(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 328 484**

(51) Int. Cl.:
G07F 7/10 (2006.01)
G06K 19/073 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **04735235 .6**
(96) Fecha de presentación : **28.05.2004**
(97) Número de publicación de la solicitud: **1634252**
(97) Fecha de publicación de la solicitud: **15.03.2006**

(54) Título: **Procedimiento para cargar datos en soportes de datos portátiles.**

(30) Prioridad: **03.06.2003 DE 103 24 995**

(45) Fecha de publicación de la mención BOPI:
13.11.2009

(45) Fecha de la publicación del folleto de la patente:
13.11.2009

(73) Titular/es: **Giesecke & Devrient GmbH**
Prinzregentenstrasse 159
81677 München, DE

(72) Inventor/es: **Flammensböck, Christian;**
Patzke, Hagen y
Ebner, Claus

(74) Agente: **Durán Moya, Luis Alfonso**

DESCRIPCIÓN

Procedimiento para cargar datos en soportes de datos portátiles.

La presente invención se refiere a un procedimiento para cargar datos en soportes de datos portátiles.

Los soportes de datos portátiles, en especial las tarjetas de chip, tienen múltiples utilizaciones, por ejemplo, para efectuar transacciones de pago, como documentos de identificación en controles de acceso, como prueba de autorización para el uso de un sistema de telefonía móvil, etc. Antes de que se pueda usar un soporte de datos portátil en una aplicación, generalmente es necesario, durante una inicialización y subsiguiente personalización, cargar datos en una memoria no volátil del soporte de datos portátil. Durante la inicialización se registran en la memoria no volátil, por ejemplo, complementos de un sistema operativo almacenado en una memoria permanente del soporte de datos portátil, y se establecen estructuras de datos. Además, se prepara la posterior personalización. En la medida de lo posible, los datos se escriben en la memoria no volátil mediante especificaciones externas de direcciones de memoria físicas, a fin de reducir al mínimo el tiempo necesario para la escritura. Se intenta que la escritura sea lo más rápida posible porque el aumento del tiempo que requiere la escritura de los datos, por regla general, incrementa los costes de inicialización y de personalización.

Durante la personalización, en la memoria no volátil se instalan, por ejemplo, aplicaciones y se escriben datos relativos a personas, de manera que generalmente no se conocen las direcciones de memoria físicas. Por ello, los datos se escriben en la memoria no volátil sin especificaciones externas de las direcciones físicas, y es el soporte de datos portátil el que, en cada caso, decide qué datos se cargan, de qué forma y en cuál de las direcciones físicas. Con ello se evita de forma segura, por ejemplo, que se sobreescriban posiciones de memoria que aún son necesarias, ya que en todo momento es conocida la asignación de posiciones de memoria dentro del soporte de datos portátil. Sin embargo, la escritura en la memoria con este procedimiento tiene un coste de tiempo elevado cuando la cantidad de datos es grande.

El documento WO 00/52635 da a conocer una posible realización de la escritura de datos en una tarjeta de chip, con o sin especificaciones externas de direcciones de memoria físicas. A fin de reducir el tiempo necesario para escribir los datos de personalización en una tarjeta de chip, en dicho documento se propone dotar a la tarjeta de chip de una interfaz de memoria separada. La interfaz de memoria separada está conectada eléctricamente con los contactores externos del chip, de modo que la memoria es directamente accesible derivando o puenteando el microprocesador de la tarjeta de chip. Mediante elementos conmutadores, integrados en un programa de control de la memoria, se puede conmutar entre una modalidad de carga directa y una modalidad de carga asistida por el microprocesador. En la modalidad de carga asistida por el microprocesador, los datos se transmiten asincrónicamente al microprocesador, desde un dispositivo de personalización a una frecuencia de reloj predeterminada por el microprocesador, y se escriben en la memoria con intervención del microprocesador. En la modalidad de carga directa, los datos se almacenan en la memoria directamente desde el dispositivo de personalización, de modo que la transmisión de datos se realiza sincrónicamente a una frecuencia de transmisión prefijada por el dispositivo de personalización.

En principio, la modalidad de carga directa permite reducir considerablemente el tiempo necesario para la personalización, en comparación con la modalidad de carga asistida por el microprocesador. No obstante, la premisa para ello es que en cada caso se conozca la manera en que se han de guardar los datos en la memoria. Sin embargo, por lo general, el dispositivo de personalización no puede prefijar libremente la ocupación física de la memoria, sino que esto depende del perfil de personalización previsto en cada caso. Así pues, para poder emplear la modalidad de carga directa se debería preparar un procedimiento de personalización propio para cada perfil de personalización y, durante la personalización, interrogar en cada caso uno de dichos procedimientos de personalización. Esto comportaría un coste muy elevado. Por otra parte, por lo general, también dentro de un mismo perfil de personalización, el contenido de, como mínimo algunos de los datos de personalización, es diferente para distintas tarjetas de chip, lo que plantea dificultades adicionales. Así pues, la utilización en la práctica de la modalidad de carga directa en la personalización de tarjetas de memoria conlleva problemas importantes.

Tal como se menciona en "Handbuch der Chipkarten" ("Manual de las tarjetas de chip"), Wolfgang Rankl/Wolfgang Effing, 4ª Edición (2002), p. 645-648, que constituye el preámbulo de las reivindicaciones independientes, en principio, mediante programas de simulación adecuados, es posible representar a la tarjeta de chip para determinar las direcciones de la memoria. No obstante, debido al elevado coste que requiere, este procedimiento sólo es adecuado de forma muy limitada. Por ello, en dicha publicación se propone inicializar mediante instrucciones lógicas una tarjeta de chip, que en una zona de memoria, de otro modo no utilizada, contiene un programa de vaciado, es decir, sin especificación externa de las direcciones de memoria físicas. Seguidamente, se lee con el programa de vaciado la memoria inicializada, y los datos conseguidos se escriben en las direcciones físicas de las tarjetas de chip a inicializar.

El documento DE 199 39 290 A1 da a conocer un concepto de personalización para tarjetas de chip de aplicaciones múltiples, según el cual, con ayuda de bloques de datos de descripción de la aplicación, por una parte, y de bloques de datos de descripción de personalización, por otra, se asegura que cada una de las varias aplicaciones de la tarjeta de chip sólo puede acceder a los campos de datos de personalización que le han sido asignados.

