(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 442 495**

(51) Int. CI.:

G06K 17/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **30.10.2007 E 07866468 (7)**

(97) Fecha y número de publicación de la concesión europea: **23.10.2013 EP 2082359**

(54) Título: **Procedimiento y dispositivo de personalización de una entidad electrónica portátil**

(30) Prioridad:

07.11.2006 FR 0654767

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.02.2014

(73) Titular/es:

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

(72) Inventor/es:

MOUNIER, RÉGIS y
LOUIS, JEAN-MARC

(74) Agente/Representante:

LINAGE GONZÁLEZ, Rafael

DESCRIPCIÓN

Procedimiento y dispositivo de personalización de una entidad electrónica portátil

La invención se refiere a un procedimiento y a un dispositivo de personalización de una entidad electrónica portátil. Se aplica, en particular, a la personalización de tarjetas de microcircuito en función de perfiles de usuarios.

La invención se refiere a entidades electrónicas portátiles que comprenden, particularmente, tarjetas de microcircuito, las tarjetas de memoria tal como una tarjeta de memoria de almacenamiento de datos numéricos, por ejemplo una tarjeta *secure digital* o una tarjeta SD (marca registrada), una llave USB (acrónimo de *universal serial bus* para bus universal en serie), una tarjeta MultiMediaCard, llamada también MMC (marcas registradas), una tarjeta Smartmedia (marca registrada), una mini-tarjeta multimedia o una PDA (acrónimo de *Personal Digital Assistant* para asistente numérico personal), también llamado organizador. La tarjeta de microcircuito está, por ejemplo, conforme a la norma ISO 7816. Puede, por ejemplo, tratarse de una tarjeta con microcontrolador asegurado.

La utilización de una entidad electrónica en un marco aplicativo determinado implica la memorización, en la entidad electrónica, de datos y/o de programas susceptibles de ser utilizados en este marco. Por eso tienen frecuentemente recursos, en particular para las entidades electrónicas portátiles en una etapa de personalización en el transcurso de la cual se inscribe en una memoria de la entidad electrónica los datos que le son específicos, tales como por ejemplo la identidad del portador de la tarjeta.

La personalización es realizada por una estación de personalización que efectúa un tratamiento de los datos de personalización. Se observa que esta personalización no se limita a la personalización “eléctrica” de la memoria sino que puede, por el contrario, extenderse a la personalización gráfica o física de la entidad electrónica portátil, por ejemplo por técnicas de impresión o de gofrado.

La entidad electrónica portátil comprende una memoria no volátil regrabable, por ejemplo, una memoria EEPROM (acrónimo de *Electrically Erasable and Programmable Read Only Memory* para memoria solo de lectura programable y borrable eléctricamente). La personalización eléctrica consiste esencialmente en una etapa de inicialización de esta memoria no volátil y así de la entidad electrónica portátil. Esta memoria está adaptada particularmente a la memorización de este tipo de datos que varían de una entidad electrónica a otra.

Hay que señalar que antes de esta inicialización, la entidad electrónica portátil no puede funcionar. Puede solamente ser personalizada. Igualmente, antes de la etapa de personalización, la memoria no volátil puede ser virgen o casi virgen, es decir, que no es inicializada.

La etapa de inicialización de la memoria no volátil es una etapa durante la que se memorizan, en la memoria no volátil, informaciones específicas de las funciones aplicativas de la entidad electrónica portátil y/o específicas de cada portador de la entidad electrónica portátil. Los datos de personalización son generalmente memorizados en una memoria no volátil regrabable.

La estructura global de los datos de personalización a inscribir en esta memoria es, en cambio, común a un conjunto de tarjetas del mismo tipo y participa así en la definición de un perfil de personalización asociado a este tipo de tarjeta.

Un perfil de personalización es así un conjunto de datos asociados a un tipo de tarjeta y que definen las características generales de la personalización de las tarjetas de este tipo, tales como la estructura de los datos, comprendidos, eventualmente, de programa, y los datos comunes a inscribir en la entidad electrónica durante la personalización, o incluso datos de personalización física, por ejemplo caracteres a gofrar o codificación de la banda magnética, o gráfica, por ejemplo logo a imprimir en la superficie de la tarjeta.

