina de transductor. Por lo tanto, los datos protegidos solo están disponibles para un lector de tarjetas de crédito después de la autenticación por dichos medios de autenticación de huellas dactilares y durante la emisión de dichas señales de datos protegidos, lo que resulta en una mejora sustancial de la seguridad de dichos datos protegidos. Proporcionando una tarjeta de crédito de acuerdo con la invención, la fabricación se simplifica y la tarjeta de crédito puede producirse en masa en gran número. Además, la física y aún más importante el aspecto electro-magnético de la bobina de transductor es sustancialmente igual que la de una banda magnética convencional, lo que resulta en que dicha tarjeta de crédito puede utilizarse con los lectores de tarjetas de crédito actualmente disponibles para las lecturas de bandas magnéticas. Una selección adecuada del material del núcleo para las bandas de núcleo influye fuertemente en la fuerza y en la distribución homogénea del campo magnético que se produce. Esto proporciona una mejora de dicho campo magnético, lo que resulta en un consumo de energía eléctrica inferior de dicha tarjeta de crédito, cuando se crea dicho campo magnético, lo que prolonga el tiempo de vida de dicha tarjeta de crédito. Además, no hay necesidad de una fuente de alimentación eléctrica externa, y por lo tanto los sistemas convencionales existentes, tales como lectores de tarjetas de identificación y los lectores de transferencia de dinero, puede usarse junto con dichas tarjetas de crédito, es decir, las inversiones en nuevos sistemas de lectura convencionales no son necesarias con el fin de mejorar la seguridad de los datos transportados por la tarjeta de crédito. Una ventaja principal de dicha tarjeta de crédito de acuerdo con la presente invención es en consecuencia el hecho de que se realiza un procedimiento de autenticación automatizado completo y autónomo antes de la comunicación que se refiere a dichos datos protegidos que se establece entre dicha tarjeta de crédito y cualquiera de los lectores de tarjetas de crédito existentes en el mercado hoy en día, independientemente del tipo (ATM automatizado o de un tipo de barrido operado de manera manual), fabricante, versión, o la posición geográfica de dicho ATM y del uso de la tarjeta de crédito, es decir, el tipo de datos protegidos en la tarjeta, por ejemplo, el número del banco, el número de la seguridad social, etc.

En una realización de dicha tarjeta de crédito, dichos medios de autenticación de huellas dactilares controlan la

activación de dichos datos protegidos basándose en la autenticación de las señales de huellas dactilares comparando estas con dichos datos de huellas dactilares de propietario de tarjeta, si la comparación es una coincidencia, entonces dichos datos protegidos se activan; si no dichos datos protegidos no se activan. Una ventaja proporcionada por esta realización incluye una realización de una tarjeta de crédito de este tipo de acuerdo con la presente invención que puede protegerse sin la necesidad de usar un número de código de identificación junto con un ATM y similares. La autenticación se realiza en la tarjeta, independientemente de cualquier dispositivo externo y puede proporcionar una seguridad adicional a dicha tarjeta de crédito de acuerdo con la presente invención. Por supuesto, la combinación de una autenticación en la tarjeta y una comprobación de un número de código de identificación pueden aumentar aún más la seguridad en torno a los datos protegidos.

En otra realización de dicha tarjeta de crédito, dicha activación de dichos datos protegidos se mantiene a lo largo de un período de tiempo de activación determinado. Una de las ventajas proporcionada por esta realización incluye que el propietario de tarjetas de crédito no necesita presionar sus dedos sobre el lector de huellas dactilares durante dicho periodo de tiempo, en el que los datos protegidos se están comunicando entre la tarjeta de crédito y el dispositivo de lectura de un sistema externo. Esto permite que la tarjeta se inserte en, por ejemplo, un ATM cuya operación requiere que el usuario de la tarjeta de crédito deje ir la tarjeta de crédito durante dicho período de tiempo de comunicación. Por lo tanto, la comunicación entre los medios de lectura y la tarjeta de crédito se mejora y se aumenta la seguridad de los datos protegidos.

En una realización adicional de dicha tarjeta de crédito, la activación de los datos protegidos se realiza por la emisión de señales de datos protegidos una o varias veces consecutivas por dicha al menos una bobina de transductor. Por lo tanto, los datos protegidos están disponibles para la comunicación con cualquier unidad de lectura solo durante dicho período de tiempo de activación determinado, o como una señal de campo magnético que se genera durante la extensión de dicho período de tiempo de activación determinado o durante un período de tiempo más corto, o como varias señales consecutivas que abarcan todo el período de tiempo determinado o segmentos de las mismas. Esto aumenta aún más la seguridad de los datos protegidos en dicha tarjeta de crédito, y permite la comunicación con varios tipos de lectores de tarjetas de crédito disponibles, tales como los lectores de tarjetas de crédito de barrido o de tipo inserción.

De acuerdo con la invención, la tarjeta de crédito comprende además al menos un sensor de detección de barrido, que es capaz de hacer que dicho procesador de datos active dichos datos protegidos por la emisión de dichas señales de datos protegidos al menos una vez por dicha al menos una bobina de transductor, cuando dicha tarjeta de crédito está en las proximidades de un lector de tarjetas de crédito. En consecuencia, las señales de datos protegidos solo se emiten en el período de tiempo de activación durante el que dicha tarjeta de crédito está en las proximidades del cabezal de lector de tarjeta de crédito, lo que mejora aún más la seguridad de dichos datos protegidos. Los datos protegidos se activan inmediatamente después de que el sensor de detección de barrido ha registrado la presencia de dicho cabezal de lector, es decir, el al menos un sensor de detección de barrido permite la activación de dichos datos protegidos por dicho procesador de datos. En una realización se proporcionan dos sensores de detección de barrido, uno en cada sección de extremo de dicha al menos una bobina de transductor con el fin de proporcionar al procesador de datos una información sobre en qué extremo se inician las señales de los datos protegidos. En otra realización más, dicho al menos un sensor de detección de barrido es capaz de detectar la velocidad con la que se barre la tarjeta de crédito por un lector de tarjetas de crédito, y basándose en esta velocidad detectada el procesador de datos es capaz de determinar el período de tiempo de activación.

En una realización preferida, dicho circuito de excitación es capaz de realizar una amplificación avanzada tal como la compensación de amplitud y la conformación de pulso en dichas señales de datos protegidos. Por lo tanto, el consumo de energía se reduce, la intensidad del campo magnético resultante se reduce y la dirección de la misma se envía hacia un cabezal de lector, y la señal de datos protegidos que puede proporcionarse se presenta al cabezal de lector, por lo que se logra una tasa de transmisión de señal de datos protegidos aumentada.

En otra realización dicho circuito de excitación se proporciona de manera integral con el procesador de datos. Esto reduce el tiempo de la línea de montaje y por lo tanto el coste de producción y prevé que se usen circuitos integrados más pequeños.

En otra realización de dicha tarjeta de crédito, dicha al menos una banda de material de núcleo inducible está provista de al menos un entrehierro distribuido. Por lo tanto, se incrementa la fuerza del campo magnético que se proporciona por una tarjeta de crédito de acuerdo con la invención, lo que ayuda además a la comunicación entre dicha tarjeta de crédito y un lector de tarjetas de crédito, y disminuye la corriente necesaria, dando como resultado una disminución del consumo de energía de dicha tarjeta de crédito, cuando se inducen las señales de datos protegidos en dicha al menos una bobina de transductor, lo que prolonga el tiempo de vida de la fuente de alimentación proporcionada en dicha tarjeta de crédito.

En otra realización de dicha tarjeta de crédito, se proporciona dicho al menos un entrehierro con unas distribuciones de material que tienen diferentes capacidades de inducción electromagnética en comparación con el material de dicha al menos una banda de material de núcleo inducible. Por lo tanto, se mejora la homogeneidad del campo magnético mediante la selección apropiada del material de entrehierro, mejorando además dicha comunicación de datos.

En otra realización de dicha tarjeta de crédito, dicho al menos un devanado de núcleo se coloca sustancialmente en una sección de extremo de dicha al menos una banda de material de núcleo inducible. Las influencias destructivas del campo magnético de dichos devanados de núcleo en relación con un cabezal de lector de un lector de tarjetas de crédito se reducen de este modo considerablemente, mientras que dichas bobinas de transductor siguen manteniendo un campo magnético fuerte y homogéneo cuando se emiten dichas señales de datos protegidos.

En otra realización de dicha tarjeta de crédito, dicha tarjeta de crédito comprende además unos medios de indicación de activación para la indicación de la activación de dicha zona de lectura. Una ventaja de esta realización es que al usuario de la tarjeta se le da la posibilidad de comprobar si dichos medios de autenticación de huellas dactilares proporcionados en la tarjeta de crédito de acuerdo con la presente invención han activado dichos datos protegidos, antes de que se intente la comunicación que se establece entre la tarjeta de crédito y un dispositivo de lectura de tarjeta, por ejemplo, obtenida a través de un lector de dispositivo de pago automático. Por lo tanto, no se desperdicia el tiempo intentando insertar una tarjeta de crédito no activada en un ATM o similares, lo que resulta en una fallo de comunicación.

En otra realización más de dicha tarjeta de crédito, dicha fuente de alimentación eléctrica comprende al menos una batería. Las ventajas comprenden unas baterías planas convencionales que son de uso económico y sencillas de implementar en una tarjeta de crédito de acuerdo con la presente invención. Además, el uso de baterías limita el período de tiempo de vida útil, lo que para algunos usos de este tipo de tarjetas de crédito es una ventaja con el fin de controlar el período de tiempo de vida de la tarjeta o el número de usos de la tarjeta.

En otra realización más de dicha tarjeta de crédito, dicha fuente de alimentación eléctrica comprende al menos una batería recargable. Una de las ventajas que incluye dicha tarjeta de crédito de acuerdo con la presente invención es que puede usarse durante un período prolongado de tiempo.

En otra realización adicional más de dicha tarjeta de crédito, dicha fuente de alimentación eléctrica comprende además unos medios de recarga para dicha batería recargable. Una de las ventajas de ser una tarjeta de crédito de acuerdo con dicha realización es que es totalmente autosuficiente de energía y puede usarse durante un período de tiempo de vida prolongado.

En aún una realización adicional de dicha tarjeta de crédito, dichos medios de recarga para dicha al menos una batería recargable comprenden una disposición de células solares. Una de las ventajas de las células solares es que pueden proporcionarse en una superficie de la tarjeta de crédito que se somete a la luz antes y/o durante la operación de comunicación entre los datos protegidos y el sistema externo.

En una realización adicional de dicha tarjeta de crédito, dicho cuerpo de tarjeta comprende además unos medios de indicación de estado de fuente de alimentación. Una de las ventajas de la información de una fuente de alimentación que falla es que está disponible para el usuario de la tarjeta en el sitio sin el uso de medios externos. Por lo tanto, se mantiene al mínimo la posibilidad de detener la operación por un fallo de alimentación de la tarjeta de crédito de acuerdo con la presente invención.