Adicionalmente, el documento DE 195 36 548 A1 da a conocer un concepto de personalización para tarjetas de chip con una fase de inicialización y una subsiguiente fase de personalización, de modo que la personalización se

realiza con la ayuda de tablas de personalización. El objeto del documento es sobre todo la creación de herramientas de inicialización, de personalización y de comunicación con una tarjeta de chip.

El documento WO 01/95271 A1 da a conocer un procedimiento para la personalización de tarjetas de chip que se basa en un texto fuente de aplicación a personalizar. La solución descrita se basa en el planteamiento de realizar totalmente el registro de alta antes de cargar la tarjeta de chip, a fin de poder poner la aplicación sobre la tarjeta de chip en una única etapa de personalización. Se propone marcar adecuadamente con datos de personalización sectores del texto fuente de la aplicación durante la confección del programa, identificar los sectores marcados mediante un dispositivo de reconocimiento, y luego introducir en los sectores identificados los datos de personalización desde una base de datos. La aplicación personalizada obtenida es compilada o interpretada directamente en la tarjeta de chip.

La presente invención tiene por objeto reducir el tiempo y el coste de la personalización de soportes de datos portátiles.

Este objetivo se consigue con un procedimiento que presenta la combinación de características de la reivindicación 1 o bien de la reivindicación 13.

En el procedimiento, según la invención, para cargar datos en soportes de datos portátiles, en una memoria no volátil de un primer soporte de datos portátil se escriben los datos generales, idénticos para varios soportes de datos portátiles, sin especificación externa de las direcciones de memoria físicas. Posteriormente, se lee un contenido de memoria, como mínimo, de un sector parcial de la memoria no volátil del primer soporte de datos portátil, y para dicho sector parcial se genera una imagen de memoria, incluyendo las direcciones de memoria físicas que le corresponden. Finalmente, utilizando las correspondientes direcciones de memoria físicas, se escribe la imagen de memoria en las memorias no volátiles de soportes de datos portátiles adicionales. La particularidad del procedimiento, según la invención, radica en que, después de la inscripción de la imagen de memoria en la memoria no volátil de cada uno de los soportes de datos portátiles adicionales, éstos ejecutan una rutina de reconversión para reconvertir la memoria no volátil cargada con la imagen de memoria.

La invención presenta la ventaja de que, cuando se cargan datos en los soportes de datos portátiles, se consiguen tiempos de carga muy breves, con medios sencillos y sin costosos trabajos de preparación. Sin embargo, gracias a la rutina de reconversión prevista según la invención, se dispone de posibilidades de configuración en lo que respecta a la ocupación de la memoria no volátil de los soportes de datos portátiles.

Los datos generales pueden contener, por ejemplo, software de aplicaciones, en especial paquetes JAVA y applets JAVA. Durante una inicialización del primer soporte de datos portátil, en la memoria no volátil del primer soporte de datos se puede escribir una rutina de lectura para leer la memoria no volátil, o bien los datos adicionales imprescindibles para la ejecución de la rutina de lectura. Durante la inicialización, también se puede almacenar la rutina de reconversión en la memoria no volátil del primer soporte de datos portátil.

El procedimiento, según la inversión, puede estar configurado de manera que el contenido de la memoria no volátil del primer soporte de datos portátil solamente se lea si previamente se ha ejecutado con éxito una comprobación de seguridad. De este modo se puede evitar una lectura no autorizada y el uso indebido que esto puede conllevar. Por los mismos motivos, se puede prever que el contenido leído de la memoria no volátil del primer soporte de datos portátil esté codificado. Otras medidas de seguridad pueden consistir en que sólo se permita realizar una sola vez la generación de la imagen de la memoria no volátil del primer soporte de datos portátil, y que la rutina de lectura destinada a leer la memoria no volátil del primer soporte de datos portátil y los datos adicionales imprescindibles para la ejecución de la rutina de lectura se borren después de la generación de la imagen de memoria. Por regla general, la imagen de memoria sólo se descodifica antes de la escritura en la memoria no volátil de cada uno de los otros soportes de datos portátiles.

La reconversión de las memorias no volátiles de los otros soportes de datos portátiles se puede realizar de forma específica para cada soporte de datos. De esta manera, a pesar de que se utiliza la misma imagen de memoria para todos los soportes de datos portátiles adicionales, se puede conseguir una ocupación de memoria individualizada. Por ejemplo, durante la reconversión de la memoria no volátil de los soportes de datos portátiles adicionales es posible generar números aleatorios y codificar los datos almacenados. Después de la reconversión de las memorias no volátiles de los soportes de datos portátiles adicionales, se pueden escribir los datos individuales específicos de cada soporte de datos portátil en la memoria no volátil del mismo, sin una especificación externa de la dirección de memoria física.

En especial, mediante el procedimiento según la invención, se pueden cargar datos en soportes de datos portátiles configurados como tarjetas de chip.

A continuación, se explica la invención con referencia al ejemplo de realización representado en los dibujos, referido a la escritura de datos en una tarjeta de chip JAVA.

En los dibujos:

- la figura 1 muestra esquemáticamente la arquitectura de una tarjeta de chip;

- la figura 2 muestra un diagrama de flujo para generar una imagen de memoria de una memoria no volátil de una primera tarjeta de chip;

- la figura 3 muestra un diagrama de flujo que ilustra el procedimiento, según la invención, para la inicialización y personalización de tarjetas de chip adicionales utilizando la imagen de memoria; y

- la figura 4 muestra un diagrama de flujo de una variante del procedimiento según la invención, para la inicialización y personalización de tarjetas de chip.

La figura 1 muestra una representación esquemática de la arquitectura de una tarjeta de chip (1), en la que se puede utilizar el procedimiento según la invención. La tarjeta de chip (1) comprende una unidad de control (2), que controla la ejecución de las funciones de la tarjeta de chip (1). La unidad de control (2) está conectada a una unidad de entrada/salida (3), a una memoria permanente (4), a una memoria no volátil (5) y a una memoria volátil (6).

