(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 663 538**

(51) Int. CI.:

G06F 9/445 (2006.01)
G06F 12/06 (2006.01)
G06F 12/14 (2006.01)
G06F 21/00 (2013.01)
G06Q 20/00 (2012.01)
G06F 21/35 (2013.01)
G06Q 20/34 (2012.01)
G06Q 20/40 (2012.01)
G07F 7/12 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **13.09.2010 E 10176449 (6)**

(97) Fecha y número de publicación de la concesión europea: **20.12.2017 EP 2302518**

(54) Título: **Procedimiento y dispositivo de instalación de una aplicación MIFARE en una memoria MIFARE**

(30) Prioridad:

14.09.2009 FR 0956297

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.04.2018

(73) Titular/es:

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

(72) Inventor/es:

DIALO, SOPHIE

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Procedimiento y dispositivo de instalación de una aplicación MIFARE en una memoria MIFARE

Antecedentes de la invención

La presente invención se sitúa en el campo de las tarjetas de microcircuitos (tarjetas de chips).

Se aplica en particular, y de manera no limitativa, a las tarjetas de microcircuitos adecuadas para comunicar con un lector de dicha tarjeta, para la implementación de una o varias aplicaciones (transacciones de pago, control de acceso, fidelización,…).

Se refiere más particularmente a las tarjetas de microcircuitos adecuadas para implementar una o varias aplicaciones MIFARE (marca registrada) de acuerdo con la norma ISO14443A.

El documento WO 2009/031065 describe un mecanismo que permite a un agente de software sustituir una aplicación MIFARE instalada en una memoria MIFARE, por otra aplicación MIFARE, siendo temporalmente memorizada esta otra aplicación MIFARE en una memoria denominada de “swap”.

Para efectuar esta sustitución, este documento muestra simplemente volver a copiar la segunda aplicación MIFARE en la memoria MIFARE.

Un mecanismo de ese tipo no permite desgraciadamente sustituir, utilizando los mecanismos clásicos del protocolo MIFARE, una aplicación por otra en una memoria MIFARE, puesto que estas aplicaciones proceden de suministradores diferentes.

La invención propone un mecanismo de instalación de una aplicación MIFARE que no presente este inconveniente.

Objeto y sumario de la invención

La invención se dirige más precisamente a un procedimiento y a un dispositivo de instalación de una aplicación MIFARE, a un programa de ordenador y a un soporte de registro de acuerdo con las reivindicaciones.

La invención se refiere también a un dispositivo portátil, por ejemplo un teléfono portátil, una tarjeta SIM o más generalmente a una tarjeta de microcircuitos, incluyendo este dispositivo portátil un dispositivo de instalación tal como se ha mencionado anteriormente y la zona de seguridad en la que este dispositivo de instalación obtiene las claves y datos de acceso habituales. Preferentemente, el dispositivo portátil según la invención incluye además la aplicación de gestión de la memoria MIFARE.

Es importante observar que la aplicación de gestión de la memoria MIFARE, paso obligado para acceder a la memoria MIFARE, no se modifica de ninguna manera por la implementación de la invención.

La invención resuelve efectivamente los inconvenientes del mecanismo de la técnica anterior, porque permite sustituir, en una memoria MIFARE, una primera aplicación MIFARE por una segunda aplicación MIFARE, incluso si estas proceden de suministradores diferentes.

En efecto, cuando una aplicación MIFARE actual se instala en la memoria MIFARE, el dispositivo de instalación según la invención puede obtener las claves y datos de acceso de esta aplicación habitual a partir de la zona de seguridad, y presentarlas a la aplicación clásica de gestión de la memoria MIFARE para que esta copie en la memoria MIFARE las claves y datos de acceso de la aplicación a instalar.

En un modo particular de realización, la zona de seguridad no puede leerse más que por el dispositivo de instalación según la invención y por la aplicación actual.

Se observará que el mecanismo presentado en el documento WO 2009/031065 de la técnica anterior es totalmente silencioso sobre este punto, e impone por tanto implícitamente que las claves y datos de acceso de la aplicación actual y de la aplicación a instalar sean idénticos o compartidos. En la práctica, esta restricción es inviable dado que se desea instalar unas aplicaciones MIFARE que proceden de suministradores diferentes.

En un modo de realización particular, al menos ciertas aplicaciones MIFARE que pueden instalarse en la memoria MIFARE se memorizan en un dominio de seguridad (en inglés “Security Domain”) tal como se define por la norma Globalplatform Card Specification v2.2, realizándose la obtención de las claves y datos de acceso actuales a partir de una zona de seguridad de este dominio de seguridad.