La definición de un perfil de personalización es particularmente compleja ya que debe respetar, de manera coherente, un conjunto de criterios unidos a la estructura y a la utilización futura de la entidad electrónica, a saber, por ejemplo, las normas, por ejemplo GSM (acrónimo de *Global System for Mobile* para sistema global para móviles) en telefonía móvil o EMV (acrónimo de *Europay, Mastercard y Visa*, marcas registradas), en el campo bancario, y las aplicaciones, por ejemplo Visa o Mastercard (marcas registradas) existentes, y la organización interna material de la entidad electrónica.

Tal definición es por lo tanto, clásicamente, bastante pesada para su implementación y no se puede eliminar un riesgo de error cuando la definición del perfil es practicada por personales experimentados.

En una tarjeta con microcircuito conforme a la norma ISO 7816, el microcircuito es generalmente un microcontrolador asegurado que contiene en su memoria ROM un sistema de explotación y/o de aplicaciones. La imagen de esta memoria solo de lectura, que se llama “máscara”, es definida generalmente por el fabricante de tarjeta durante una etapa de concepción, y puede evolucionar con el transcurso del tiempo, particularmente con

motivo de evolución o de corrección de error de software.

Durante la fabricación de las tarjetas de microcircuito, los microcontroladores son entregados por el fabricante de semiconductor con una máscara dada. El sistema de explotación de cada máscara comprende una codificación específica de los comandos.

En el procedimiento descrito en la patente US 5889941, esta codificación es memorizada en el transcurso de la etapa de personalización en un fichero de sistema de explotación.

En cuanto a las tarjetas inteligentes, son generalmente fabricadas y personalizadas por lotes de tarjetas de un mismo tipo (por ejemplo en el campo bancario, mismo banco, mismo tipo de tarjeta, etc.). En cada lote, hay un solo tipo de máscara.

Es así que, en el procedimiento descrito en la patente US 5889941, citado más arriba, no se utiliza más que un solo fichero de sistema de explotación por lote, del que cada microcontrolador de las tarjetas de un mismo lote tiene la misma máscara. Es igualmente el procedimiento descrito en la patente US 6196459, en el que se trabaja por lote.

Se comprende muy bien que sea particularmente interesante estar en condiciones de personalizar tarjetas cuyas máscaras son diferentes en el seno de un mismo lote, por ejemplo para simplificar la gestión de stock de microcontroladores.

Se conoce, en la técnica anterior, una solución que permite realizar una personalización de cada tarjeta con datos relativos a una persona, descrita en la patente EP 0706150. No obstante, esta solución tiene el inconveniente de necesitar una escritura de un identificador en la memoria regrabable de la tarjeta, lo que aumenta los costes, ya que hace falta, para ello, utilizar una máquina de personalización.

La solicitud de patente europea EP 1434168 describe un procedimiento de fabricación de tarjetas personalizadas. Durante la fase de personalización una marca precedentemente aplicada, propia de un operador al que está destinada la tarjeta, es leída con el fin de determinar el operador por el sesgo de una base de datos antes de registrar datos de personalización.

En el procedimiento descrito en la patente US 6196459, un identificador del objeto tarjeta es transmitido por un controlador a la estación de personalización, y después la estación de personalización transmite el identificador al servidor.

En la patente US 6575360, un sistema de personalización comprende un sistema de control de tarjeta inteligente y un sistema de administración de una tarjeta inteligente. El sistema de control de tarjeta inteligente asegura la interfaz con la tarjeta inteligente y transmite de forma transparente, es decir, sin otro tratamiento que el decodificado o codificado, por una parte, de los comandos elaborados por el sistema de administración con destino a la tarjeta inteligente y, por otra parte, de las respuestas a estos comandos elaboradas por la tarjeta inteligente con destino al sistema de administración.

Según esta patente, la ATR (acrónimo de *Answer to Reset* para respuesta a la puesta en tensión) puede formar parte de la petición de ejecución de aplicación y se refiere al protocolo de comunicación con el que se puede comunicar con la tarjeta (tipo de protocolo, frecuencia, etc.). Además, en esta patente, no está previsto tratar lotes de tarjetas a priori diferentes.