La unidad de entrada/salida (3) sirve para la comunicación con aparatos externos, que se puede realizar mediante la conexión por contacto de la tarjeta de chip (1) o mediante conexión inalámbrica. En la memoria permanente (4) están almacenados datos que permanecen inalterados durante toda la vida de la tarjeta de chip (1). El término "datos" se utiliza en lo sucesivo de forma muy general para cualquier clase de información, con independencia de su contenido, e incluye, por ejemplo, programas, parámetros, especificaciones relativas a personas, claves, etc. En especial, en la memoria permanente (4) está almacenado el sistema operativo de la tarjeta de chip (1). La memoria volátil (6) sirve de memoria de trabajo para la unidad de control (2). En la memoria volátil (6) el contenido de la memoria sólo se conserva durante el tiempo en que la tarjeta de chip (1) recibe tensión de alimentación. En la memoria no volátil (5) se puede volver a escribir durante toda la vida útil de la tarjeta de chip (1). El contenido correspondiente se conserva aunque la tarjeta de chip (1) no reciba tensión de alimentación. En la memoria no volátil (5) se cargan, por ejemplo, complementos del sistema operativo, software de aplicaciones, claves, datos de personas, etc. Estos datos se escriben en la memoria no volátil (5) antes de la entrega de la tarjeta de chip (1) al cliente y transforman la tarjeta de chip (1), que hasta ese momento sólo estaba equipada con algunas funciones básicas, en un producto generalmente muy complejo que dispone de todas las funcionalidades e informaciones necesarias para cada una de las aplicaciones previstas. Por lo general, esto hace que en la memoria no volátil (5) se deba cargar una cantidad de datos muy elevada.

Tal como se explicará con más detalle a continuación, el procedimiento según la invención se refiere a la escritura de datos en la memoria no volátil (5) antes de la entrega de la tarjeta de chip (1) al cliente. La escritura se realiza, en parte, a una velocidad muy elevada durante una rutina de preparación ejecutada durante la inicialización de la tarjeta de chip (1) y, en parte, durante una rutina de personalización comparativamente lenta, de modo que el procedimiento según la invención hace posible escribir la mayor parte de los datos durante la rutina de preparación. En la rutina de preparación, los datos se escriben en la memoria no volátil (5) con especificaciones externas de las direcciones físicas de memoria correspondientes. Esto significa que se transmiten a la tarjeta de chip (1) no sólo los propios datos, sino también las direcciones de memoria físicas correspondientes a los mismos. Por ello, antes de la ejecución de la rutina de preparación, todos los datos a escribir con la rutina de preparación y sus direcciones de memoria físicas se agrupan formando una imagen de memoria. En relación con la figura 2 se explica la generación de la imagen de memoria.

La figura 2 muestra un diagrama de flujo para generar la imagen de memoria. La imagen de memoria sólo necesita ser creada una vez con ayuda de una primera tarjeta de chip (1), y luego se puede escribir en muchas tarjetas de chip (1) adicionales. No obstante, se debe prestar atención a que la primera tarjeta de chip (1) no salga del proceso de producción. En una primera etapa (S1), se inicializa del modo habitual la primera tarjeta de chip (1), es decir, en especial, se añade una rutina de preparación con los datos habituales previstos para ello. Adicionalmente a los datos habituales, en el procedimiento según la invención, junto con la rutina de preparación se escriben otros datos en la memoria no volátil (5) de la tarjeta de chip (1). Estos otros datos representan una rutina de lectura destinada a leer la memoria no volátil (5) de la primera tarjeta de chip (1), una rutina de reconversión, una clave de lectura y una clave de carga, cuya significación se explicará con más detalle a continuación.

En lugar de la rutina de lectura, los otros datos también pueden comprender sólo los datos adicionales imprescindibles para la ejecución de la rutina de lectura. En este caso, la propia rutina de lectura ya está disponible en la memoria permanente (4), y se puede ejecutar en combinación con los datos adicionales. En caso de que dicha rutina de lectura ya esté almacenada en la memoria permanente (4), para la rutina de preparación se puede prescindir de las claves como parte de los datos adicionales. De hecho, los datos adicionales para la rutina de preparación contienen un indicador que señala que los datos están previstos para una variante del proceso de escritura según la invención.

Para poder insertar los otros datos mencionados en el juego de datos generalmente previsto para la preparación, en primer lugar se codifica este juego de datos. Seguidamente, se realizan las inserciones y se efectúa una codificación de los resultados. Esta combinación de datos para la preparación se puede realizar durante el proceso de producción dentro del cual se ejecuta la rutina de preparación, o bien de forma separada del mismo en un momento anterior, de forma que para el proceso de producción ya están preparados los datos finales elaborados.

A la etapa (S1) sigue la etapa (S2), en la que se realiza una personalización de la primera tarjeta de chip (1). No obstante, esta personalización se limita a la escritura en la memoria no volátil (5) de la primera tarjeta de chip (1), de solamente aquellos datos que están previstos para varias tarjetas de chip (1) y que, en lo sucesivo, se denominan datos generales. En todos los casos, la escritura se realiza sin especificación externa de la dirección de memoria física. Como datos generales, se pueden escribir de esta manera en la memoria no volátil (5) de la tarjeta de chip (1), entre otros, datos generales de personas, paquetes JAVA, applets JAVA, etc. También es adecuado incluir en la tarjeta las claves necesarias para los cálculos criptográficos de las utilizaciones de la tarjeta previstas. A fin de conseguir con el procedimiento según la invención la máxima utilidad posible, en la etapa (S2) se deberían escribir en la memoria no volátil (5) de la primera tarjeta de chip (1) el mayor número posible de datos generales. Solamente no se escriben durante la personalización según la etapa (S2) los datos individuales específicos previstos correspondientes a cada una de las tarjetas de chip (1).

Las claves incorporadas a las tarjetas y, adecuadamente, también los demás datos incluidos en la tarjeta de chip (1), no se almacenan como texto legible sino codificado. La codificación se realiza, por ejemplo, mediante una transformación con vinculación a valores aleatorios.

Para asegurar la posterior incorporación de los datos individuales específicos de la tarjeta, es conveniente que en la etapa (S2), junto con los datos generales, se escriban otras claves en la memoria no volátil (5) de la tarjeta de chip (1). Estas claves adicionales se utilizarán durante la incorporación de los datos individuales específicos de una tarjeta, para realizar una verificación o una autenticación recíproca.

Después de la personalización, en una etapa subsiguiente (S3) se comprueba si está permitida la lectura de la memoria no volátil (5) de la tarjeta de chip (1) mediante la rutina de lectura. Esta comprobación puede estar prevista de manera que la clave de lectura almacenada en la memoria no volátil (5), o bien en la memoria permanente (4), se compara con un valor introducido. Debido a las elevadas exigencias de seguridad, se permite sólo un intento de introducción. Adicionalmente, mediante una conexión conductora que se puede destruir de forma irreversible, es posible, por ejemplo, comprobar si se trata de una primera lectura de la memoria no volátil (5).