De una manera general, un dominio de seguridad es una aplicación memorizada en la memoria del chip de una tarjeta de chips, establecida a nombre de una entidad externa a la tarjeta, por ejemplo un suministrador de la aplicación o una autoridad de control.

Un dominio de seguridad ofrece unos servicios de seguridad tales como la gestión de claves, el cifrado, el descifrado y la generación y verificación de firmas a las aplicaciones presentes sobre la tarjeta así como a las entidades externas. Más precisamente, y según la norma antes mencionada, un dominio de seguridad incluye un conjunto de claves (en inglés “key-set”), no pudiendo accederse a estas claves más que por el dominio de seguridad, permitiendo este mecanismo a varios suministradores independientes prever unos servicios mientras se asegura que un suministrador no pueda acceder a las claves criptográficas de otro.

En este modo particular de realización, la invención propone de ese modo utilizar el conjunto de claves del dominio de seguridad de una aplicación MIFARE para memorizar las claves y datos de acceso propios de esta aplicación MIFARE, siendo el procedimiento y dispositivo de instalación según la invención adecuados para leer este conjunto de claves, cuando esta aplicación MIFARE se instala actualmente en la memoria MIFARE, para sustituirla por la otra.

Esta característica permite preservar una imagen fiel de la aplicación MIFARE actual antes de la sustitución.

La invención puede utilizarse también para instalar una primera aplicación MIFARE en una memoria MIFARE de una manera segura. En efecto, en un modo de realización particular de la invención, la memoria MIFARE está protegida por unas claves definidas durante una etapa de personalización de la memoria MIFARE, denominadas claves de inicialización, siendo memorizadas estas claves en una zona de seguridad y utilizándose para instalar la primera aplicación MIFARE en la tarjeta. En un modo particular de realización, esta zona de seguridad no puede ser leída más que por el dispositivo de instalación según la invención.

Se observará que este modo de realización refuerza considerablemente la seguridad de las tarjetas MIFARE, siendo estas proporcionadas tradicionalmente sin protección, por ejemplo inicializadas con unos valores de tipo “FF”.

En un modo particular de realización, las diferentes etapas del procedimiento de instalación se determinan mediante unas instrucciones de programas informáticos.

Como consecuencia, la invención se dirige también a un programa informático sobre un soporte de informaciones, siendo susceptible este programa de ser implementado en un terminal portátil, por ejemplo un teléfono, o más generalmente en un ordenador, incluyendo este programa unas instrucciones adaptadas para la implementación de las etapas del procedimiento de instalación tal como se ha mencionado anteriormente.

Este programa puede utilizar no importa qué lenguaje de programación, y estar en la forma de código fuente, código objeto, o código intermedio entre código fuente y código objeto, tal como en una forma parcialmente compilada, o en no importa qué otra forma deseable.

La invención se dirige también a un soporte de informaciones legible por un ordenador, y que incluye unas instrucciones de un programa informático tal como se ha mencionado anteriormente.

El soporte de informaciones puede ser no importa qué entidad o dispositivo capaz de almacenar el programa. Por ejemplo, el soporte puede incluir un medio de almacenamiento, tal como una ROM, por ejemplo un CD ROM o una ROM de circuito microelectrónico, o incluso un medio de registro magnético, por ejemplo un disquete (disco flexible) o un disco duro.

Por otro lado, el soporte de informaciones puede ser un soporte transmisible tal como una señal eléctrica u óptica, que puede encaminarse a través de un cable eléctrico u óptico, por radio o por otros medios. El programa según la invención puede en particular descargarse desde una red de tipo Internet.

Alternativamente, el soporte de informaciones puede ser un circuito integrado en el que se incorpora el programa, estando adaptado el circuito para ejecutar o para ser utilizado en la ejecución del procedimiento en cuestión.

Breve descripción de los dibujos

Surgirán otras características y ventajas de la presente invención de la descripción realizada a continuación, con referencia a los dibujos adjuntos que ilustran un ejemplo de realización desprovisto de cualquier carácter limitativo. En las figuras:

- la figura 1 representa una memoria MIFARE;
- la figura 2 representa un teléfono portátil que incluye, en una tarjeta de microcircuito, un dispositivo de instalación de acuerdo con un modo particular de realización de la invención; y

- la figura 3 representa, en forma de organigrama, las principales etapas de un procedimiento de instalación de acuerdo con un modo particular de realización de la invención.

Descripción detallada de un modo de realización

La figura 1 representa una memoria MIFARE 1340 organizada en dieciséis sectores de cuatro bloques cada uno, siendo el primer bloque (bloque 0) del primer sector (sector 0) un bloque especial reservado al fabricante y que incluye el número de serie de la memoria.