El sistema descrito en esta patente presenta igualmente el inconveniente de necesitar intercambios importantes entre el sistema de control de la tarjeta inteligente y el sistema de administración de la tarjeta inteligente. Además, el sistema de control está en espera, es decir, no efectúa ningún tratamiento, entre el momento en el que suministra una respuesta elaborada por la tarjeta al sistema de administración y el momento en el que recibe un nuevo comando de parte del sistema de administración. En consecuencia, en un sistema en el que se han debido tratar millares o decenas de millares de tarjetas por hora, estos intercambios pueden limitar la cadencia de personalización de las tarjeras, particularmente cuando un solo sistema de administración es utilizado para la comunicación con varias estaciones de personalización.

La presente invención pretende remediar estos inconvenientes y, en particular, permitir la personalización de tarjetas diferentes con el mismo sistema de personalización, es decir, servidor y estación de personalización.

A este efecto, la presente invención pretende, según un primer aspecto, un dispositivo de personalización de una entidad electrónica portátil, según la reivindicación 1.

Gracias a estas disposiciones, el dispositivo de personalización puede efectuar simplemente la personalización de lotes de entidades electrónicas que comprenden plataformas diferentes en términos de circuitos y/o de sistemas de explotación. Dado que el identificador primero proviene de la memoria no regrabable (ROM) de la entidad electrónica portátil, este identificador primero está disponible desde antes de la que etapa de personalización y puede identificar

características técnicas, materiales y/o de programas de la entidad electrónica portátil.

Se observa que el dispositivo de personalización tal como el sucintamente expuesto anteriormente puede ser incorporado en un servidor de personalización o en una estación de personalización.

Según unas características particulares, los medios de memorización de una pluralidad de grupos de datos de personalización están adaptados a que cada grupo de datos de personalización sea asociado a un identificador segundo, porque comprende unos medios de asociación de un identificador segundo a dicho identificador primero, y porque los medios de selección están adaptados para seleccionar al menos un grupo de datos de personalización en función del identificador segundo correspondiente al identificador primero.

Gracias a estas disposiciones, la puesta en relación de los datos de personalización con los identificadores primeros es más ágil ya que el mismo grupo de datos de personalización puede ser asociado a varios identificadores primeros, sin que todos los grupos de datos de personalización asociados a estos identificadores primeros sean comunes. Además, los grupos de datos de personalización pueden ser generados independientemente de los identificadores primeros, y puestos, después, en relación con ciertos identificadores primeros.

Según unas características particulares, los medios de comunicación están adaptados a que dicha entidad electrónica sea conforme al menos en parte a la norma ISO 7816 y a que dicho mensaje sea una ATR (acrónimo de *Answer to Reset* para respuesta a la puesta en tensión).

Gracias a cada uno de estos dispositivos, desde la puesta en tensión de la entidad electrónica portátil, el dispositivo de personalización tal como el sucintamente expuesto anteriormente dispone del identificador primero. El proceso de personalización no necesita por lo tanto interrogar a la entidad electrónica portátil y puede por lo tanto ser a la vez más rápido, menos oneroso y más fiable.

Según unas características particulares, los medios de comunicación están adaptados para efectuar una puesta a cero de la entidad electrónica portátil y para efectuar una puesta a cero de la entidad electrónica portátil y para recibir el identificador primero en al menos una parte de un mensaje suministrado por la entidad electrónica portátil durante su puesta a cero.

Según unas características particulares, los medios de comunicación están adaptados para recibir un identificador primero que comprende al menos un octeto llamado “históricos” según la norma ISO 7816 (octetos T1, T2,…, T9) de la ATR.

Gracias a cada uno de estos dispositivos, la implementación de la presente invención es particularmente fácil y fiable ya que el mensaje suministrado por la entidad electrónica portátil durante su puesta en tensión es siempre idéntico y no depende de una instrucción específica emitida por la estación de personalización. La invención es por lo tanto particularmente práctica para su implementación concretamente en una tarjeta de microcircuito.

Según unas características particulares, los medios de memorización están adaptados a que dichos grupos de datos de personalización comprenden al menos una imagen de la estructura de la memoria no volátil de la entidad electrónica portátil. Se pueden así preparar los datos de personalización, para que, cuando el dispositivo obtiene el identificador primero, por ejemplo la ATR, haya menos tratamiento a realizar para obtener los datos de personalización.