En una realización adicional de dicha tarjeta de crédito, dichos medios portadores de datos incluyen un primer almacenamiento de datos para mantener los datos de huellas dactilares de propietario de tarjeta, y un segundo almacenamiento de datos para mantener los datos protegidos. De esta manera, dichos datos se guardan separados para mayor seguridad y además dichos almacenamientos de datos pueden ser medios de almacenamiento de datos convencionales lo que reduce los gastos de producción.

En unas realizaciones adicionales de dicha tarjeta de crédito, dicho almacenamiento de datos primero y/o segundo es una memoria EEPROM o de tipo FLASH, o dicho segundo almacenamiento de datos es una banda magnética o un circuito integrado de tarjeta inteligente. Una ventaja de esto es que dicho almacenamiento de datos primero y/o segundo es un medio de almacenamiento de datos convencional, lo que reduce los gastos de producción de las tarjetas de crédito y facilita la comunicación de la tarjeta de crédito con los dispositivos de lectura externos existentes en un ATM o similares.

En una realización adicional de dicha tarjeta de crédito dicho medio de autenticación de huellas dactilares y dichos medios portadores de datos se combinan en un único circuito integrado, tal como un microcontrolador con una memoria. En consecuencia, el número de componentes necesarios para la operación de una tarjeta de crédito de este tipo se mantiene bajo, lo que reduce los costes de dicha tarjeta de crédito.

En una realización adicional de dicha tarjeta de crédito, dicho único circuito integrado es capaz de ponerse en un primer estado, en el que dichos datos protegidos y dichos datos de huellas dactilares de propietario de tarjeta están disponibles de manera temporal durante una activación de dichos datos protegidos. En consecuencia, la seguridad de dichos datos protegidos se aumenta aún más, porque fuera de dicho periodo temporal los datos no están disponibles para su lectura por cualquier dispositivo de lectura o de aprovechamiento externo, que un ladrón potencial puede tener en su poder.

En una realización adicional de dicha tarjeta de crédito, dichos medios de lectura de huellas dactilares comprenden al menos un sistema de lectura de huellas dactilares. De este modo, se proporciona una posibilidad de seleccionar

un sistema de lectura de huellas dactilares específico para la activación de un conjunto asociado de datos protegidos. Además, es posible mediante la selección de una o una combinación de huellas dactilares una activación de un servicio de tarjeta de crédito proporcionado en dicha tarjeta en la forma de un conjunto de datos protegido específico. En una realización alternativa de la tarjeta de crédito comprende unos medios de selección de servicios de tarjetas de crédito, tal como, por ejemplo, un interruptor, por el que uno puede seleccionar un servicio de tarjeta de crédito seleccionando diferentes conjuntos de datos protegidos, uno para cada servicio de tarjeta de crédito disponible.

En otra realización de dicha tarjeta de crédito, dichos medios de selección de servicios de tarjetas de crédito comprenden un sistema de lectura de huellas dactilares para cada servicio de tarjeta de crédito disponible en dicha tarjeta de crédito. En consecuencia, están disponibles varios servicios de tarjetas de crédito para un propietario de tarjeta para activarse en la forma de varios conjuntos de datos protegidos, que por selección de una huella dactilar apropiada o una combinación de huellas dactilares activa un conjunto dado de datos protegidos para su lectura en dicha zona de lectura. En una realización alternativa dichos medios de selección de servicios de tarjetas de crédito comprenden un único sistema de lectura de huellas dactilares para todos los servicios de tarjetas de crédito disponibles, en los que dichos datos de huellas dactilares de propietario de tarjeta comprenden al menos una huella dactilar o una combinación de huellas dactilares que corresponden a una huella dactilar de activación para cada servicio de tarjeta de crédito, y en los que dicho procesador de datos está adaptado para la activación de la zona de lectura durante un período de tiempo de activación determinado, cuando dicha huella dactilar de activación se presiona contra dicho sistema de lectura de huellas dactilares. Por lo tanto, el número de sistemas de lectura de huellas dactilares se reduce, disminuyendo el coste de producción.

En otra realización de dicha tarjeta de crédito, dichos medios de lectura de huellas dactilares son capaces de pre-almacenar una huella dactilar de propietario de tarjeta en dichos medios portadores de datos en una operación de una sola vez. En consecuencia, los datos de identificación personales, es decir, los datos de huellas dactilares del propietario de tarjeta, se almacenan solamente una vez y solo en una localización, lo que mejora aún más la seguridad de dichos datos de identificación personales. Esto es debido al hecho de que no hay necesidad de ningún otro o registro adicional en una base de datos o portador externo a la memoria proporcionada en una tarjeta de crédito de acuerdo con la invención, y por lo tanto, no se prevé ninguna posibilidad ni de un registro central de tales datos de identificación personales como datos de huellas dactilares ni de un aprovechamiento potencial de un registro central de este tipo.

En otra realización de dicha tarjeta de crédito, dichos datos de huellas dactilares de propietario de tarjeta comprenden al menos una huella dactilar o una combinación de huellas dactilares que corresponden a una huella dactilar de desactivación, y dicho procesador de datos está adaptado para la desactivación de la zona de lectura durante un periodo de desactivación determinado, cuando dicha huella dactilar de desactivación se presiona contra dichos medios de lectura de huellas dactilares. Por lo tanto, si coaccionado por un criminal en el uso de la tarjeta de crédito biométrica para, por ejemplo, transferencias de dinero en efectivo, se proporciona a un dueño de tarjetas de crédito la oportunidad de hacer la tarjeta de crédito inoperable durante un período de tiempo más largo, por ejemplo, horas, días o meses, incluso de manera permanente con el fin de disuadir a los posibles criminales de tal coacción. Por lo tanto, los servicios proporcionados por dichos datos protegidos se han protegido aún más frente al mal uso por tales criminales.

Además, es también un objeto de la invención proporcionar un sistema de activación de datos protegidos para un portador de datos, tal como una tarjeta de crédito de acuerdo con la invención, lo que mejora la seguridad de dichos datos protegidos mejorando la comunicación de datos entre dicho portador de datos y un lector de soporte de datos.

A continuación, se describirá la tarjeta de crédito de acuerdo con la presente invención, a modo de ejemplo, con referencia a los dibujos esquemáticos, en los que:

La figura	es un diagrama de bloques de una tarjeta de crédito de acuerdo con una realización de la presente invención;
La figura 2	muestra una primera tarjeta de crédito que comprende una banda magnética;
La figura 3	muestra una segunda tarjeta de crédito que comprende un circuito integrado inteligente;
La figura 4	muestra el lado posterior de una tarjeta de crédito de acuerdo con una realización de la presente invención;
La figura 5	muestra una tarjeta de crédito de acuerdo con una realización preferida de la presente invención;
La figura 6	muestra una bobina de transductor de una tarjeta de crédito de acuerdo con la realización preferida de la presente invención en las proximidades de un lector de tarjetas de crédito, y
Las figuras 7A, 7B, 7C	muestran unas curvas de amplitud del campo magnético a lo largo de la extensión de una bobina de transductor sin una conversión DA, una curva de conversión DA resultante, y la amplitud resultante después de la adición de las dos curvas, respectivamente, como una función de la posición en la bobina de transductor.

La figura 1 muestra un diagrama de bloques esquemático de una tarjeta de crédito de acuerdo con la invención. Dicha tarjeta de crédito comprende un cuerpo 1 de tarjeta, una fuente 12 de alimentación eléctrica en la tarjeta, unos

medios 14 de lectura de huellas dactilares, unos medios 16 de autenticación de huellas dactilares que comprenden un procesador de datos, y unos medios 18 portadores de datos.

Dicha fuente 12 de alimentación eléctrica suministra corriente eléctrica a al menos unos medios 14 de lectura de huellas dactilares y en la realización mostrada en la figura 1 también a los medios 16 de autenticación de huellas dactilares usando cualquier conexión eléctrica convencional (línea continua). Obviamente, algunos o todos los componentes eléctricos de dicha tarjeta de crédito pueden estar provistos de energía eléctrica a partir de dicha fuente 12 de alimentación. Dichos medios 14 de lectura de huellas dactilares proporcionan unas señales 14s de huellas dactilares a dichos medios 16 de autenticación de huellas dactilares con el fin de permitir una comparación entre dichas señales 14a de huellas dactilares y los datos 18fd de huellas dactilares de propietario de tarjeta pre-almacenados en dichos medios 18 portadores de datos para activar los datos 18sd protegidos asimismo pre-almacenados en dichos medios 18 portadores de datos.

Dicha fuente 12 de alimentación eléctrica puede comprender ventajosamente una o más baterías recargables y/o no recargables. La fuente 12 de alimentación preferentemente comprende además unas conexiones eléctricas a los diversos componentes eléctricos proporcionados en el cuerpo de tarjeta, y, en el caso de las baterías recargables proporcionándose preferentemente unos medios de recarga, por ejemplo, unos terminales para la conexión a una batería proporcionada externamente al sistema de carga o, ventajosamente, unas células solares dispuestas en dicho cuerpo de tarjeta, estando dichos medios de recarga en comunicación eléctrica con dicha batería o baterías recargables.

Las baterías no recargables actuales son compactas, tanto en energía como en tamaño, y una o más baterías proporcionan la energía adecuada para varias lecturas de huellas dactilares y autenticaciones de acompañamiento para las operaciones de comunicaciones entre una tarjeta de crédito de acuerdo con la presente invención y un dispositivo lector de tarjetas. En algunos usos para una tarjeta de crédito de este tipo puede preferirse limitar el período de tiempo de vida de la batería en el que dicha tarjeta puede estar activa, por ejemplo, limitando el uso de una tarjeta a dos autenticaciones en un ensayo de prueba de usuario de una nueva tarjeta de este tipo.

Los medios 14 de lectura de huellas dactilares pueden comprender cualquier dispositivo convencional disponible, preferentemente un sistema de lectura de huellas dactilares pequeño y plano proporcionado en uno o en los dos lados del cuerpo 1 de tarjeta, cuyo sistema puede comprender algunos o todos de entre uno o más biosensores, un tomador de imagen de huella dactilar, un almacenamiento de datos de huellas dactilares, un analizador de datos de huellas dactilares, o similares. Los señales 14s de huellas dactilares proporcionadas a dichos medios 16 de autenticación de huellas dactilares pueden comprender unas señales que abarcan varios datos, por ejemplo, unos datos de imagen de huellas dactilares analizados o en bruto, unos datos de sensor de calor, etc. Dichos medios 14 de lectura de huellas dactilares son capaces de este modo de proporcionar unas señales 14s de huellas dactilares basándose en uno o más dedos que se presionan contra cualquier biosensor proporcionado en la tarjeta.