Cada sector 1 a 15 incluye tres bloques de datos 0 a 2, incluyendo el primer sector 0 dos bloques de datos 1 y 2.

En lo que sigue de la descripción, se denotará globalmente por D^1_i a los datos del sector i.

De acuerdo con el protocolo MIFARE, el acceso a los datos D^1_i de un sector i está protegido por dos claves y las condiciones de este acceso se definen por unos datos de acceso (en inglés Access Bits, “AB”), siendo memorizados las claves y los datos de acceso en el bloque 3 de este sector.

A título de ejemplo, el acceso de escritura o de lectura a los datos D^1_{15} de los datos del sector 15 está protegido por las claves K^1_{32} y K^1_{31} y definido por los datos de acceso AB^1_{15}.

En lo que sigue de la descripción, los datos D^i_i se denominarán “datos de aplicación” para distinguirlos sin ambigüedad de los datos de acceso AB^i_j.

La figura 2 representa de manera esquemática unos elementos de la arquitectura del hardware del teléfono portátil 2000.

Este teléfono portátil incluye principalmente una antena 1400 y un módulo de interfaz hombre-máquina 1500, estando conectados la antena y el módulo de interfaz hombre-máquina al procesador 1200 de una tarjeta SIM 1000.

La tarjeta SIM 1000 es una tarjeta de microcircuito de acuerdo con un modo de realización de la invención. Incluye una memoria 1300 no volátil reescribible por ejemplo de tipo EEPROM en la que se encuentra la memoria MIFARE 1340.

La tarjeta SIM 1000 incluye una memoria no volátil 1100 de tipo ROM en la que se memoriza una aplicación 1110 adecuada para implementar el protocolo MIFARE para acceder a la memoria MIFARE 1340.

Esta aplicación 1110 es un punto de paso obligado para acceder a la memoria MIFARE 1340.

Más precisamente, cuando una entidad desea acceder en lectura o en escritura a los datos de aplicación D^1_i del sector i de la memoria MIFARE 1340, esta entidad debe enviar un comando a la aplicación 1110, siendo acompañado este comando por una contraseña calculada partir de las claves y K^1_{2i+1} y unos datos de acceso AB^1_i con el fin de permitir a la aplicación 1110 autentificar a la entidad en cuestión a partir de las claves K^1_{2i} y K^1_{2i+1} y de unos datos de acceso AB^1_i memorizados en la memoria MIFARE 1340, por ejemplo según un mecanismo de reto/respuesta.

Es importante observar que la aplicación 1110 de gestión de la memoria MIFARE se ve como una “caja negra”, y que no se modifica de ninguna forma por la implementación de la invención.

En el ejemplo de realización descrito en este caso, la tarjeta SIM 1000 incluye, en la memoria EEPROM 1300, dos zonas de memoria 1310, 1320 asociándose cada una a una aplicación MIFARE que puede instalarse en la memoria MIFARE 1340.

De acuerdo con la invención, cada una de estas zonas de memoria 1310, 1320 incluye:

- una zona de seguridad 1311, 1321 en la que se memorizan las claves K y los datos de acceso AB para esta aplicación MIFARE; y
- una zona 1312, 1322 de seguridad o no, en la que se memorizan los datos de aplicación de esta aplicación MIFARE.

Dicho de otra manera, para instalar una aplicación MIFARE a partir de una zona de memoria 1310 por ejemplo, conviene:

- volver a copiar las claves K^i_j y los datos de acceso AB^i_j a partir de la zona de seguridad 1311 en los bloques 3 de los sectores de la memoria MIFARE 1340; y
- volver a copiar los datos de aplicación D^i_j de la zona 1312 de seguridad o no en los bloques 0 a 2 de la memoria MIFARE 1340.

En el modo de realización descrito en este caso, las zonas de memoria 1310, 1320 son unos dominios de seguridad (en inglés “Security Domains”) tal como se define por la norma Globalplatform Card Specification v2.2.

En el modo de realización descrito en este caso, las zonas de seguridad 1311, 1321 constituyen una subparte del conjunto de claves (key-set) de los dominios de seguridad 1310, 1320.

En el modo de realización descrito en este caso, la tarjeta SIM 1000 incluye, en la memoria no volátil 1100, una aplicación 1105 adecuada para instalar un nuevo dominio de seguridad 1360 (del tipo de 1310 y 1320) en la memoria EEPROM 1300.

De acuerdo con la norma Globalplatform Card Specification v2.2, esta aplicación 1105 es adecuada para:

- instanciar una zona de seguridad 1361 para recibir el conjunto de claves de la aplicación;
- verificar que la memoria EEPROM 1300 incluye suficiente espacio para acoger la zona de seguridad o no 1362, y si esto es así, para reservarla;
- recibir y volver a copiar el conjunto de claves de la aplicación en la zona de seguridad 1361; y
- recibir y volver a copiar los datos de esta aplicación en la zona de seguridad o no 1362.