Si la comprobación conduce a un resultado positivo, es decir, cuando la verificación de la clave de lectura tiene éxito o cuando se trata de una primera lectura, se pasa de la etapa (S3) a una etapa (S4), en la que se borran los datos y rótulos de estado que, para la protección de la rutina de lectura, se encuentran en la memoria no volátil (5) de la primera tarjeta de chip (1), y que sólo se necesitan para la activación pero no para la ejecución corriente de la rutina de lectura, así como, en su caso, un marcador de posición previsto, de modo que se impide un eventual uso futuro no autorizado de la rutina de lectura.

Por otra parte, inmediatamente antes de la salida del primer bloque de datos, la rutina de lectura ajusta el estado interno de la tarjeta de chip (1) a un valor que se corresponde con el de una tarjeta de chip recién fabricada. De esta forma, para una utilización normal no autorizada, la tarjeta de chip (1) se debería someter a una nueva inicialización completa. Con ello, se impide de manera segura una utilización normal de la tarjeta de chip (1) con una ocupación no modificada de la memoria.

De este modo, la tarjeta de chip (1) queda asegurada contra un uso no autorizado, incluso si durante el proceso de lectura se produce un corte de corriente. También es posible realizar un corte irreversible de una conexión conductora, mediante el cual es posible determinar sin lugar a dudas que la rutina de lectura ya se ha ejecutado.

Tras la etapa de seguridad (S4) sigue una etapa (S5), en la que se lee la memoria no volátil (5) de la primera tarjeta de chip (1). Comenzando en cada caso con una dirección de memoria física definida, se lee un sector parcial definido de la memoria no volátil (5) y se escribe en un registro tampón de la primera tarjeta de chip (1). El contenido de memoria así determinado se combina con la dirección de memoria física y se codifica con la ayuda de la clave de carga almacenada para ello en la memoria permanente (4) o en la memoria no volátil (5) de la primera tarjeta de chip (1). A continuación, la secuencia de datos codificada así generada se transmite a la unidad de entrada/salida (3) de la primera tarjeta de chip (1) y se entrega a un dispositivo de personalización externo. Seguidamente, se lee de la misma manera otro sector parcial de la memoria no volátil (5), comenzando por una dirección de memoria física más alta.

Esta forma de proceder se repite hasta que se ha leído todo el contenido de la memoria no volátil (5). Es adecuado omitir los contadores de transacciones. También se omiten las áreas vacías, que en las tarjetas de chip (1) adicionales a personalizar ya están correctamente ocupadas, gracias a una instrucción de lectura ejecutada para ellas.

Todos los datos leídos se transfieren al dispositivo de personalización en una forma codificada con la clave de carga. Cada uno de los datos secretos leídos, en especial, también la aplicación de la rutina de lectura y los datos adicionales imprescindibles para la ejecución de la rutina de lectura, es sustituido por un valor prefijado, o bien ni siquiera se le da salida, para evitar lecturas no autorizadas.

En el dispositivo de personalización externo, las secuencias de datos codificadas recibidas se deben componer para conformar la imagen de memoria. Para ello, las secuencias de datos no necesitan ser descodificadas, sino que se pueden guardar con una forma que se pueda utilizar directamente para cargarlas en tarjetas de chip adicionales.

Para evitar eficazmente un uso no autorizado, se puede añadir después de la lectura una etapa (S6), en la que se realiza el borrado físico de la rutina de lectura.

Con la etapa (S6) concluye el ciclo del diagrama de flujo. También se llega a la etapa (S5) directamente desde la etapa (S3) cuando la comprobación allí realizada conduce a un resultado negativo.

La imagen de memoria de la memoria no volátil (5) de la tarjeta de chip (1), generada con el proceso representado en la figura 2, se transfiere a múltiples tarjetas de chip (1) adicionales, en las que posteriormente, para completar la personalización, sólo se escriben unos pocos datos individuales. Esta forma de proceder se representa en la figura 3.

La figura 3 muestra un diagrama de flujo que ilustra la forma de proceder, según la invención, para la inicialización y personalización de tarjetas de chip (1) adicionales mediante la imagen de memoria. Al contrario que en la figura 2, esta forma de proceder se utiliza no en la primera tarjeta de chip (1), sino en múltiples tarjetas de chip (1) adicionales que, de esta manera, reciben todos los datos necesarios para la posterior utilización de las tarjetas de chip (1).

El recorrido del diagrama de flujo comienza con una primera etapa (S7), en la que se comprueba si es admisible inscribir la imagen de memoria en la memoria no volátil (5) de la tarjeta de chip (1). Esto, se puede realizar de forma similar a la lectura de la memoria no volátil (5), representada en la figura 2, para generar la imagen de memoria, por ejemplo, de manera dependiente del resultado de una verificación de claves o del estado de una conexión conductora irreversiblemente destructible. En caso de no estar permitida la escritura, no se realiza ninguna personalización y concluye la ejecución del diagrama de flujo.

En caso contrario, se continúa con la etapa (S8), en la que se escribe la imagen de memoria, con especificación de las direcciones de memoria físicas, en la memoria no volátil (5) de la tarjeta de chip (1). Esta escritura se realiza durante la rutina de preparación. Al realizar la escritura, las secuencias de datos de la imagen de memoria de la tarjeta de chip (1) se descodifican, una por una, con la clave de carga, y se escriben en la memoria no volátil (5) en la dirección de memoria física correspondiente prevista.

A la etapa (S8) sigue la etapa (S9), en la que se comprueba si la imagen de memoria se ha escrito sin errores en la memoria no volátil (5). Si se detecta un error, se interrumpe el proceso y termina el recorrido del diagrama de flujo.

Si el resultado de la comprobación en la etapa (S9) es positivo, se ejecutan en la tarjeta de chip (1) un “RESET” (“reposición”) y un “REBOOT” (“rearranque”). Seguidamente, en una etapa (S10) se inicia la rutina de reconversión inscrita en la memoria no volátil (5) junto con la imagen de memoria.