Los medios 18 portadores de datos comprenden uno o más dispositivos de almacenamiento, es decir, un primer almacenamiento de datos que comprende al menos una o más unidades de memoria para almacenar datos de huellas dactilares de propietario de tarjeta y un segundo almacenamiento de datos que comprende una o más unidades de memoria para almacenar datos protegidos. Dichos almacenamientos de datos pueden ser una y la misma unidad de almacenamiento de todos los datos, o dos o más unidades almacenando cada una su tipo de datos, o una combinación de los mismos.

Los datos 18fd de huellas dactilares de propietario de tarjeta son unos datos relativos a uno o más dedos de un propietario de tarjeta autorizado, estando dichos datos pre-almacenados preferentemente en la tarjeta de crédito de acuerdo con la presente invención. Dicho pre-almacenamiento puede realizarse de cualquier manera convencional, por ejemplo, mediante una operación de almacenamiento de huellas dactilares de propietario de tarjeta certificada por el proveedor de la tarjeta de crédito. Las unidades de memoria usadas para almacenar los datos de huellas dactilares de propietario de tarjeta pueden tomar la forma de una RAM, una ROM, una PROM, una EEPROM, unos circuitos integrados de tarjetas inteligentes, unas bandas magnéticas o similares.

Se proporcionada una seguridad añadida por el hecho de que el pre-almacenamiento y por lo tanto el registro de las huellas dactilares del propietario de la tarjeta puedan realizarse solo en un número limitado de tarjetas de crédito, preferentemente solo en una tarjeta de crédito. De este modo es posible evitar tener que registrar las huellas dactilares fuera de la tarjeta de crédito de que se trata, y por lo tanto, la posibilidad de que una persona no autorizada robe un conjunto de datos de huellas dactilares para que hacer que coincidan con una tarjeta robada es virtualmente no existente. Preferentemente, dicho pre-almacenamiento de las huellas dactilares del propietario de la tarjeta se realiza en la tarjeta en una operación de una sola vez, en la que los datos de huellas dactilares se obtienen por dichos medios 14 de lectura de huellas dactilares proporcionados en dicha tarjeta de crédito. Por lo tanto, las huellas dactilares originales del propietario de la tarjeta solo se almacenan en un lugar, es decir, en la tarjeta de crédito en el primer almacenamiento de datos y no en, por ejemplo, una base de datos de almacenamiento central. Esto se suma a la seguridad de dichos datos de huellas dactilares, ya que elimina la preocupación del cliente de tener sus muy personales huellas dactilares registradas de manera centralizada. Además, esto elimina cualquier posibilidad de adquirir ilegalmente tales datos almacenados de manera centralizada por un posible ladrón. El procesador de datos de dicha tarjeta de crédito puede configurarse como para que sea capaz de impedir cualquier

pre-almacenamiento adicional que se realice o puede configurarse para permitir que solo un registro de una o más huellas dactilares de propietario de tarjeta o combinaciones de huellas dactilares, o bien una vez para cada momento de vida de dicha tarjeta de crédito, o para cada prestación o anulación de cada servicio de tarjeta de crédito en dicha tarjeta, que se realiza añadiendo o eliminando uno o más conjuntos de datos protegidos en dicho segundo almacenamiento.

La expresión “propietario de tarjetas de crédito” denota una o más personas, todas ellas con sus respectivos conjuntos de datos de huellas dactilares pre-almacenados en dichos medios portadores de datos de una tarjeta de crédito de acuerdo con la invención. Esto permite que más de una persona sea capaz de activar los datos protegidos mantenidos en dicha una tarjeta de crédito. La expresión “usuario de tarjeta de crédito” se refiere a la persona, que está tratando de activar los datos protegidos en una tarjeta de crédito de acuerdo con la invención.

Los datos 18sd protegidos comprenden uno o más conjuntos de datos protegidos, conteniendo cada conjunto de datos protegidos, por ejemplo, datos personales o información de cajero de banco, tal como el número de tarjeta, o similares, los datos que se usan para conseguir el acceso a los servicios personales, o al efectivo, al pago automático de mercancías, o similares. Dichos datos protegidos pueden estar en la forma de datos legibles de libre acceso o, como alternativa, en la forma de datos cifrados, o una combinación de ambos, en la que el suministro de datos cifrados proporciona una seguridad adicional durante una transferencia de comunicación de datos. Las unidades de memoria usadas para almacenar datos protegidos en la tarjetas de crédito convencionales a menudo toman la forma de circuitos integrados de tarjetas inteligentes o bandas magnéticas, pero preferentemente los datos protegidos y los datos de huellas dactilares de propietario de tarjeta pueden almacenarse en medios portadores de datos, tal como una memoria EEPROM o de tipo FLASH como el almacenamiento de datos primero y/o segundo. Por lo tanto, la tarjeta de crédito de acuerdo con la invención crea un bloqueo eficaz de la disponibilidad de dichos datos protegidos, especialmente para evitar cualquier copia no legal de la información magnética proporcionada en una banda magnética convencional, ya que los datos protegidos solo se liberan en la zona de lectura en forma de señales de datos protegidas electromagnéticamente inducidas a partir de dicha una o más bobinas de transductor después de que se haya realizado un procedimiento de autenticación de usuario de tarjeta.

Dichos medios 16 de autenticación de huellas dactilares comprenden unos medios para autenticar las señales 14s de huellas dactilares proporcionadas por dichos medios 14 de lectura de huellas dactilares, en los que dicha autenticación comprende preferentemente un procedimiento de comparación usando los datos de propietario de tarjeta pre-almacenados en dichos medios 18 portadores de datos, y un procedimiento de activación de datos protegidos para activar dichos datos protegidos pre-almacenados en dichos medios 18 portadores de datos, pero que pueden incluir más u otras etapas de autenticación, por ejemplo, comprendiendo unas opciones de selección de proveedor de usuario/tarjeta.

Dichos medios 16 de autenticación de huellas dactilares comprenden un procesador de datos capaz de realizar los procedimientos de autenticación. Dicho procesador de datos puede ser dedicado para dicha autenticación o también puede incorporarse en un circuito integrado de tarjeta inteligente para dichos datos protegidos.

Preferentemente, dichos medios 16 de autenticación de huellas dactilares y dichos medios portadores de datos pueden proporcionarse en combinación como un único circuito integrado en dicha tarjeta de crédito, por ejemplo, en la forma de un circuito integrado microcontrolador con una memoria EEPROM o de tipo FLASH. Con el fin de mejorar aún más la seguridad de los datos mantenidos en dicha memoria, es decir, los datos protegidos y los datos de huellas dactilares de propietario de tarjeta, dicho único circuito integrado o incluso dicho uno o más almacenamientos de datos pueden no estar disponibles para su lectura externa, por ejemplo, cortocircuitando las clavijas correspondientes del circuito integrado, durante el período de tiempo, en la que dicha tarjeta de crédito no está en uso. Esto inhibe cualquier intento por parte de un ladrón potencial, que tenga acceso a los medios de lectura de circuitos integrados, para leer dichos datos sin una autenticación de huellas dactilares anterior. A continuación, se abre dicho cortocircuito de dicho único circuito integrado de manera temporal con el fin de hacer los datos disponibles para la activación por el procedimiento de autenticación de huellas dactilares mencionado anteriormente. Esta apertura del cortocircuito puede iniciarse realizando una operación en la tarjeta, por ejemplo, uno o más dedos que tocan los medios de lectura de huellas dactilares, o por cualquier otro medio adecuado.

Preferentemente, dicha activación autenticada de huellas dactilares de los datos protegidos puede mantenerse durante un período de tiempo de activación determinado. Los ejemplos que muestran la aplicabilidad de esta activación abarcan la actividad de los datos protegidos durante el período de tiempo en el que uno o más dedos se presionan contra dichos medios de lectura de huellas dactilares, por ejemplo, durante una rápida pasada de la tarjeta de crédito a través de un dispositivo de lectura en un dispositivo de pago automático, o, como alternativa, durante el período de tiempo que se extiende desde el mismo momento en que el propietario de la tarjeta ha liberado la tarjeta de crédito en un ATM, y el momento, cuando el cajero automático ha completado la lectura de los datos protegidos proporcionados en la tarjeta de crédito. Una ventaja principal de dicha tarjeta de crédito de acuerdo con la presente invención es el hecho de que se realiza un procedimiento de autenticación automatizado completo y autosuficiente antes de la comunicación que se establece entre dicha tarjeta de crédito y cualquiera de los ATM existentes en el mercado hoy en día, con independencia del tipo (automático u operado de manera manual), el fabricante, la versión, o la posición geográfica de dicho ATM.

Preferentemente, dichos datos protegidos se activan durante un período de tiempo determinado fijado de manera precisa, lo que permite suficiente tiempo para que la comunicación se establezca y se termine. Si se elige dicho periodo de tiempo demasiado largo, esto puede proporcionar un tiempo suficiente al ladrón de tarjetas para realizar su propia transacción, lo que resulta en una menor seguridad para dichos datos protegidos. Si el período de tiempo se fija demasiado corto, puede que no haya tiempo suficiente para completar la comunicación entre la tarjeta de crédito y el cajero automático, o similares. Después de dicho periodo de tiempo, los datos protegidos no se envían por el procesador de datos, y se realiza una nueva autenticación de nuevo, cuando sea necesario. Este procedimiento se usa preferentemente, cuando no son críticos el momento de inicio y de final de la activación de los datos protegidos.

Como alternativa, como se describirá a continuación, se proporciona al menos un sensor 30 de detección de barrido en la tarjeta de crédito para activar los datos protegidos en una o más ráfagas de datos cuando el sensor de detección de barrido registra un barrido que se hace al pasar por un cabezal de lector de un lector de tarjetas de crédito.

En la figura 2 se muestra una superficie de una tarjeta de crédito de acuerdo con otra realización de la presente invención que comprende un cuerpo 1 de tarjeta en un lado provisto de una banda magnética como medio 18 portador de datos, y provisto de una fuente 12 de alimentación eléctrica tal como una batería recargable o una batería no recargable.

Ventajosamente, una tarjeta de crédito de acuerdo con la presente invención también puede comprender un medio de indicación de activación para indicar el estado de activación de los datos protegidos, es decir, si los datos protegidos proporcionados en una tarjeta de este tipo están o no en un estado de activación. En la figura 3, se muestran unos medios 160 de indicación de activación de este tipo comprendiendo en esta realización un LED verde o verde/rojo, en el que la luz verde indica la activación de los datos protegidos pre-almacenados en dichos medios portadores de datos y ninguna luz verde o una roja indica que no hay activación de dichos datos protegidos. La ventaja de tales medios es que el usuario de la tarjeta puede asegurarse el mismo del estado de activación antes de que utilice la tarjeta de crédito de acuerdo con la presente invención en un dispositivo de lectura con el fin de evitar intentos inútiles del dispositivo de lectura para comunicarse con dichos medios portadores de datos proporcionados en la tarjeta, si no se ha iniciado la activación debido a la falta de coincidencia de las huellas dactilares, la energía de la batería baja o similares.