En el modo particular de realización de la invención descrito en este caso, la memoria MIFARE 1340 se protege, durante una fase de personalización de la tarjeta SIM 1000, mediante las claves de inicialización KI_j, siendo memorizadas estas claves en una zona de seguridad 1305 y en los bloques 3 de los sectores de la memoria MIFARE. De ese modo, para poder instalar una primera aplicación en la memoria MIFARE 1340, es necesario, de acuerdo con el protocolo MIFARE, enviar un comando a la aplicación 1110, acompañado de una contraseña calculada a partir de estas claves de inicialización. Esto protege a la memoria MIFARE contra la instalación de una primera aplicación no deseada.

En el modo de realización descrito en este caso, la interfaz hombre-máquina 1500 ofrece al usuario del teléfono portátil 2000, unos medios, por ejemplo en la forma de un menú, para instalar una aplicación MIFARE a partir de una zona de memoria 1310, 1320, 1360 en la memoria 1340.

En el modo de realización descrito en este caso, este comando de instalación se recibe y trata mediante un software piloto 1313, 1323, 1363 desarrollado por la entidad que haya establecido la aplicación MIFARE.

Estos pilotos 1313, 1323, 1363 son adecuados para comunicar con la aplicación 1110 de gestión de la memoria MIFARE, única aplicación habilitada para acceder como lectura/escritura al contenido de la memoria MIFARE 1340.

Como se ha dicho anteriormente, en el modo de realización descrito en este caso, la memoria MIFARE 1340 está protegida en el origen por las claves inicialización KI_j memorizadas en la zona de seguridad 1305.

En consecuencia, la instalación de una primera aplicación 1310, 1320, 1360 en la memoria MIFARE 1340, necesita, de acuerdo con el protocolo MIFARE, la presentación de las claves de inicialización KI_j a la aplicación 1110 de gestión de la memoria MIFARE.

De la misma manera, la sustitución de una primera aplicación 1310 por una segunda aplicación 1320 en la memoria MIFARE 1340, necesita la presentación de las claves K^1_j y de los datos de acceso AB^1_j de la primera aplicación 1310 a la aplicación 1110 de gestión de la memoria MIFARE.

Con este fin, la tarjeta SIM 1000 incluye un dispositivo de instalación 1330 de acuerdo con la invención adecuado para:

- acceder a las zonas de seguridad 1305, 1311, 1321, 1361;
- identificar la aplicación MIFARE actualmente instalada en la memoria MIFARE 1340;
- recibir un comando del piloto de la aplicación que el usuario desea instalar en la memoria MIFARE 1340;
- recuperar las claves K^j_i y los datos de acceso AB^j_i de la aplicación MIFARE actualmente instalada en la memoria MIFARE 1340, o antes de la primera instalación, las claves de inicialización KI_j, siendo denominadas estas claves y datos de acceso “claves y datos de acceso actuales”; y
- recuperar las claves K^k_i y los datos de acceso AB^k_i de la aplicación MIFARE a instalar en la memoria MIFARE 1340, siendo denominadas estas claves y datos de acceso “nuevas claves y datos de acceso”; y
- enviar uno o varios comandos de acuerdo con el protocolo MIFARE a la aplicación 1110 de gestión de la memoria MIFARE 1340 para solicitarle copiar las nuevas claves y datos de acceso en la memoria MIFARE 1340 presentándole las claves y datos de acceso actuales necesarias para esta escritura.

Cada una de las zonas 1305, 1311, 1321, 1361 es de seguridad, lo que significa, en este modo de realización que:

- la zona 1305 no puede ser leída más que por el dispositivo de instalación 1330;
- la zona 1311 no puede ser leída más que por el dispositivo de instalación 1330 y por el piloto 1313;

- la zona 1321 no puede ser leída más que por el dispositivo de instalación 1330 y por el piloto 1323;
- la zona 1361 no puede ser leída más que por el dispositivo de instalación 1330 y por el piloto 1363.

En el modo de realización descrito en este caso, el dispositivo de instalación 1330 es un módulo adecuado para implementar el programa informático de acuerdo con la invención para implementar el procedimiento de instalación cuyas principales etapas se describirán a continuación con referencia a la figura 3.

En el modo de realización descrito en este caso, el dispositivo de instalación 1330 incluye una memoria no volátil reescribible 1370 en la que se memoriza un identificador ID de la aplicación MIFARE actualmente instalada en la memoria MIFARE 1340. Durante la personalización de la tarjeta SIM 1000, este identificador ID se inicializa con un valor NULL representativo del hecho de que no se ha instalado ninguna aplicación MIFARE en la memoria 1340.