La rutina de reconversión es de importancia fundamental para el procedimiento según la invención. Durante la reconversión, todas las claves necesarias para el ulterior proceso de personalización, es decir, tanto las claves en posiciones conocidas como, por ejemplo, claves contenidas en, por ejemplo, objetos Java, se adaptan a la tarjeta de chip (1) a personalizar. La reconversión hace posible que la tarjeta de chip (1) se pueda utilizar para la ulterior personalización individualizadora con los datos de la imagen de memoria almacenados en la memoria no volátil (5). Para ejecutar la reconversión, es necesario que toda la imagen de memoria esté presente en la memoria no volátil (5) de forma no codificada. Durante la reconversión, el contenido de la memoria no volátil (5) de la tarjeta de chip (1) se procesa de modo individual para cada chip, es decir, que varias tarjetas de chip (1) en cuyas memorias no volátiles (5) se ha inscrito la misma imagen de memoria, después de la reconversión, se diferencian en lo que respecta a su ocupación de la memoria. Las funcionalidades y las informaciones sobre direcciones están almacenadas en la memoria permanente (4) y/o en la memoria no volátil (5). La propia ejecución de la reconversión se realiza mediante la rutina de reconversión inscrita en la memoria no volátil (5).

Ya durante la inicialización de la tarjeta de chip (1), o bien durante la reconversión, se generan y almacenan tablas de números aleatorios individuales para cada chip. Con estos números aleatorios individuales para cada chip se vuelven a codificar todos los elementos ocultados con los valores aleatorios de la primera tarjeta de chip, de la que, según el diagrama de flujo de la figura 2, se transfirieron los datos al dispositivo de personalización, es decir, por regla general, en especial, las claves necesarias para los cálculos criptográficos a realizar en las utilizaciones previstas de la tarjeta, de modo que dichos elementos quedan presentes en una forma secreta adaptada a la tarjeta de chip (1). Para la recodificación, los elementos ocultados se someten a una transformación utilizando los números aleatorios individuales para la tarjeta de chip (1), lo que hace que sean utilizables los elementos de los cálculos efectuados en la tarjeta de chip (1) basados en los números aleatorios válidos en la tarjeta de chip (1). Por ejemplo, un juego de claves (k’) secreto generado a partir de un juego de claves básico (k) mediante codificación con un conjunto de números aleatorios (Z1) de la tarjeta de chip (1), que contiene, como mínimo, un número aleatorio, se transforma en un juego de claves (k”), el cual se utiliza, en combinación con un conjunto de números aleatorios (Z2) de la tarjeta de chip (1) que igualmente contiene, como mínimo, un número aleatorio, para todos los cálculos criptográficos a realizar en la tarjeta de chip (1).

A continuación de la etapa (S10), se inicia la personalización que individualizará la tarjeta de chip. Para ello, en una etapa (S11) se comprueba si es admisible una ulterior ampliación de la imagen de memoria reconvertida almacenada en la memoria no volátil (5).

La admisibilidad requiere la ejecución con éxito de una verificación de claves, así como una autenticación recíproca entre la tarjeta de chip (1) y el dispositivo de personalización. Para la comprobación se utilizan las claves que fueron transferidas por el dispositivo de personalización a la memoria no volátil (5) durante la incorporación de los datos generales en la etapa (S2), luego retomadas en la imagen de memoria en la etapa (S5) posterior, seguidamente inscritas con la imagen de memoria en la memoria no volátil (5) de la tarjeta de chip (1) a fabricar, y vueltas a armonizar con los contenidos de las claves, en la etapa (S10), durante la reconversión individual para el chip de la imagen de memoria.

Después de la etapa (S11) se ejecuta una etapa (S12), en la que se personaliza individualmente la tarjeta de chip (1). En la memoria no volátil (5) de la tarjeta de chip (1) se inscriben ahora datos individuales tales como, por ejemplo, datos referidos a personas, sin especificación externa de una dirección de memoria. Por lo general, el volumen de estos datos individuales es mucho menor que el de los datos generales inscritos mediante la imagen de memoria. La escritura de los datos individuales se puede realizar sin volver a modificar la estructura lógica de la memoria no volátil (5), simplemente cambiando los contenidos concretos de algunas posiciones de almacenamiento. Esto se puede realizar, por ejemplo, de forma que los datos individuales sustituyan a marcadores de posición previstos en la imagen de memoria.

A la etapa (S12) sigue una etapa (S13), en la que se coloca en la tarjeta de chip (1) un indicativo de que la personalización ha concluido con éxito. Con esto concluye el recorrido del diagrama de flujo.

En la medida en que los requisitos de seguridad del proceso de personalización y la estructura de la personalización lo permitan, como variante del procedimiento antes descrito, se puede prever que también la ejecución de la etapa (S12) esté, en principio, totalmente almacenada en el dispositivo de personalización y que se ejecute allí antes de la inscripción, es decir, antes de la ejecución de las etapas (S7) y (S8). Con ello se puede reducir aún más el tiempo necesario para la personalización de una tarjeta de chip (1). La figura 4 muestra una posible secuencia de etapas para esta variante.

En este caso, en la personalización de la tarjeta de chip (1), en la etapa (S2), en la memoria no volátil (5) se escriben falsos datos individuales, los cuales sirven de marcadores de posición para los datos individuales específicos de la tarjeta, que se incorporarán en la etapa (S12). Adecuadamente, los falsos datos individuales son fácilmente reconocibles como tales y tienen, por ejemplo, la estructura “NÚMERO1”, que más adelante se ha de sustituir por el número individual, por ejemplo, “0123456”.

Los datos leídos durante la etapa (S5) y transmitidos al dispositivo de personalización, se descodifican allí a fin de determinar, en una etapa (S14), las posiciones de los campos ocupados con los falsos datos individuales.

Los campos de falsos datos individuales determinados se ocupan entonces en el dispositivo de personalización con los datos individuales específicos para la tarjeta de chip (1) a personalizar. Para ello, de forma similar a la etapa (S11), en el dispositivo de personalización se comprueba si está permitido ejecutar la etapa de personalización (S12). Seguidamente se escriben sobre el marcador de posición los datos individuales específicos de la tarjeta. Después de la comprobación de admisibilidad según la etapa (S7), el juego de datos resultante se transfiere a la tarjeta de chip (1) mediante una operación de escritura (S8). Para esta transferencia es adecuado volver a asegurar los datos mediante codificación con una correspondiente clave de carga que se encuentra en la tarjeta de chip (1).

Posteriormente, el juego de datos transferido a la tarjeta de chip (1), después de ser descodificado con la clave de carga, se somete a una reconversión según la etapa (S10). La reconversión se realiza del modo antes descrito.