Dichos medios 160 de indicación de activación pueden de manera ventajosa, por razones de consumo de energía, apagarse cuando no se está usando la tarjeta, es decir, solo durante un corto período de tiempo después de que uno o más dedos se han colocado sobre dichos medios de lectura de huellas dactilares.

La figura 3 muestra, además, una tarjeta de crédito proporcionada con unos medios 120 de indicación de estado de fuente de alimentación, consistiendo en esta realización en una banda de cambio de color eléctricamente conductora, indicando el cambio de color el estado de alimentación de la batería. Esto se usa especialmente, cuando las baterías recargables se proporcionan en la tarjeta de crédito para indicar a un usuario de la tarjeta cuando es el momento de cargar dichas baterías, pero también pueden usarse para indicar el estado de desgaste de la tarjeta para un uso de tiempo de vida corto.

La figura 4 muestra una realización adicional de la tarjeta de crédito de acuerdo con la presente invención, en la que un lado del cuerpo 1 de tarjeta está provisto en parte de células 125 solares para recargar las baterías recargables que se proporcionan en dicha tarjeta de crédito. El tipo exacto, la disposición, el tamaño, el número y otras características de dichas células solares puede variar, pero éstos coinciden preferentemente en la necesidad de recarga de dichas baterías para al menos una autenticación que se realiza por la tarjeta y para las indicaciones opcionales asociadas para el usuario de la tarjeta. Dichos medios de recarga pueden, por supuesto, asumir otras formas, por ejemplo, unos terminales de recarga que se proporcionan en dicha tarjeta de crédito para la conexión a unos medios de carga proporcionados externamente, tales como los terminales de carga correspondientes en un cargador de batería convencional.

En la figura 5, se muestra una tarjeta de crédito de acuerdo con la invención en una realización preferida, que comprende un cuerpo 1 de tarjeta, que comprende una batería 12 recargable que suministra una corriente eléctrica a los medios 14 de lectura de huellas dactilares, los medios 16 de autenticación de huellas dactilares que comprenden una memoria 18 EEPROM y un procesador de datos tal como un microcontrolador, y una zona 40 de lectura. Dichos medios 16 de autenticación de huellas dactilares son capaces de comparar las señales de huellas dactilares recibidas desde dichos medios 14 de lectura de huellas dactilares con los datos de huellas dactilares de propietario de tarjeta almacenados en dicha memoria 18 con el fin de, durante un intervalo de tiempo determinado, enviar las señales correspondientes a los datos protegidos también almacenados en dicha memoria 18 a través de un circuito 20 de excitación también proporcionado en dicho cuerpo 1 de tarjeta a una zona 40 de lectura en dicho cuerpo 1 de tarjeta para la emisión de dichas señales de datos protegidos. No se emiten datos protegidos desde dicha zona 40 de lectura fuera de dicho intervalo de tiempo de activación determinado. El circuito 20 de excitación puede comprender preferentemente las electrónicas de amplificador, tales como los amplificadores operacionales y, puede proporcionarse, preferentemente, de manera integral con el procesador de datos, por ejemplo, en un ASIC.

La zona 40 de lectura comprende tres bobinas 42 de transductor, de las que se muestra una en la figura 6, comprendiendo cada una de las mismas un número de devanados 420 de núcleo enrollados alrededor de una sección de extremo de una banda 422 de un material de núcleo electromagnéticamente inducible. Cada bobina 42 de transductor puede inducirse de manera individual por dicho circuito 20 de excitación. El número de bobinas de transductor puede elegirse como tres con el fin de inducir las señales de datos protegidos correspondientes a la información de banda magnética convencional, que se encuentra en las bandas magnéticas en tres pistas, pero puede, como una alternativa, proporcionarse en números que van de uno a más de tres. Para la mayoría de las aplicaciones, los datos son solo para generarse en dos bobinas 42 de transductor, que corresponden a la primera y a la segunda de dichas bandas magnéticas convencionales. En las bandas magnéticas convencionales, los datos se presentan permanentemente de manera magnética a un lector de tarjetas de crédito usando un denominado formato F2F, o en un formato de dos frecuencias, en la que un bit “0” está formado por una parte de imán de una longitud predeterminada en dicha magnética banda, y un bit “1” son dos partes de imán dirigidas longitudinalmente, magnéticamente de manera opuesta, teniendo una longitud combinada igual a dicha longitud de la parte de imán de bit “0”. Una pista de imán convencional está provista normalmente de 476 bits/cm. Por lo tanto, las bobinas 42 de transductor de la tarjeta de crédito y el sistema de activación de datos protegidos de acuerdo con la presente invención es, preferentemente, para emitir y presentar dichas señales de datos protegidos en tal formato F2F a un lector de tarjetas de crédito, que es para leer dicha tarjeta de crédito con un cabezal 50 de lector.

La bobina 42 de transductor, producirá un campo magnético homogéneo y relativamente fuerte con el fin de que pueda leerse por un lector de tarjetas de crédito. La naturaleza de este campo magnético está fuertemente influenciada por la construcción de la bobina de transductor, tal como por la elección del material de núcleo y la construcción del núcleo de las bandas 422 de núcleo, el número y la posición de los devanados 420 de núcleo en las bandas 422 de núcleo. Las variaciones en las señales para una bobina 42 de transductor generan un campo magnético variable a lo largo de la banda, que es idéntico al campo magnético, que está influenciado por un cabezal de lector, cuando se pasa una tarjeta de crédito de banda magnética convencional que mantiene los mismos datos protegidos a través del mismo lector.

El material de la banda 422 de núcleo es de manera ventajosa un material electromagnéticamente inducible, tal como metal, preferentemente una laminación electromagnética, una chapa de hierro u otro tipo de chapa metálica, o proporcionada como una lámina simple o doble en uno o en cada lado del cuerpo de tarjeta, teniendo de manera ventajosa una anchura y una posición correspondiente a una pista magnética convencional con el fin de tener un aspecto magnético y físico similar. La elección del material de núcleo de las bandas de núcleo influye fuertemente en la fuerza y la distribución del campo magnético producido, y permite que se produzca una mejora del campo magnético, lo que resulta en la necesidad de una corriente más baja en los devanados de núcleo, lo que reduce el consumo de energía de dicha tarjeta de crédito.

La banda 422 de núcleo puede estar provista preferentemente de entrehierros distribuidos (no mostrados), o contaminaciones de otro material más o menos electromagnéticamente inducible, tal como el plástico o el papel, o proporcionado a lo largo de la extensión del material de núcleo o dentro del cuerpo de tarjeta con el fin de que la bobina de transductor produzca varios campos magnéticos pequeños a lo largo del material de núcleo para proporcionar una distribución de campo magnético homogénea para facilitar la legibilidad mejorada por un entrehierro de lectura de un lector de tarjetas de crédito que se usa en la tarjeta de crédito de acuerdo con la invención. Sin tales entrehierros, la parte más fuerte del campo magnético tiene una tendencia a fluir desde un extremo de la banda de núcleo al otro extremo de la misma y, en consecuencia lejos de un entrehierro de lectura de un cabezal de lector magnético de un lector de tarjetas de crédito.

La expresión “banda de núcleo” ha de entenderse como una indicación de las partes sustancialmente alargadas de un material de núcleo, también comprende por lo tanto varias secciones de material de núcleo relativamente pequeñas o grandes colocadas de manera sucesiva y/o una sección de material de núcleo integral, que tiene una capa de material de espesor relativamente pequeña o grande y que tienen unas anchuras y unas alturas dimensionadas de manera adecuada para producir un campo magnético de una fuerza, homogeneidad y extensión deseadas.

Se ha descubierto que proporcionando los devanados 420 de núcleo de la bobina 42 de transductor en una sección de extremo de la banda 422 de un material de núcleo electromagnéticamente inducible, es capaz de proporcionar un campo magnético homogéneo que se emite por toda la zona 40 de lectura. Proporcionando dichos devanados 420 de núcleo en una sección de extremo de dichas bandas 422 de núcleo como se ve en la figura 5 y 6 también ayuda a reducir las interferencias magnéticas entre los devanados 420 de núcleo proporcionados en dicha tarjeta de crédito y el cabezal 50 de lector de un lector de tarjetas de crédito. Por lo tanto, la disposición de los devanados 420 de núcleo de las tres bobinas 42 de transductor respectivas pueden como alternativa de manera ventajosa proporcionarse de manera consecutiva en las secciones de extremo opuestas. Obviamente, los devanados de núcleo de dicha bobina de transductor pueden también, como alternativa, proporcionarse de manera uniformemente distribuida a lo largo de la extensión de la banda de núcleo, o pueden distribuirse en una o más secciones de dicha banda de núcleo o en secciones de los mismos. Los devanados 420 de núcleo se proporcionan preferentemente alrededor del lado corto de la banda 422 de núcleo y pueden proporcionarse en cualquier número apropiado en relación con la fuerza de campo magnético deseada, la carga de corriente de los devanados de núcleo, el aspecto magnético, etc. Obviamente, los devanados de núcleo son de un material, que es capaz de inducir un campo

magnético en dichas bandas de núcleo inducibles, por ejemplo, un metal como el hierro u otro material conductor adecuado.

Mediante la invención, los inventores se han dado cuenta de que una “banda magnética activable” de este tipo en la zona de lectura puede ser útil para otras aplicaciones, en las que los datos protegidos de una banda magnética requieren una entrada antes de que se activen, por ejemplo, los sistemas automáticos de asistencia de empleados, las tarjetas individualizadas de tienda de Internet, las insignias de identificación, etc. Dicha entrada no se limita a una autenticación de huellas dactilares, sino que también puede ser una retina, una firma, u otra autenticación, o incluso puede ser una entrada de botón de pulsación simple, y puede ser de cualquier persona, no solo de la persona o la entidad a la que se refieren dichos datos protegidos. Por lo tanto, también se desvela en el presente documento un sistema de activación de datos protegidos, mostrado como un ejemplo que es una tarjeta de crédito con una autenticación de huellas dactilares.