Según unas características particulares, dicha imagen de estructura es, adicionalmente, representativa del contenido y del tamaño de fichero de la entidad electrónica portátil.

Según unas características particulares, dicha imagen de estructura es representativa de las zonas de memorias de la entidad electrónica portátil que contienen variables, así como su valor, fuera de los datos específicos al futuro portador de la entidad electrónica portátil.

Según unas características particulares, los medios de personalización están adaptados para completar los campos vírgenes de dicha imagen de estructura con datos de personalización.

Según unas características particulares, la entidad electrónica es una tarjeta de microprocesador asegurada conforme al menos en parte a la norma ISO 7816.

Según unas características particulares, los medios de personalización están adaptados para formar al menos una instrucción de personalización a partir de dicho grupo de datos de personalización seleccionado.

Según unas características particulares, al menos una instrucción de personalización es una instrucción directamente comprensible y ejecutable por la entidad electrónica portátil.

Gracias a estas disposiciones, la estación de personalización no tiene que interpretar las instrucciones de

personalización directamente comprensibles y ejecutables por la entidad electrónica portátil y no hace más que transmitírselas.

Según características particulares, los medios de personalización están adaptados a que al menos una instrucción de personalización permite la inscripción, por la entidad electrónica portátil, de datos en la memoria de la entidad electrónica portátil.

Según características particulares, los medios de personalización están adaptados a que al menos una instrucción de personalización sea específica al portador para venir de la entidad electrónica portátil.

Según unas características particulares, el dispositivo tal como el sucintamente expuesto anteriormente comprende:

- unos medios de tratamiento adaptados para tratar dichos datos de personalización y para generar al menos un grupo de instrucciones de personalización de la entidad electrónica portátil, al menos un grupo de instrucciones de personalización que comprende al menos una instrucción de control de personalización que permite a una estación de personalización controlar la buena ejecución de al menos una instrucción de personalización, y

- unos medios de emisión de cada grupo de instrucciones de personalización.

Estas disposiciones particulares se refieren particularmente a un dispositivo constituido por un servidor de personalización. Gracias a cada una de estas disposiciones, con el fin de mejorar las cadencias de personalización:

- se hace efectuar lo esencial de los tratamientos en un servidor de personalización, que limita así los tratamientos realizados por las estaciones de personalización,

- se limitan los intercambios de datos entre las estaciones de personalización y el servidor de personalización.

Estos objetivos se logran particularmente gracias a la elaboración de grupos de instrucciones de personalización por el servidor de personalización. Así, la estación de personalización no tiene que elaborar las instrucciones de personalización y no tiene que requerir una a una las instrucciones de personalización.

En definitiva, el servidor de personalización tiene así igualmente un rol de definición de los controles de la personalización que son ejecutados por la estación de personalización. El aumento de carga, por la estación de personalización, de estas instrucciones de control definidas por el dispositivo de personalización permite limitar los intercambios entre las estaciones de personalización y el servidor, limitando al máximo los tratamientos efectuados por las estaciones de personalización.

Según unas características particulares, los medios de tratamiento son, adicionalmente, adaptados para generar al menos una instrucción de notificación de personalización que permite a la estación de personalización confirmar al dispositivo la buena ejecución de al menos una parte de un grupo de instrucciones de personalización, y para insertar al menos una instrucción de notificación en al menos un grupo de instrucciones de personalización, estando adaptados los medios de emisión para emitir al menos una instrucción de notificación con destino a la estación de personalización, comprendiendo el dispositivo, además, unos medios de recepción de al menos una notificación que proviene de la estación de personalización. Así, el dispositivo puede verificar la buena realización de la personalización.

Los intercambios de instrucciones entre el dispositivo de personalización y la estación de personalización son así limitados a grupos de instrucciones de personalización que comprenden, a la vez, instrucciones para hacer ejecutar a la entidad electrónica portátil e instrucciones de notificación.

Según unas características particulares, el dispositivo tal como el sucintamente expuesto anteriormente comprende, adicionalmente, unos medios de análisis capaces de analizar al menos una notificación recibida y de activar una acción en función del resultado de dicho análisis. Así, es el servidor el que asegura el control de personalización y por lo tanto se descargan las estaciones al máximo de tareas de tratamiento.