Básicamente, ya no es necesaria una ulterior personalización especial según la etapa (S12). No bstante, debido a la clase de los datos individuales específicos de la tarjeta, puede suceder que una parte de los datos individuales básicamente no se preste a su incorporación con la ayuda de falsos datos individuales. Por ejemplo, esto es válido para datos basados en la vinculación de un número aleatorio específico de la tarjeta con datos individuales. Tales datos solamente se pueden insertar después de la reconversión. En este caso, después de la reconversión en la etapa (S10), se añade una etapa de personalización del tipo de la etapa (12), en la que incorporan a la tarjeta (1) los datos que no se pueden incluir en el dispositivo de personalización.

Como modificación de la variante antes descrita, se puede prever el uso de una técnica criptográfica que permita determinar los campos de falsos datos individuales en el dispositivo de personalización, sin una descodificación total de los datos transferidos. En este caso, se determinan del modo antes descrito los campos de falsos datos individuales, pero sin la descodificación previa de todos los datos, y dichos campos se ocupan con los datos individuales específicos para la tarjeta de chip (1) a personalizar. Seguidamente, los campos ocupados se codifican con la clave de carga. Posteriormente, el juego de datos codificado completo obtenido se escribe en la etapa (S8) sobre la tarjeta de chip (1), donde se descodifica y posteriormente se somete a una reconversión.

REIVINDICACIONES

1. Procedimiento para cargar con datos soportes de datos portátiles (1), en el que: en una memoria no volátil (5) de un primer soporte de datos portátil (1) se escriben datos generales idénticos para varios soportes de datos portátiles (1), sin especificación externa de direcciones de memoria físicas; se lee un contenido de memoria de, como mínimo, un sector parcial de la memoria no volátil (5) del primer soporte de datos portátil (1), y se genera para dicho sector parcial una imagen de memoria con inclusión de las correspondientes direcciones de memoria físicas; y se escribe la imagen de memoria, usando las correspondientes direcciones de memoria físicas, en las memorias no volátiles (5) de soportes de datos portátiles (1) adicionales; **caracterizado** porque después de la escritura de la imagen de memoria en la memoria no volátil (5) de cada uno de los soportes de datos portátiles (1) adicionales, este soporte de datos portátil (1) adicional ejecuta una rutina de reconversión para reconvertir la memoria no volátil (5) cargada con la imagen de memoria, durante la cual se recodifican todos los diversos elementos transmitidos con la imagen de memoria, en especial, las claves para los cálculos criptográficos de las aplicaciones previstas, de modo que dichos elementos quedan en una forma oculta adaptada a la tarjeta de chip (1); y porque, después de la reconversión, los correspondientes datos individuales específicos de cada soporte de datos portátil (1) se escriben en la memoria no volátil (5) del correspondiente soporte de datos portátil (1) sin especificación externa de una dirección de memoria física.

2. Procedimiento, según la reivindicación 1, **caracterizado** porque, durante la reconversión, una ocultación de una clave (k') basada en un número aleatorio (Z1) se transforma en una ocultación basada en un número aleatorio (Z2) individual para el soporte de datos (1).

3. Procedimiento, según la reivindicación 1, **caracterizado** porque, como datos generales, en la memoria no volátil (5) del primer soporte de datos portátil (1) se escribe software, en especial, paquetes JAVA y applets JAVA.

4. Procedimiento, según una de las reivindicaciones anteriores, **caracterizado** porque durante la inicialización del primer soporte de datos portátil (1) se escribe una rutina de lectura destinada a leer la memoria no volátil (5) o los datos adicionales imprescindibles para la ejecución de la rutina de lectura, en la memoria no volátil (5) del primer soporte de datos portátil (1).

5. Procedimiento, según una de las reivindicaciones anteriores, **caracterizado** porque, durante la inicialización del primer soporte de datos portátil (1), se escribe la rutina de reconversión en la memoria no volátil (5) del primer soporte de datos portátil (1).

6. Procedimiento, según una de las reivindicaciones anteriores, **caracterizado** porque el contenido de la memoria no volátil (5) del primer soporte de datos portátil (1) solamente se lee en caso de que previamente se haya ejecutado con éxito una comprobación de seguridad.

7. Procedimiento, según una de las reivindicaciones anteriores, **caracterizado** porque se codifica el contenido de memoria leído de la memoria no volátil (5) del primer soporte de datos portátil (1).

8. Procedimiento, según una de las reivindicaciones anteriores, **caracterizado** porque sólo se permite realizar una vez la generación de la imagen de la memoria no volátil (5) del primer soporte de datos portátil (1).

9. Procedimiento, según una de las reivindicaciones anteriores, **caracterizado** porque la rutina de lectura para leer la memoria no volátil (5) del primer soporte de datos portátil (1), o los datos adicionales imprescindibles para la ejecución de la rutina de lectura, se borran después de la generación de la imagen de memoria.

10. Procedimiento, según una de las reivindicaciones anteriores, **caracterizado** porque la imagen de memoria se descodifica antes de la escritura en la memoria no volátil (5) de cada uno de los soportes de datos portátiles (1) adicionales.

11. Procedimiento, según una de las reivindicaciones anteriores, **caracterizado** porque la reconversión de la memoria no volátil (5) de los soportes de datos portátiles (1) adicionales se realiza de forma específica para cada soporte de datos.

12. Procedimiento, según una de las reivindicaciones anteriores, **caracterizado** porque durante la reconversión de la memoria no volátil (5) de los soportes de datos portátiles (1) adicionales se generan números aleatorios y se codifican los datos almacenados.

13. Procedimiento para cargar con datos soportes de datos portátiles (1), en el que: en una memoria no volátil (5) de un primer soporte de datos portátil (1) se escriben datos generales idénticos para varios soportes de datos portátiles (1) sin especificación externa de direcciones de memoria físicas; se lee un contenido de memoria, como mínimo, de un sector parcial de la memoria no volátil (5) del primer soporte de datos portátil (1), y se genera para dicho sector parcial una imagen de memoria con inclusión de las correspondientes direcciones de memoria físicas; **caracterizado** porque, además de los datos generales, se escriben en la memoria (5) falsos datos individuales, que se determinan después de la lectura en la imagen de memoria y se sobrescriben con datos individuales específicos para un soporte de

datos portátil (1) a personalizar, y la imagen de memoria personalizada obtenida se escribe en la memoria no volátil (5) de un soporte de datos portátil (1) a personalizar, y después de cada escritura en la memoria no volátil del soporte de datos portátil (1) se ejecuta una rutina de reconversión para reconvertir la memoria no volátil (5) cargada con la imagen de memoria, durante la cual se recodifican todos los diversos elementos ocultos transferidos con la imagen de memoria, en especial, las claves para el cálculo criptográfico de las aplicaciones previstas, de modo que los elementos están presentes en una forma oculta adaptada al soporte de datos portátil (1); y porque, después de la reconversión, los correspondientes datos individuales específicos de cada soporte de datos portátil (1) se escriben en la memoria no volátil (5) del correspondiente soporte de datos portátil (1) sin especificación externa de una dirección de memoria física.