En la figura 5, la tarjeta de crédito que se muestra comprende además, un sensor 30 de detección de barrido, que se coloca en una de dichas bobinas 42 de transductor para la detección de un lector 50 de tarjetas de crédito, cuando la tarjeta de crédito de acuerdo con la invención está en las proximidades de un lector de este tipo, es decir, cuando dicho sensor 30 es adyacente a un cabezal 50 de lectura de recogida de un lector de tarjetas de crédito. Un sensor 30 de detección de barrido de este tipo puede comprender al menos un devanado de sensor (no mostrado) dispuesto alrededor de una de dichas bandas 422 de núcleo. Durante el uso, el barrido de la tarjeta de crédito a través de un lector de tarjetas de crédito inducirá una corriente en dicho al menos un devanado de sensor, porque dicho cabezal 50 de recogida es magnético y la tarjeta o el cabezal se mueve, lo que se detecta por el sensor 30 de detección de barrido. Otros sensores de detección de barrido, que pueden usarse como alternativa comprenden: a) un interruptor, que está cerrado, cuando un cabezal de lector de un lector de tarjetas de crédito está en las proximidades de dicho sensor, o b) dos conductores, que se cortocircuitan cuando el cabezal de lector de un lector de tarjetas de crédito se pasa por las proximidades de dicho sensor, o cualquier otro medio de sensor de detección de barrido adecuado. La ventaja de un sensor de detección de barrido que está presente es que al menos el comienzo del período de tiempo de activación y también la duración de dicho periodo de tiempo puede determinarse basándose en la entrada de dicho sensor.

Como una alternativa, puede proporcionarse más de un sensor de detección de barrido, por ejemplo, uno en cada sección de extremo de una bobina de transductor o, como alternativa, en cada sección final de la zona de lectura, con el fin de alimentar el procesador de datos con información sobre en qué extremo de la bobina de transductor se inicia el conjunto de datos protegidos basándose en dicha detección de proximidad de cabezal de lector.

En otra realización, el sensor o los sensores de detección de barrido detectan la velocidad con la que pasa el cabezal de recogida, y esta información se alimenta al procesador de datos, que a su vez determina el comienzo y la duración del período de tiempo de activación necesario para comunicar las señales de datos protegidos al lector de tarjetas de crédito. Esto es especialmente ventajoso cuando se usa la tarjeta de crédito de acuerdo con la invención en máquinas de tipo ATM, porque la duración de la emisión de las señales de datos protegidos se reduce solo al periodo de tiempo de comunicación y la velocidad de lectura en un ATM convencional se preajusta a menudo a una velocidad preestablecida de sistema constante o bien definida.

Cuando las huellas dactilares de propietario de tarjeta están registradas por dichos medios 14 de lectura de huellas dactilares, la presentación de los datos protegidos a dichas bobinas 42 de transductor puede activarse durante un período de tiempo determinado. Durante dicho periodo de tiempo, las señales de datos protegidos solo se emiten desde el zona de lectura, cuando y si el sensor 30 de detección de barrido detecta una proximidad de este tipo de un cabezal 50 de lector de tarjetas de crédito, inmediatamente después de que se proporcione, preferentemente, solo una emisión de las señales de datos protegidos por dicha zona 40 de lectura. Esto es útil cuando se barre dicha tarjeta de crédito a través de un lector de tarjetas de crédito con un movimiento relativamente rápido de dicha tarjeta de crédito. Como alternativa, pueden realizarse varias emisiones durante dicho periodo de tiempo. Esto puede ser útil cuando dicha tarjeta de crédito se deja en el interior de dicho lector de tarjetas de crédito durante un período de comunicación de mayor duración.

En la figura 6 se muestra un cabezal 50 de lector de tarjetas de crédito convencional que lee una bobina 42 de transductor de una tarjeta de crédito de acuerdo con la presente invención (no mostrado). El lector de tarjetas de crédito decodifica los datos que se emiten por una tarjeta de crédito, tras la que se coloca la bobina, preferentemente de acuerdo con ciertas normas de presentación conocidas de los datos de tarjetas de crédito para los expertos en la materia, tales como la norma ISO 7811. En dicha norma, se usa un protocolo que comprende un centinela de inicio, 76 caracteres alfanuméricos que comprenden un código de formato inicial y los separadores de campo entre las partes de datos, un centinela de final, y un carácter de comprobación de redundancia longitudinal. Las bobinas de la tarjeta de crédito pueden generar preferentemente datos protegidos como se ha descrito anteriormente con el fin de cumplir con dichas normas dadas.

En una realización preferida, el circuito 20 de excitación es capaz de realizar una amplificación avanzada que comprende una compensación de amplitud, que puede realizarse con la tecnología de conversión DA o incluso un circuito determinado de temporización analógica, y una conformación de pulso, que puede realizarse por una conversión DA o un filtrado analógico de los datos protegidos o las señales de datos protegidos a través de dicha

bobina de transductor o por un filtrado activo o pasivo. Estas tecnologías son bien conocidas por los expertos en la materia.

La conformación de pulso (compensación rápida) es la actividad de ajustar la forma del pulso de las señales de datos protegidos transmitidas al cabezal de lector de tal manera, que se consigue una característica de transmisión mejorada, lo que permite un aumento de la tasa de transmisión de la señal de datos protegidos.

En las figuras 7A, 7B y 7C se ilustra un ejemplo de una compensación de amplitud del campo que se distribuye por la bobina 42 de transductor. La compensación de amplitud (compensación lenta) es la regulación de la intensidad del campo magnético, que es una función de la corriente a través de los devanados de núcleo de la bobina de transductor con el fin de mantener el campo magnético estable en amplitud a lo largo de la extensión de la bobina 42 de transductor y una parte más allá del borde de la misma. La figura 7A muestra una característica de amplitud sobre la extensión de una banda de núcleo sin compensación de amplitud, en la que se ve, que la intensidad del campo magnético B, que es una función de la corriente de devanado de núcleo I, no es constante a lo largo de la extensión de una bobina 42 de transductor, especialmente no en las partes extremas, en las que la amplitud tiende a aumentar. La desventaja de esto es el hecho de que una gran cantidad de la energía eléctrica se usa fuera de la zona de lectura, lo que reduce la eficacia de la transferencia de señal. Además, este efecto proporciona a las señales de datos protegidos una intensidad relativamente alta que se extiende alejándose de dicha tarjeta de crédito, incluso más allá del ATM y/o del titular de la tarjeta de crédito, añadiendo de este modo el riesgo de que una persona malintencionada que tiene intenciones de copiar las señales de datos protegidos puede ser capaz de “aprovechar” las señales de datos protegidos durante la emisión de las mismas. En la figura 7B se muestra un ejemplo de una señal de compensación de amplitud proporcionada por la conversión DA en el circuito de excitación, que por una conversión DA adicional se añade a la característica de amplitud de la figura 7A. En la figura 7C se muestra la amplitud de campo magnético resultante compensado por la conversión DA, en la que una amplitud sustancialmente constante se ve que es el resultado sobre la extensión de la bobina 42 de transductor. Se dan como resultado dos ventajas de esto. En primer lugar, la amplitud de las señales de datos protegidos puede mantenerse a un mínimo constante para el cabezal de lector que es capaz de leer las señales de datos protegidos, lo que reduce el riesgo de copia por unas personas malintencionadas, también porque el campo magnético puede compensarse de este modo por una dirección hacia el cabezal de lector. En segundo lugar, se reduce significativamente el consumo de energía resultante a través de los devanados de núcleo, lo que a su vez extiende el tiempo de vida de la fuente de alimentación eléctrica proporcionada en el cuerpo de la tarjeta. Preferentemente, la intensidad del campo magnético durante la emisión de las señales de datos protegidos se corresponde con la intensidad actualmente disponible a partir de las bandas magnéticas convencionales.

En uso, el propietario de una tarjeta de crédito de acuerdo con la presente invención agarra dicha tarjeta de crédito, presiona uno o más dedos contra dichos medios de lectura de huellas dactilares, y unos medios de autenticación de huellas dactilares proporcionados en la tarjeta de crédito activan los datos protegidos proporcionados en dicha tarjeta de crédito solo si la autenticación de las huellas dactilares realizada en la tarjeta coincide con los datos de huellas dactilares de propietario de tarjeta también proporcionados en la tarjeta de crédito. Si se establece una coincidencia de las huellas dactilares, los datos protegidos pre-almacenados en la tarjeta se activan por dichos medios de autenticación de huellas dactilares y dichos datos protegidos pueden leerse desde cualquier dispositivo de lectura de un ATM o similares.

Una función ventajosa que se proporciona por dicha tarjeta de crédito de acuerdo con la invención es la disposición del almacenamiento en dichos medios 18 portadores de datos de al menos una huella dactilar o combinación de huellas dactilares correspondientes a la desactivación de las huellas dactilares de dicho propietario de tarjeta. Si un criminal está tratando de coaccionar al propietario de la tarjeta en la activación de los datos protegidos con el fin de proporcionar, por ejemplo, dinero en efectivo para dicho criminal, este intento puede neutralizarse o incluso evitarse. Esto se debe al hecho de que el criminal no es consciente de que la huella dactilar o las huellas dactilares pueden activar o desactivar los datos protegidos. En consecuencia, el propietario de la tarjeta hace uso de la oportunidad de seleccionar un dedo o una combinación de dedos de autenticación, que en dicha tarjeta de crédito se almacena como unas huellas dactilares de desactivación, y por lo tanto desactivan los datos protegidos durante un período de tiempo de desactivación apropiadamente largo, que puede seleccionarse para que sean horas, días, o más, incluso de manera permanente. La huella dactilar de desactivación se autentica por el procesador de datos, que se basa en la autenticación positiva con una huella dactilar de desactivación almacenada que hace dichos datos protegidos inaccesibles durante un periodo de tiempo de desactivación preseleccionado, que puede almacenarse en dichos medios 18 portadores de datos o programarse en dichos medios 16 de autenticación de huellas dactilares que comprenden un procesador de datos.

El procesador de datos o microcontrolador es capaz de programarse para un registro del que se van a usar las huellas dactilares específicas de diferentes dedos o combinaciones de huellas dactilares para la desactivación de las tarjetas de crédito a largo plazo o para la activación de los conjuntos de datos protegidos respectivos para cada función de tarjeta de crédito disponible en una tarjeta de crédito de acuerdo con la invención. Preferentemente, dicho procesador de datos o microcontrolador está configurado de tal manera que dicha programación es solo para realizarse una vez, por ejemplo, una vez por el tiempo de vida de dicha tarjeta de crédito o una vez para cada adición o eliminación de diferentes funciones de la tarjeta de crédito, es decir, el servicio de tarjeta de crédito que se proporciona por dicha tarjeta de crédito.

El procedimiento de autenticación que se realiza en la tarjeta y con independencia de cualquier dispositivo de lectura o de otro aparato externo, solo es posible porque la fuente de alimentación para este procedimiento se proporciona en la propia tarjeta de crédito. Una fuente de alimentación sustancialmente autónoma, en la tarjeta e independiente está provista en una tarjeta de crédito de acuerdo con la presente invención.