Según unas características particulares, los medios de tratamiento comprenden unos medios de definición de grupos de instrucciones tales que el dispositivo necesita la notificación de ejecución de al menos una de las instrucciones precedentes para generar la primera instrucción del próximo grupo de instrucciones de personalización. Gracias a estas disposiciones, el tamaño de los grupos de instrucciones es máximo y las interacciones entre el dispositivo y la estación de personalización son reducidas, lo que aumenta la cadencia de personalización.

Según unas características particulares, los medios de comunicación están adaptados para recibir, adicionalmente, al menos un identificador de dicha estación de personalización. Gracias a cada una de estas disposiciones, el servidor puede generar los grupos de instrucciones de personalización en función de un identificador de la estación de personalización. Lo que limita los riesgos de error.

Según unas características particulares, los medios de tratamiento están adaptados para generar al menos un grupo de instrucciones de personalización en paralelo con la ejecución de un grupo de instrucciones de personalización por la estación de personalización. Gracias a estas disposiciones, la cadencia de personalización puede ser aumentada ya que desde que un grupo de instrucciones de personalización ha sido ejecutado por la estación de personalización, otro grupo de instrucciones de personalización puede serle enviado por el dispositivo, sin tener que esperar que este nuevo grupo de instrucciones de personalización sea preparado.

Según unas características particulares, el dispositivo tal como sucintamente expuesto anteriormente comprende:

- unos medios de recepción de al menos un grupo de instrucciones de personalización de la entidad electrónica portátil, al menos un grupo de instrucciones que comprenden al menos una instrucción de control de personalización que permite controlar la buena ejecución de al menos una instrucción de personalización,

- unos medios de transmisión de al menos una instrucción de personalización a la entidad electrónica portátil, y

- unos medios de tratamiento adaptados para tratar cada instrucción de control para controlar la buena ejecución de al menos una instrucción de personalización por la entidad electrónica portátil.

Estas disposiciones se aplican más particularmente a las estaciones de personalización. Gracias a estas disposiciones, con el fin de mejorar las cadencias de personalización:

- se hace efectuar lo esencial de los tratamientos en un servidor de personalización, que limita así los tratamientos realizados por las estaciones de personalización,

- se limitan los intercambios de datos entre las estaciones de personalización y el servidor de personalización.

Estos objetivos se logran particularmente gracias a la elaboración de grupos de instrucciones de personalización por el servidor de personalización. Así, la estación de personalización no tiene que elaborar las instrucciones de personalización y no tiene que requerir una a una las instrucciones de personalización.

En definitiva, el servidor de personalización tiene así igualmente un rol de definición de los controles de la personalización que son ejecutados por la estación de personalización. El aumento de carga, por la estación de personalización, de estas instrucciones de control definidas por el dispositivo de personalización permite limitar los intercambios entre las estaciones de personalización y el servidor, limitando al máximo los tratamientos efectuados por las estaciones de personalización.

Según unas características particulares, los medios de tratamiento están adaptados para realizar al menos una instrucción de control de al menos una instrucción de personalización después de que los medios de transmisión sean transmitidos, a la entidad electrónica portátil, otra instrucción de personalización no referida por dicha instrucción de control. Así, esperando la respuesta de la entidad electrónica a una instrucción de personalización, la estación de personalización puede analizar la respuesta de la instrucción de personalización precedente e insertar las informaciones necesarias en dicha notificación.

Según unas características particulares, los medios de recepción son, adicionalmente, adaptados para recibir al menos una instrucción de notificación de personalización y los medios de tratamiento son, adicionalmente, adaptados para preparar una notificación de ejecución de al menos un grupo de instrucciones de personalización, comprendiendo el dispositivo, adicionalmente, unos medios de emisión de notificación con destino a un servidor de personalización.

Según unas características particulares, los medios de recepción están adaptados para extraer al menos una instrucción de notificación de al menos un grupo de instrucciones de personalización.

Según un segundo aspecto, la presente invención pretende un procedimiento de personalización de una entidad electrónica portátil según la reivindicación 17.