En el modo de realización descrito en este caso, el piloto de la instalación MIFARE actualmente instalada (por ejemplo 1310) en la memoria MIFARE 1340 es adecuado para enviar uno o varios comandos MIFARE a la aplicación 1110 de gestión de la memoria MIFARE 1340 para leer el contenido de la memoria MIFARE 1340 y actualizar la zona 1312 de seguridad o no de su dominio de seguridad para guardar una imagen fiel de la aplicación MIFARE actual antes de la sustitución.

Con referencia a la figura 3, se describirá ahora un procedimiento de instalación de una aplicación MIFARE 1320 en la memoria MIFARE 1340.

Se supondrá que la aplicación MIFARE 1320 a instalar es un dominio de seguridad 1320 de la memoria EEPROM 1300. Si no es este el caso, esta aplicación MIFARE puede instalarse por la aplicación 1105 mediante la implementación del protocolo Globalplatform como ya se ha descrito.

En el transcurso de una etapa E10, el usuario elige, utilizando la interfaz hombre-máquina 1500 del teléfono portátil 2000 una aplicación MIFARE 1320 a instalar en la memoria MIFARE 1340.

Esta operación genera el envío, mediante la interfaz hombre-máquina 1500 de un comando al sistema operativo del teléfono portátil 2000. Este comando, es, en el modo particular de realización de la invención descrito en este caso, un comando SELECT de acuerdo con la norma ISO7816.

Tras la recepción de este comando, el sistema operativo envía un comando de selección al piloto 1323 de la aplicación seleccionada.

En el transcurso de una etapa E20, el piloto 1323 solicita al dispositivo de instalación 1330 copiar las claves K^2_i y los datos de acceso AB^2_i de la aplicación MIFARE 1320 en la memoria MIFARE 1340.

Para conocer la aplicación actualmente instalada en la memoria MIFARE 1340, el dispositivo de instalación 1330 lee la memoria no volátil reescribible 1370 (etapa E30) y obtiene el identificador ID. Se recuerda que no está instalada ninguna aplicación actualmente en la memoria MIFARE 1340, el identificador ID incluye un valor predeterminado NULL.

Se supone que la aplicación actualmente instalada es la aplicación MIFARE 1310.

En el modo de realización de la invención descrita en este caso, cuando el piloto 1323 recibe el comando SELECT, el sistema operativo envía, en el transcurso de una etapa E40, un comando de deselección al piloto 1313 de la aplicación MIFARE 1310 actualmente instalada en la memoria MIFARE 1340.

Con la recepción de este comando, el piloto 1313 guarda, enviando uno o varios comandos a la aplicación 1110 de gestión de la memoria MIFARE, los datos D^1_i de la aplicación MIFARE contenidos en los bloques 0 a 2 de los sectores 1 a 15 y 1 y 2 del sector 0 de la memoria MIFARE 1340 en la zona de seguridad o no 1312.

El diálogo entre el piloto 1313 y la aplicación 1110 de gestión de la memoria MIFARE para este guardado está de acuerdo con el protocolo MIFARE y es conocido por el experto en la materia.

En el transcurso de una etapa E50, el dispositivo de instalación 1330 lee las claves K^1_i y los datos de acceso AB^1_i actuales a partir de la zona de seguridad (conjunto de claves) 1311 del dominio de seguridad 1310.

En el transcurso de una etapa E60, el dispositivo de instalación 1330 lee las nuevas claves K^2_i y los nuevos datos de acceso AB^2_i a partir de la zona de seguridad (conjunto de claves) 1312 del dominio de seguridad 1320 correspondiente a la aplicación MIFARE a instalar.

En el transcurso de una etapa E70, el dispositivo de instalación 1330 presenta las claves K^1_i y los datos de acceso AB^1_i actuales a la aplicación 1110 de gestión de la memoria MIFARE para solicitarle copiar las nuevas claves K^2_i y datos de acceso AB^2_i en los bloques 3 de los sectores 0 a 15 de la memoria MIFARE 1340. El diálogo entre el

dispositivo de instalación 1330 y la aplicación 1110 de gestión de la memoria MIFARE 1340 está de acuerdo con el protocolo MIFARE.

En el transcurso de una etapa E80, el piloto 1323 solicita a la aplicación 1110 de gestión de la memoria MIFARE 1340 copiar los datos D^2_i de la aplicación 1320, que se encuentra en la zona de seguridad o no 1322, en los bloques 0 a 2 de los sectores 1 a 15 y 1 y 2 del sector 0 de la memoria MIFARE 1340. Con este fin, el piloto 1323 presenta, a la aplicación 1110 de gestión de la memoria MIFARE 1340, sus propias claves K^2_i y datos de acceso AB^2_i.