La configuración exacta de la tarjeta de crédito de los diferentes componentes proporcionados en dicha tarjeta no es importante y solo se muestra en las figuras a modo de ejemplo. Uno puede preferir una integración de todos los componentes, en última instancia dentro de un dispositivo de lectura de huellas dactilares, de autenticación, de portador de datos, de fuente de alimentación, tal como un circuito integrado proporcionado en dicha tarjeta, siendo dicha integración ventajosa por razones de coste y de miniaturización.

Mediante la invención se comprende que una tarjeta multi-función se activa proporcionando la tarjeta de crédito con medios de selección de servicios de tarjeta de crédito para que un propietario de una tarjeta seleccione los diferentes servicios de tarjeta de crédito en la forma de diferentes conjuntos de datos protegidos, por ejemplo, una número de seguridad social, un número de identificación bancaria, y un número de identificación de proveedor de crédito. Esto puede hacerse o bien proporcionando un interruptor convencional en dicha tarjeta de crédito para seleccionar entre estos o proporcionando al menos un sistema de lectura de huellas dactilares. Un propietario de tarjeta puede seleccionar un sistema entre una pluralidad de sistemas de lectura de huellas dactilares presionando uno o más dedos contra dicho sistema seleccionado. Por lo tanto, la selección activa un conjunto asociado de datos protegidos, que opcionalmente pueden proporcionarse desde el mismo proveedor o diferentes proveedores de tarjetas. Como un ejemplo, la selección de un primer sistema de lectura de huellas dactilares puede activar, por ejemplo, un primer conjunto de datos protegidos que se refieren a un número de identificación de banco; una selección de un segundo sistema de lectura de huellas dactilares puede activar un segundo conjunto de datos protegidos que se refieren a un número de seguridad social. Como alternativa, dichos medios de selección de servicios de tarjeta de crédito comprenden un único sistema de lectura de huellas dactilares para todos los servicios de tarjeta de crédito disponibles, en el que dichos datos de huellas dactilares de propietario de tarjeta comprenden al menos una huella dactilar o una combinación de huellas dactilares que corresponden a una huella dactilar de activación para cada servicio de tarjeta de crédito, y en el que dicho procesador de datos está adaptado para la activación de la zona de lectura durante un período de tiempo de activación determinado, cuando dicha huella dactilar de activación se presiona contra dicho sistema de lectura de huellas dactilares. La ventaja de los medios de selección de servicios de tarjeta de crédito de este tipo comprende, como se ha indicado anteriormente, prescindir de manera opcional de un número de código de identificación dedicado para cada conjunto de datos protegidos a activarse, lo que mitiga la necesidad de que un usuario de tarjeta recuerde varios números de códigos de identificación, uno por cada tarjeta que posea.

REIVINDICACIONES

1. Una tarjeta de crédito que comprende un cuerpo de tarjeta, que comprende

- medios (14) de lectura de huellas dactilares que proporcionan unas señales de huellas dactilares representativas de al menos una huella dactilar de un usuario de tarjeta, cuando al menos un dedo de dicho usuario se presiona contra dichos medios de lectura de huellas dactilares;
- medios (18) portadores de datos que mantienen al menos unos datos (18fd) de huellas dactilares de propietario de tarjeta y unos datos (18sd) protegidos;
- una zona (40) de lectura;
- medios (16) de autenticación de huellas dactilares que comprenden un procesador de datos, que es capaz de autenticar dichas señales de huellas dactilares con dichos datos de huellas dactilares de propietario de tarjeta,
- una fuente (12) de alimentación eléctrica que suministra energía eléctrica a al menos dichos medios de lectura de huellas dactilares, dichos medios de autenticación de huellas dactilares y dicha zona de lectura,
- al menos un circuito (20) de excitación en comunicación con al menos una bobina (42) de transductor en dicha zona de lectura que comprende al menos un devanado (420) de núcleo alrededor de al menos una banda (422) de material de núcleo inducible electromagnéticamente, pudiendo cada banda ser inducida de manera individual por dicho procesador de datos para emitir un campo magnético que contiene unas señales de datos protegidos correspondientes a dichos datos protegidos, y
- al menos un sensor (30) de detección de barrido que es capaz de hacer que dicho procesador de datos active dichos datos protegidos por la emisión de dichas señales de datos protegidos al menos una vez por dicha al menos una bobina de transductor, cuando dicha tarjeta de crédito está en las proximidades de un lector (50) de tarjetas de crédito,

en la que dichos medios de autenticación de huellas dactilares controlan la activación de dichos datos protegidos basados en la autenticación de las señales de huellas dactilares comparando estas con dichos datos de huellas dactilares de propietario de tarjeta, si la comparación es una coincidencia, entonces dichos datos protegidos se activan, si no, dichos datos protegidos no se activan,

estando la tarjeta de crédito **caracterizada porque** el sensor de barrido comprende al menos un devanado sensor proporcionado alrededor de al menos una de dichas bandas de material de núcleo inducible electromagnéticamente.

2. Una tarjeta de crédito de acuerdo con la reivindicación 1, en la que la activación de dichos datos protegidos se mantiene a lo largo de un período de tiempo de activación determinado.

3. Una tarjeta de crédito de acuerdo con la reivindicación 2, en la que dicha activación de datos protegidos se realiza por la emisión de señales de datos protegidos una o varias veces consecutivas por dicha al menos una bobina de transductor.

4. Una tarjeta de crédito de acuerdo con la reivindicación 1, en la que se proporcionan dos sensores de detección de barrido, uno en cada sección de extremo de dicha al menos una bobina de transductor con el fin de proporcionar información al procesador de datos sobre el extremo en el cual se inician las señales de los datos protegidos.

5. Una tarjeta de crédito de acuerdo con la reivindicación 1, en la que dicho al menos un sensor de detección de barrido es capaz de detectar la velocidad con la que se barre la tarjeta de crédito por un lector de tarjetas de crédito, y basándose en esta velocidad detectada el procesador de datos es capaz de determinar el período de tiempo de activación.

6. Una tarjeta de crédito de acuerdo con cualquiera de las reivindicaciones anteriores, en la que dicho circuito de excitación es capaz además de realizar una amplificación avanzada tal como una compensación de amplitud y una conformación de pulso en dichas señales de datos protegidos.

7. Una tarjeta de crédito de acuerdo con cualquiera de las reivindicaciones anteriores, en la que dicho circuito de excitación se proporciona de manera integral con el procesador de datos.

8. Una tarjeta de crédito de acuerdo con cualquiera de las reivindicaciones anteriores, en la que dicha al menos una banda del material de núcleo inducible está provista de al menos un entrehierro distribuido.

9. Una tarjeta de crédito de acuerdo con la reivindicación 8, en la que dicho al menos un entrehierro está provisto de unas distribuciones de material que tiene una capacidad de inducción electromagnética diferente en comparación con el material de dicha al menos una banda de material de núcleo inducible.

10. Una tarjeta de crédito de acuerdo con cualquiera de las reivindicaciones anteriores, en la que dicho al menos un devanado de núcleo está colocado sustancialmente en una sección de extremo de dicha al menos una banda de material de núcleo inducible.

11. Una tarjeta de crédito de acuerdo con cualquiera de las reivindicaciones anteriores, que comprende además unos medios de indicación de activación para la indicación de la activación de dicha zona de lectura.

12. Una tarjeta de crédito de acuerdo con cualquiera de las reivindicaciones anteriores, en la que dicha fuente de alimentación eléctrica comprende al menos una batería.

13. Una tarjeta de crédito de acuerdo con cualquiera de las reivindicaciones anteriores, en la que dicha fuente de alimentación eléctrica comprende al menos una batería (12) recargable.

14. Una tarjeta de crédito de acuerdo con la reivindicación 13, en la que dicha fuente de alimentación eléctrica comprende además unos medios de recarga para dicha batería recargable.

15. Una tarjeta de crédito de acuerdo con la reivindicación 14, en la que dichos medios de recarga para dicha al menos una batería recargable comprenden una disposición (125) de células solares.

16. Una tarjeta de crédito de acuerdo con cualquiera de las reivindicaciones anteriores, en la que dicho cuerpo de tarjeta comprende además unos medios (120) de indicación de estado de la fuente de alimentación.

17. Una tarjeta de crédito de acuerdo con cualquiera de las reivindicaciones anteriores, en la que dichos medios portadores de datos incluyen un primer almacenamiento de datos para mantener los datos de huellas dactilares del propietario de la tarjeta, y un segundo almacenamiento de datos para mantener los datos protegidos.

18. Una tarjeta de crédito de acuerdo con la reivindicación 17, en la que dicho almacenamiento de datos primero y/o segundo es una memoria EEPROM o de tipo FLASH.

19. Una tarjeta de crédito de acuerdo con la reivindicación 17, en la que dicho segundo almacenamiento de datos es un circuito integrado de tarjeta inteligente o una banda magnética.

20. Una tarjeta de crédito de acuerdo con cualquiera de las reivindicaciones anteriores, en la que dichos medios de autenticación de huellas dactilares y dichos medios portadores de datos están combinados en un único circuito integrado, tal como un microcontrolador con una memoria.

21. Una tarjeta de crédito de acuerdo con la reivindicación 20, en la que dicho circuito integrado único es capaz de ponerse en un primer estado, en el que dichos datos protegidos y dichos datos de huellas dactilares de propietario de tarjeta están disponibles de manera temporal para una activación de dichos datos protegidos.

22. Una tarjeta de crédito de acuerdo con cualquiera de las reivindicaciones anteriores, en la que dichos medios de lectura de huellas dactilares comprenden al menos un sistema de lectura de huellas dactilares.

23. Una tarjeta de crédito de acuerdo con cualquiera de las reivindicaciones anteriores, que comprende además unos medios de selección de servicios de tarjeta de crédito, tales como un interruptor, por el que un propietario de tarjetas de crédito puede seleccionar un servicio de tarjeta de crédito seleccionando a partir de diferentes conjuntos de datos protegidos, uno para cada servicio de tarjeta de crédito disponible.

24. Una tarjeta de crédito de acuerdo con la reivindicación 23, en la que dichos medios de selección de servicios de tarjeta de crédito comprenden un sistema de lectura de huellas dactilares para cada servicio de tarjeta de crédito disponible.

25. Una tarjeta de crédito de acuerdo con la reivindicación 23, en la que dichos medios de selección de servicios de tarjeta de crédito comprenden un único sistema de lectura de huellas dactilares para todos los servicios de tarjeta de crédito disponibles, en la que dichos datos de huellas dactilares de propietario de tarjeta comprenden al menos una huella dactilar o una combinación de huellas dactilares que corresponde a una huella dactilar de activación de cada servicio de tarjeta de crédito, y en la que dicho procesador de datos está adaptado para la activación de la zona de lectura durante un período de tiempo de activación determinado, cuando dicha huella dactilar de activación se presiona contra dicho sistema de lectura de huellas dactilares.