14. Procedimiento, según una de las reivindicaciones anteriores, **caracterizado** porque se cargan con datos soportes de datos portátiles (1) conformados como tarjetas de chip.

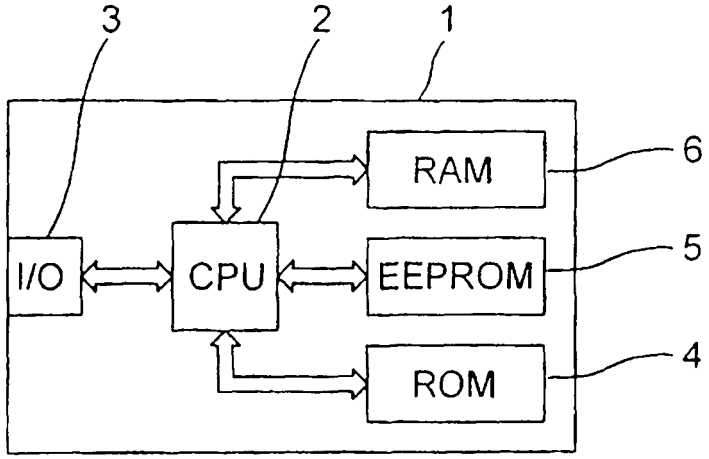
3
2
1
RAM
6
I/O
CPU
EEPROM
5
ROM
4

Fig. 1

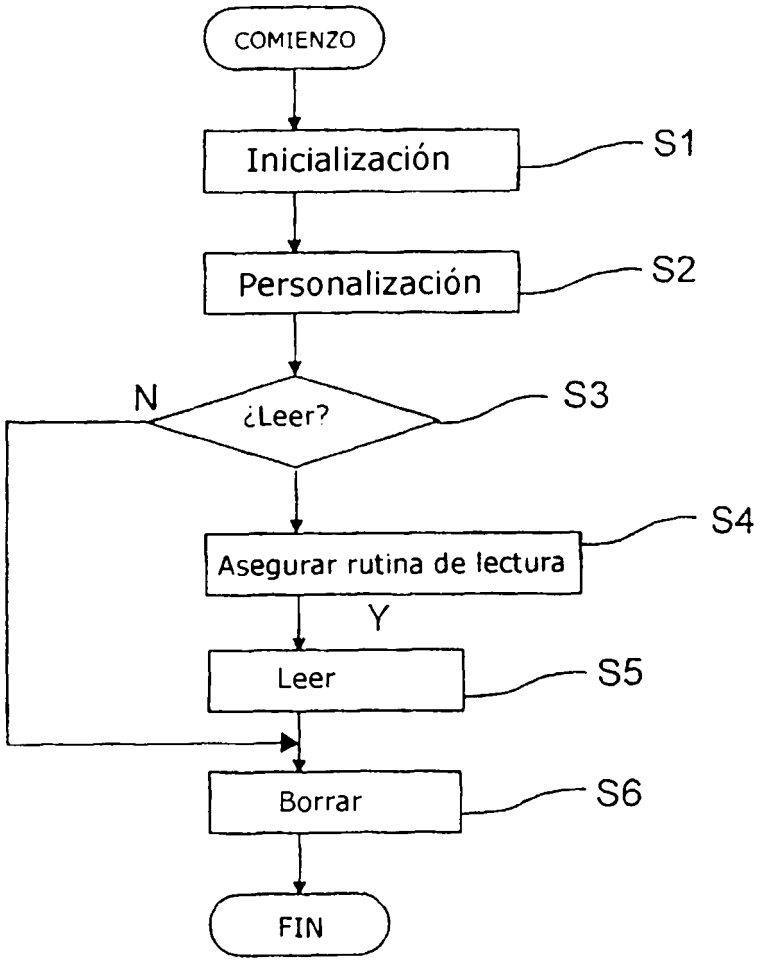
COMIENZO
Inicialización
S1
Personalización
S2
N
¿Leer?
S3
Asegurar rutina de lectura
S4
Y
Leer
S5
Borrar
S6
FIN