En el modo de realización descrito en este caso, la sustitución de una primera aplicación MIFARE por una segunda aplicación MIFARE se realiza directamente, es decir utilizando las claves de la primera aplicación MIFARE para escribir las de la segunda aplicación MIFARE en la memoria 1340.

Como variante, se puede utilizar un juego de claves temporal, memorizado en una zona de seguridad en el sentido de la invención. De ese modo, la sustitución de una primera aplicación MIFARE por una segunda aplicación MIFARE se realiza en dos tiempos:

- en un primer tiempo, se escriben las claves temporales en la memoria 1340 utilizando las claves de la primera aplicación MIFARE; posteriormente,
- en un segundo tiempo, se escriben las claves de la segunda aplicación MIFARE utilizando las claves temporales.

En el modo de realización descrito anteriormente, la aplicación 1110 de gestión de la memoria MIFARE, las zonas de seguridad 1305, 1311, 1321, 1361 y el dispositivo 1330 de instalación estaban incorporados en la tarjeta SIM 1000.

Como variante, al menos uno de estos elementos está en el teléfono portátil 2000, en el exterior de la tarjeta SIM.

REIVINDICACIONES

1. Procedimiento de instalación de la aplicación MIFARE en una memoria MIFARE (1340), estando la aplicación MIFARE de acuerdo con la norma ISO 14443A y memorizada en un dominio de seguridad (1320) tal como se define por la norma Globalplatform Card Specification v2.2, incluyendo el procedimiento:

- una etapa (E50) de obtención, a partir de una zona de seguridad (1305, 1311) de una clave de inicialización (Klj) para la instalación de una primera aplicación (1310) o de una clave (K1i) y unos datos de acceso (AB1i) de la primera aplicación (1310) para la sustitución de la primera aplicación (1310) por una segunda aplicación (1320) en la memoria MIFARE (1340) protegiendo el acceso a dicha memoria MIFARE (1340), denominados “claves y datos de acceso actuales”; y
- una etapa de obtención (E60) de al menos una nueva clave (K2i) y unos datos de acceso (AB2i) correspondientes a la aplicación MIFARE a instalar, denominados “nuevas claves y datos de acceso”;
- una etapa (E70) de envío según el protocolo MIFARE de dichas claves y datos de acceso actuales a una aplicación (1110) de gestión de la memoria MIFARE (1340), siendo dicha aplicación (1110) un punto de paso obligado para acceder a la memoria MIFARE (1340) y de envío de al menos una instrucción que desencadena la copia por dicha aplicación (1110) de gestión de dichas nuevas claves y datos de acceso en dicha memoria MIFARE (1340) utilizando dichas claves y datos de acceso actuales; y
- una etapa de envío de un comando a la aplicación (1110) de gestión de la memoria MIFARE (1340) que desencadena la copia de los datos (D2i) de la aplicación MIFARE a instalar en la memoria MIFARE (1340) utilizando dichas nuevas claves y datos de acceso.

2. Procedimiento de instalación de una aplicación MIFARE (1320) según la reivindicación 1, caracterizado por que dichas claves y datos de acceso actuales son unas claves (K1i) y unos datos de acceso (AB1i) de una aplicación MIFARE actual (1310) instalada en dicha memoria MIFARE (1340) para la sustitución de la aplicación MIFARE actual (1310) por una segunda aplicación MIFARE (1320) en dicha memoria MIFARE (1340).

3. Procedimiento de instalación de una aplicación MIFARE (1320) según la reivindicación 2, en la que dicha aplicación MIFARE actual (1310) se memoriza en otro dominio de seguridad (1310), caracterizado por que dicha etapa (E50) de obtención de las claves y datos de acceso actuales se realiza a partir de una zona de seguridad (1311) de este dominio de seguridad.

4. Procedimiento de instalación de una aplicación MIFARE (1310) según la reivindicación 1, caracterizado por que dichas claves y datos de acceso actuales son unas claves de inicialización (Klj) definidas durante una etapa de personalización de dicha memoria (1340).

5. Procedimiento de instalación de una aplicación MIFARE (1320) según una cualquiera de las reivindicaciones 1 a 4, caracterizado por que dicha instalación se efectúa tras la recepción (E10) de un comando generado a consecuencia del envío de un comando de selección de dicha aplicación MIFARE (1320) de acuerdo con el comando SELECT de la norma ISO7816.