26. Una tarjeta de crédito de acuerdo con cualquiera de las reivindicaciones anteriores, en la que dichos medios de lectura de huellas dactilares por medio de dicho procesador de datos son capaces de pre-almacenar una huella dactilar de propietario de tarjeta en dichos medios portadores de datos en una única operación.

27. Una tarjeta de crédito de acuerdo con cualquiera de las reivindicaciones anteriores, en la que dichos datos de huellas dactilares de propietario de tarjeta comprenden al menos una huella dactilar o una combinación de huellas dactilares que corresponden a una huella dactilar de desactivación, y en la que dicho procesador de datos está adaptado para la desactivación de la zona de lectura durante un período de desactivación determinado, cuando se presiona dicha huella dactilar de desactivación contra dichos medios de lectura de huellas dactilares.

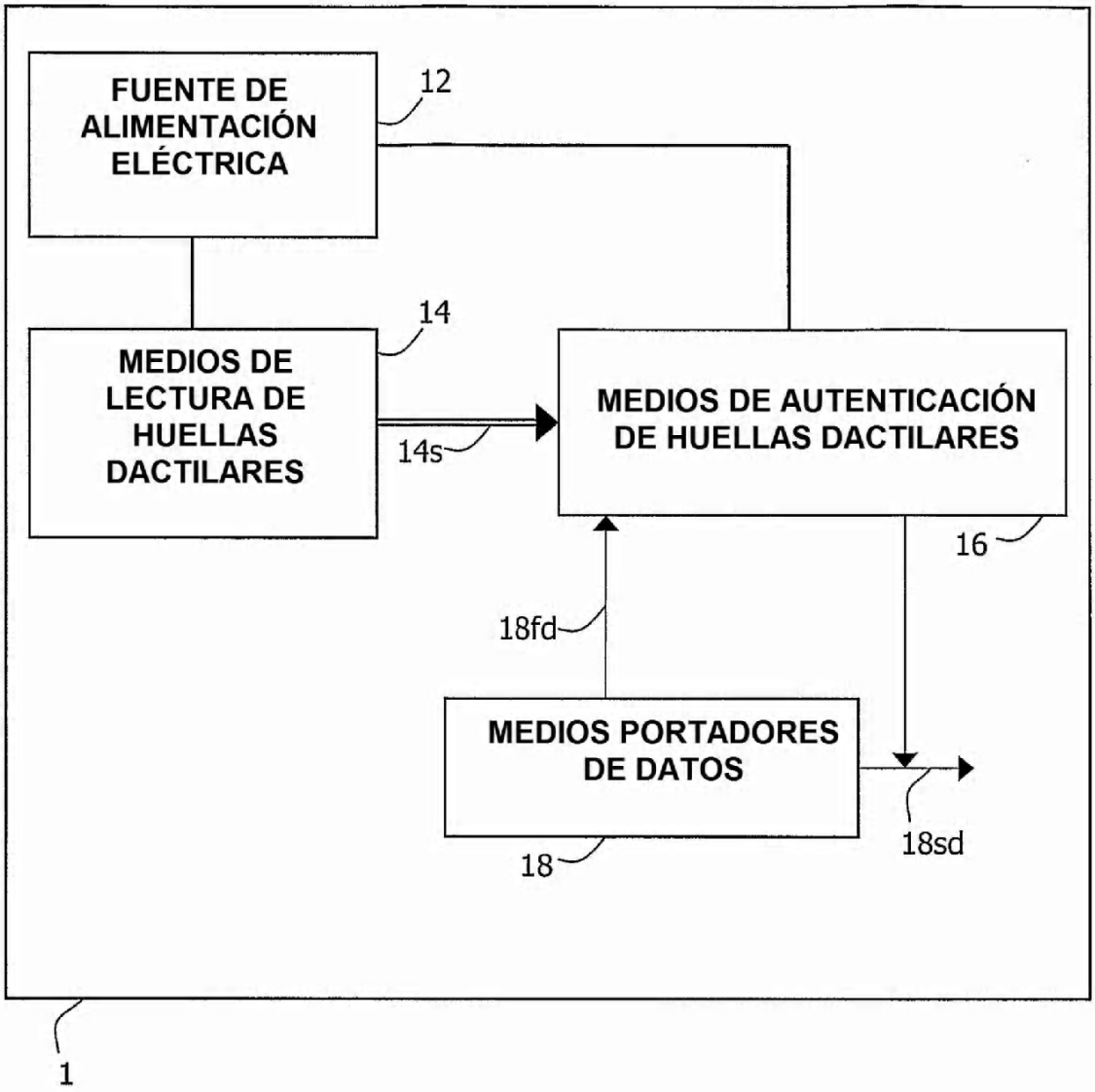
FUENTE DE ALIMENTACIÓN ELÉCTRICA
12
MEDIOS DE LECTURA DE HUELLAS DACTILARES
14
14s
MEDIOS DE AUTENTICACIÓN DE HUELLAS DACTILARES
16
18fd
MEDIOS PORTADORES DE DATOS
18
18sd
1