Fig. 2

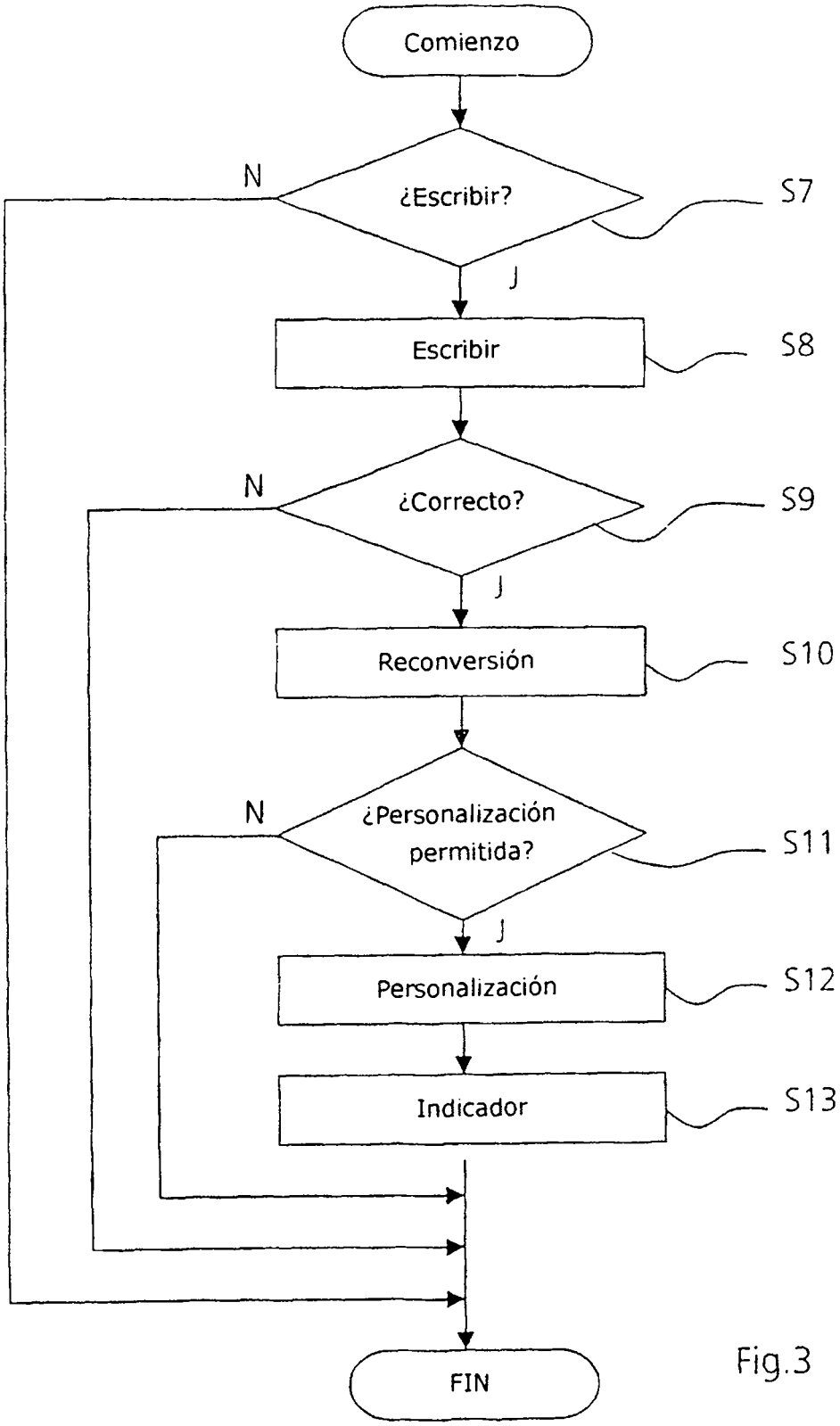
Comienzo
¿Escribir?
N
S7
J
Escribir
S8
¿Correcto?
N
S9
J
Reconversión
S10
¿Personalización permitida?
N
S11
J
Personalización
S12
Indicador
S13
FIN

Fig.3

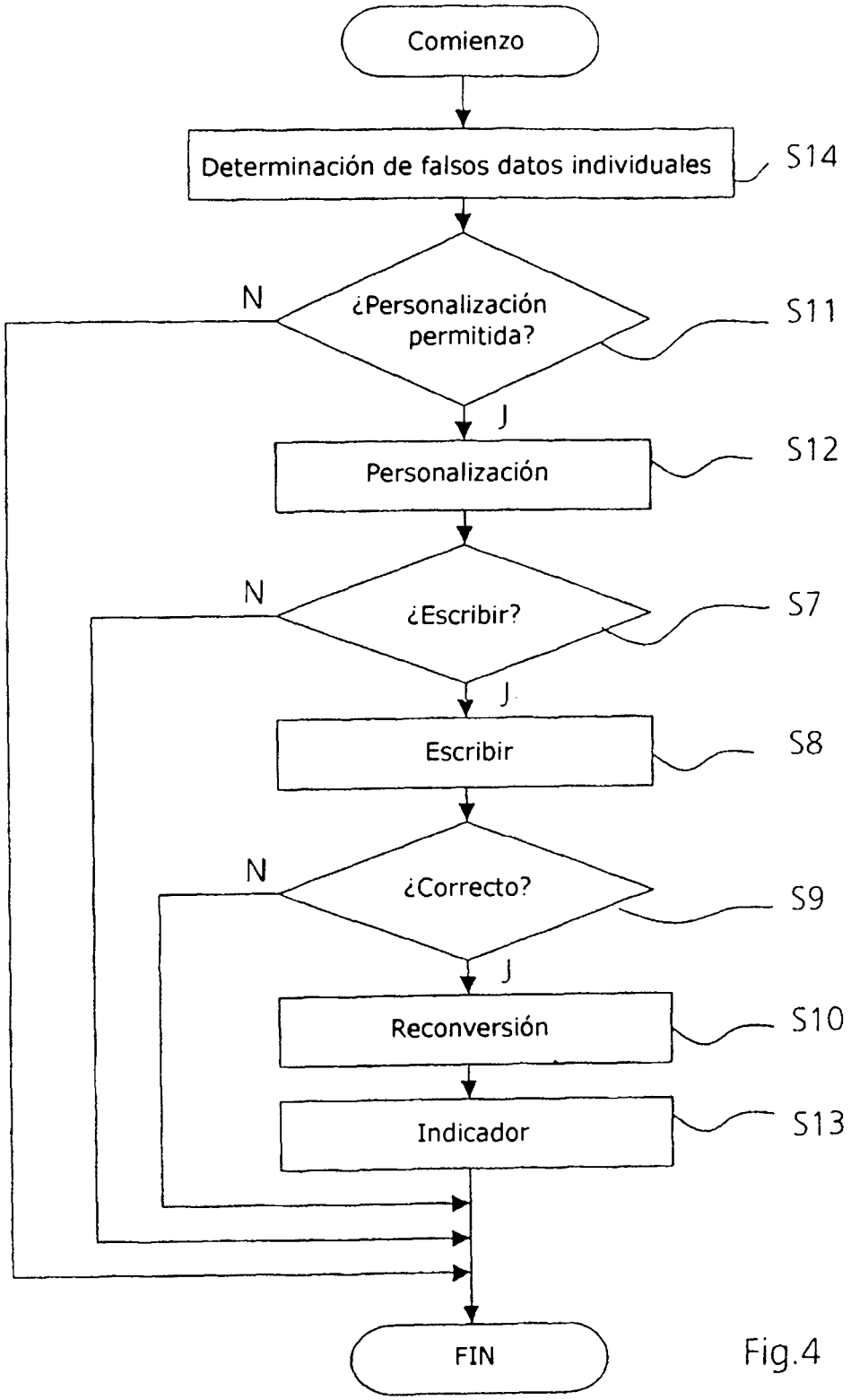
Comienzo
Determinación de falsos datos individuales
S14
¿Personalización permitida?
S11
N
J
Personalización
S12
¿Escribir?
S7
N
J
Escribir
S8
¿Correcto?
S9
N
J
Reconversión
S10
Indicador
S13
FIN

Fig.4