6. Dispositivo (1330) de instalación de una aplicación MIFARE en una memoria MIFARE (1340), estando la aplicación MIFARE de acuerdo con la norma ISO 14443A y memorizada en un dominio de seguridad (1320) tal como se define por la norma Globalplatform Card Specification v2.2, estando el dispositivo caracterizado por que incluye:

- unos medios de obtención de una clave de inicialización (Klj) para la instalación de una primera aplicación (1310) o de una clave (K1i) y unos datos de acceso (AB1i) de la primera aplicación (1310) para la sustitución de la primera aplicación (1310) por una segunda aplicación (1320) en la memoria MIFARE (1340) protegiendo el acceso a dicha memoria MIFARE (1340), denominados “claves y datos de acceso actuales”; y
- unos medios de obtención según el protocolo MIFARE de al menos una nueva clave (K2i) y unos datos de acceso (AB2i) correspondientes a la aplicación MIFARE a instalar, denominados “nuevas claves y datos de acceso”;
- unos medios de envío según el protocolo MIFARE de dichas claves y datos de acceso actuales a una aplicación (1110) de gestión de la memoria MIFARE (1340), siendo dicha aplicación (1110) un punto de paso obligado para acceder a la memoria MIFARE (1340) y de envío de al menos una instrucción que desencadena la copia por dicha aplicación (1110) de gestión de dichas nuevas claves y datos de acceso en dicha memoria MIFARE (1340), utilizando dichas claves y datos de acceso actuales; y
-unos medios de envío de un comando a la aplicación (1110) de gestión de la memoria MIFARE (1340) que desencadena la copia de los datos (D2i) de la aplicación MIFARE a instalar en la memoria MIFARE (1340) utilizando dichas nuevas claves y datos de acceso.

7. Dispositivo portátil (1000, 2000) que incluye un dispositivo de instalación de una aplicación MIFARE según la reivindicación 6 y dicha zona de seguridad (1305, 1311).

8. Dispositivo portátil (1000, 2000) según la reivindicación 7, caracterizado por que incluye además dicha aplicación (1110) de gestión de dicha memoria MIFARE (1340).

9. Dispositivo portátil (1000, 2000) según la reivindicación 7 u 8, caracterizado por que está constituido por un teléfono portátil (200) o una tarjeta de microcircuitos (1000).

10. Programa informático que incluye unas instrucciones para la ejecución de las etapas del procedimiento de instalación según una cualquiera de las reivindicaciones 1 a 5 cuando dicho programa se ejecuta por un ordenador.

11. Soporte de registro legible por un ordenador en el que está registrado un programa informático que comprende unas instrucciones para la ejecución de las etapas del procedimiento de instalación según una cualquiera de las reivindicaciones 1 a 5, cuando dicho programa se ejecuta por un ordenador.

Sector	Bloque	N.º de octeto en el bloque														
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
15	3	K^1_{32}						AB^1_{15}				K^1_{31}					
	2	D^1_{15}															
	1																
	0																
14	3	K^1_{28}						AB^1_{14}				K^1_{29}					
	2	D^1_{14}															
	1																
	0																
...	...	...															
	...																
	...																
	...																
1	3	K^1_2						AB^1_1				K^1_2					
	2	D^1_1															
	1																
	0																
0	3	K^1_0						AB^1_0				K^1_1					
	2	D^1_0															
	1																
	0	Bloque fabricante															