FIG. 1

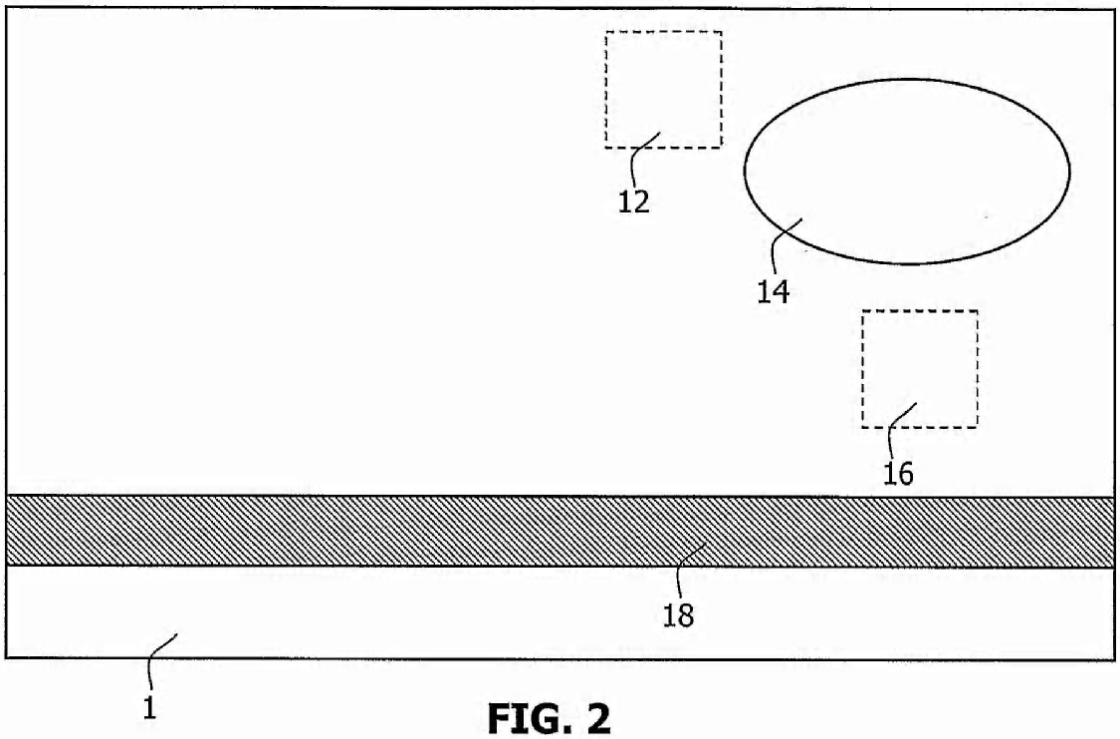

FIG. 2

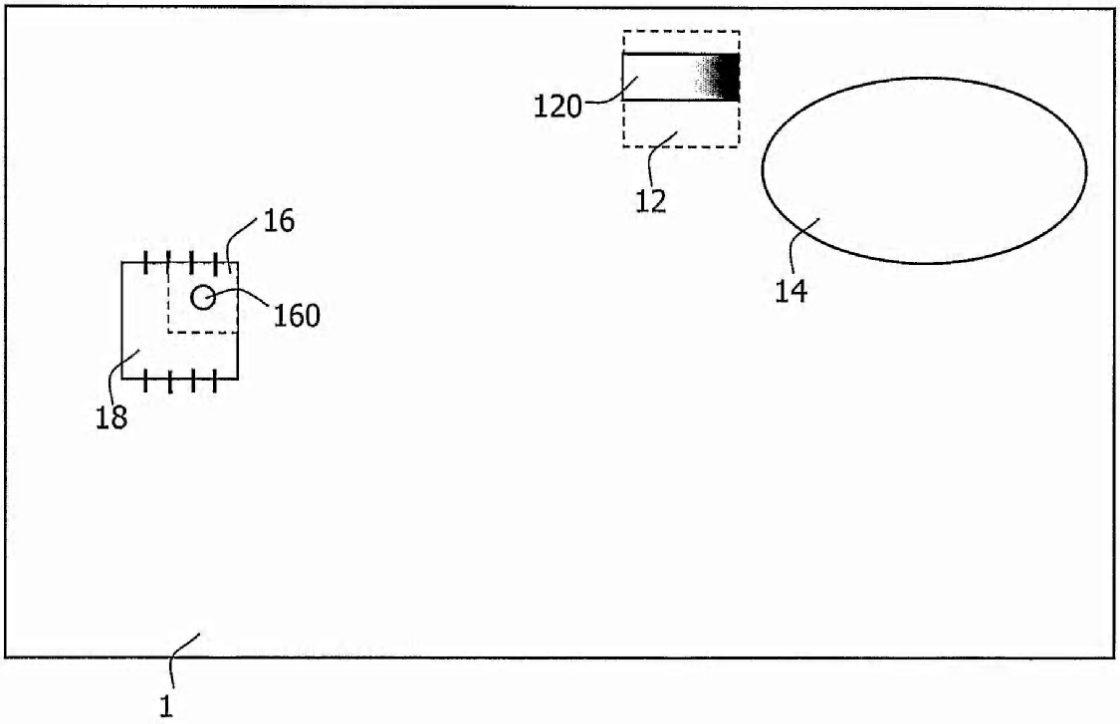

FIG. 3

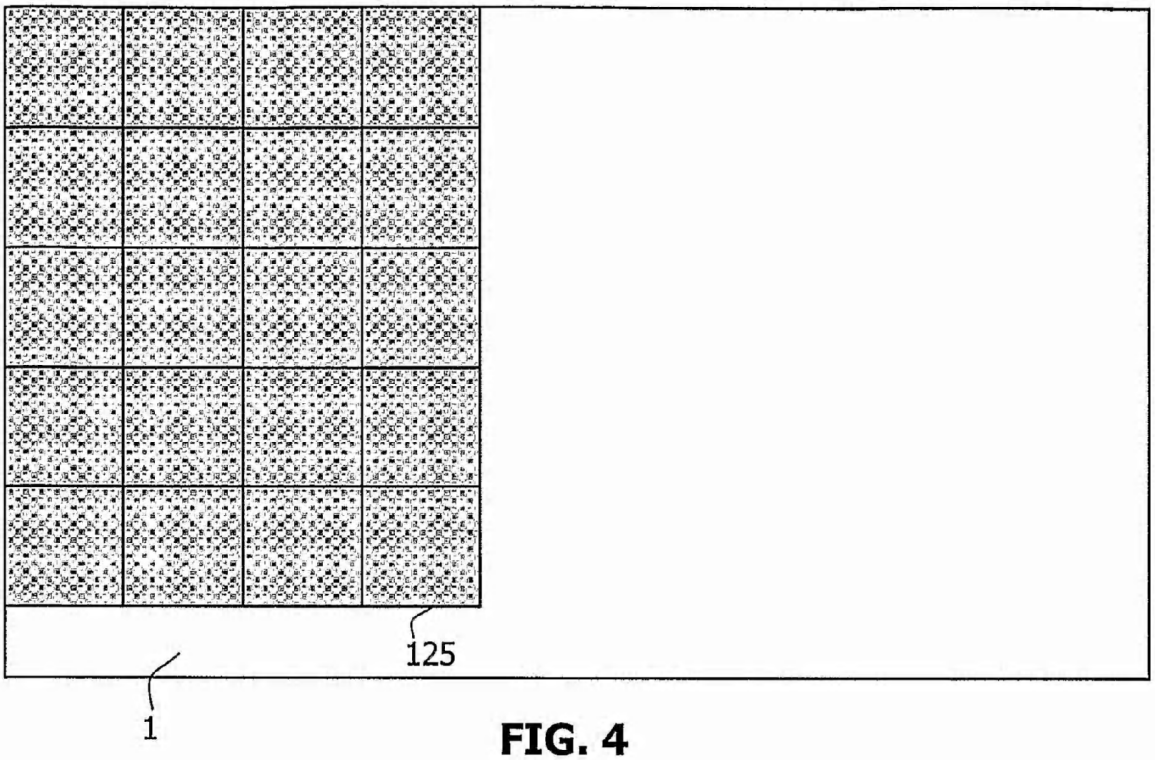

FIG. 4

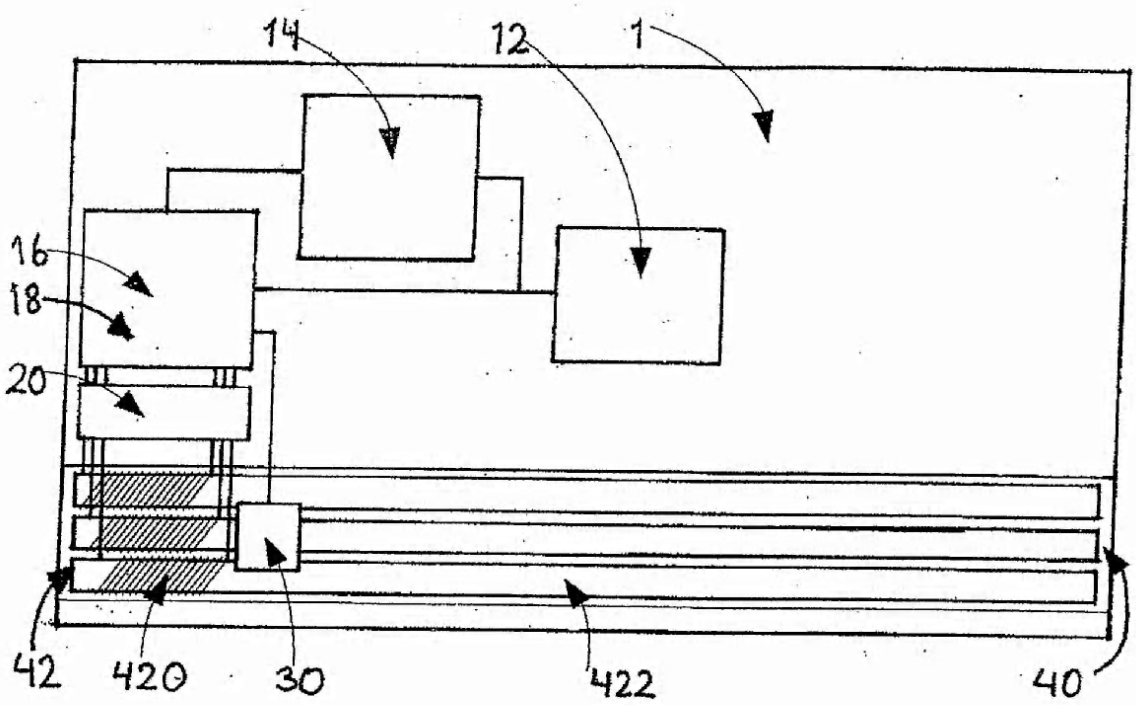

Fig.5

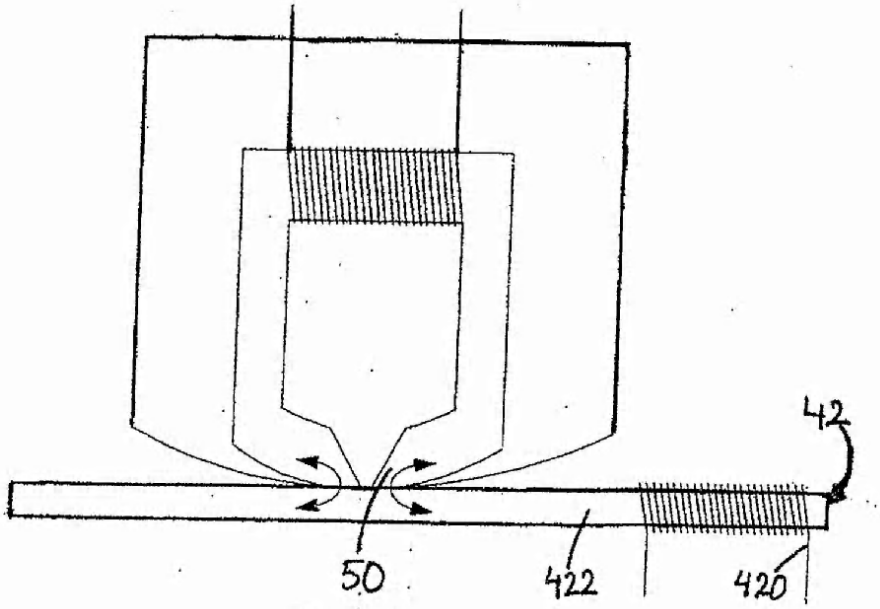

Fig.6

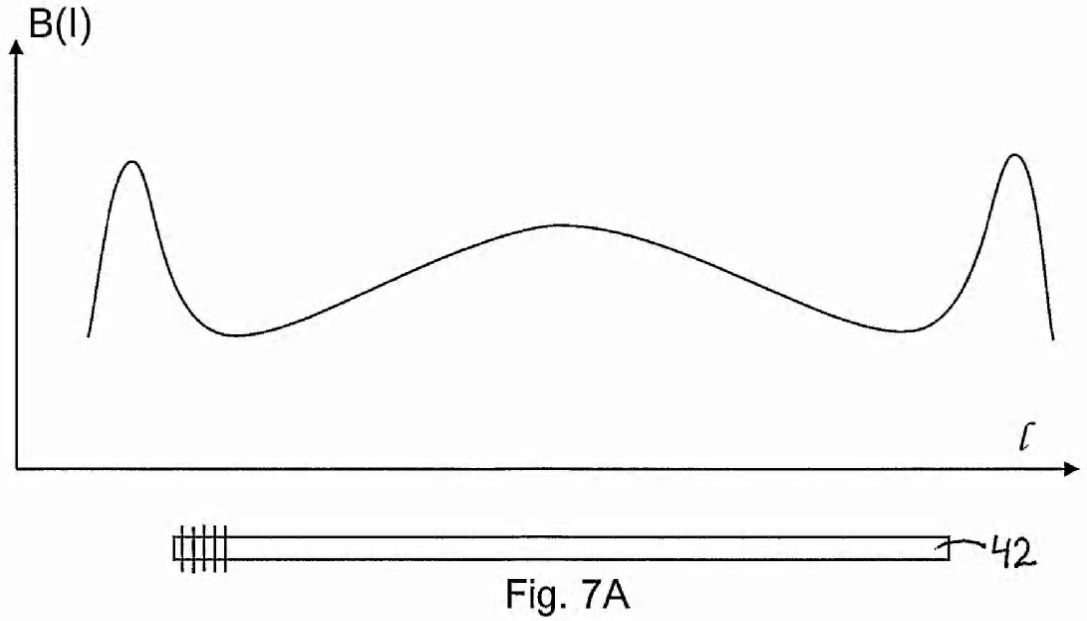

Fig. 7A

+

Fig. 7B

=

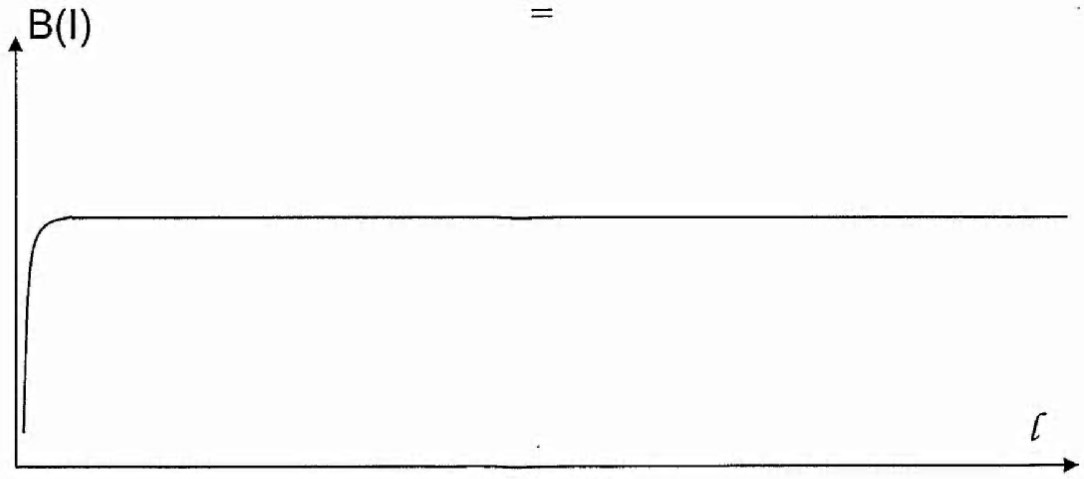

Fig. 7C