FIG. 1

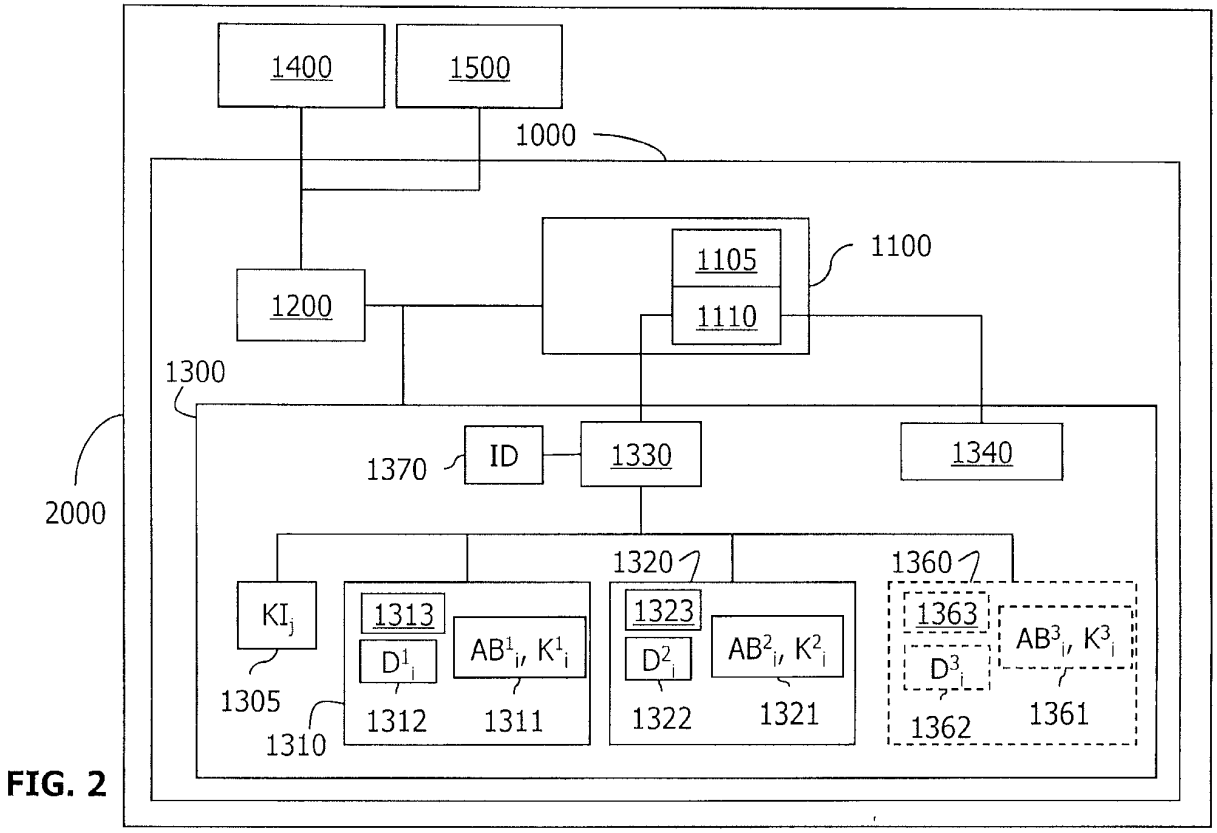

FIG. 2

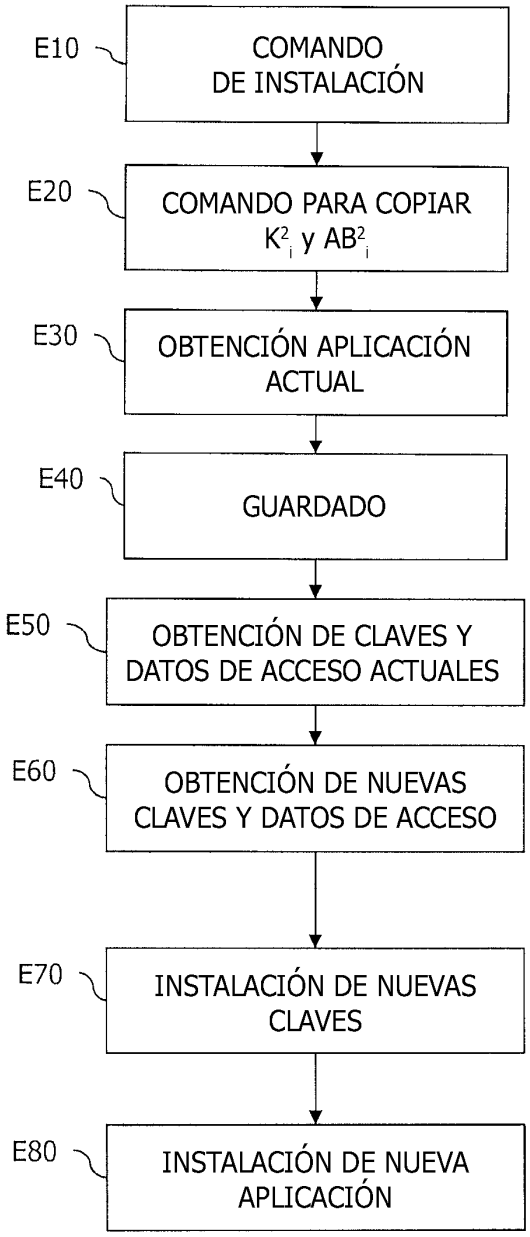
E10
COMANDO DE INSTALACIÓN
E20
COMANDO PARA COPIAR K^2_i y AB^2_i
E30
OBTENCIÓN APLICACIÓN ACTUAL
E40
GUARDADO
E50
OBTENCIÓN DE CLAVES Y DATOS DE ACCESO ACTUALES
E60
OBTENCIÓN DE NUEVAS CLAVES Y DATOS DE ACCESO
E70
INSTALACIÓN DE NUEVAS CLAVES
E80
INSTALACIÓN DE NUEVA APLICACIÓN

FIG. 3