Las ventajas, objetivos y características del procedimiento objeto del según aspecto de la presente invención que son similares a las del dispositivo objeto del primer aspecto de la presente invención no son recordadas aquí.

Otros objetos, características y ventajas de la invención aparecerán a la luz de la descripción que sigue, hecha, con un fin explicativo y nulamente limitativo, en referencia a los dibujos adjuntos, en los que:

- la figura 1 representa, esquemáticamente, una entidad electrónica portátil en cuya personalización se aplica la presente invención,

- la figura 2 representa, esquemáticamente, un modo de realización particular de un sistema, de un servidor, y de una estación de personalización objetos de la presente invención,

- la figura 3 representa, en forma de diagrama de flujo, unas etapas implementadas en un modo de realización particular del procedimiento de personalización objeto de la presente invención,

- la figura 4 representa, en forma de un diagrama de flujo, unas etapas implementadas en un modo de realización particular del procedimiento objeto de la presente invención,

- las figuras 5A a 5I representan, esquemáticamente, tramos de datos intercambiados entre diferentes entidades para la implementación de un modo de realización particular del procedimiento objeto de la presente invención,

- la figura 6 representa, en forma de un diagrama de flujo, unas etapas implementadas en una de las etapas ilustradas en la figura 3, y

- las figuras 7A a 7I representan, esquemáticamente, unos tramos de datos intercambiados entre diferentes entidades para la implementación de un modo de realización particular del procedimiento objeto de la presente invención.

La invención se refiere a la personalización de una entidad electrónica portátil. Se recuerda que en el transcurso de tal personalización, se graban en una memoria de la entidad electrónica los datos que son específicos a esta entidad, a unas funciones aplicativas de la entidad, por ejemplo, tipos de servicios autorizados, funciones de seguridad y criptográficas a veces llamadas datos de inicialización, y/o específicas del portador que viene de la entidad electrónica portátil, por ejemplo, el nombre, el número de cuenta o de teléfono, la fecha límite de validez y/o una fotografía. La personalización cubre, en particular, la realización de *softmasks* o máscaras de programa en el caso de una tarjeta de microcircuito.

Se observa que, en ciertos documentos de la técnica anterior, se distingue la noción de inicialización de la personalización. En el sentido de la presente invención, estas dos nociones son reagrupadas en el mismo término de “personalización”, aunque estas etapas pueden ser distintas, y realizadas, por ejemplo, por estaciones de personalización diferentes, por ejemplo por razones de seguridad.

Un ejemplo de entidad electrónica portátil 100 es representada en la figura 1. Esta entidad electrónica portátil 100 puede ser una tarjeta de microcircuito conforme a la norma ISO 7816, un documento de identificación, una llave USB, una PDA, o una tarjeta de microcircuito por ejemplo conforme a la especificación MMC (MultiMediaCard) que comprende una memoria por ejemplo de tipo flash. Puede también tratarse de una tarjeta inteligente sin contacto o de una tarjeta llamada dual, es decir, que comprende una interfaz sin contacto y una interfaz con contacto, por ejemplo conforme a la norma ISO 14443. La entidad electrónica portátil 100 puede igualmente ser un pasaporte que comprende en el espesor de la cubierta un microcontrolador asegurado dotado de medios de comunicación sin contacto conforme a la norma ISO 14443.

En el caso de una tarjeta de microcircuito conforme a la norma ISO 7816, y desde un punto de vista aplicativo, la entidad electrónica portátil 100 es particularmente una tarjeta de identificación asegurada o un documento de identificación asegurado, es decir, por ejemplo, una tarjeta bancaria, una tarjeta de identificación de un subscriptor de una red de telefonía móvil, o una tarjeta o un documento oficial o de transporte (tarjeta de transporte, tarjeta de identidad, tarjeta de identificación de vehículo automóvil de tipo tarjeta gris, etc.).

En el modo de realización ilustrado en la figura 1, la entidad electrónica portátil 100 es una tarjeta de microcircuito de dimensión preferentemente conforme a la norma ISO 7816, particularmente de 1,76 mm de espesor. Comprende una interfaz de entradas-salidas, de alimentación y de suministro de señal de temporizador 110, un microcontrolador asegurado 120, una memoria solo de lectura ROM 130 y una memoria regrabable EEPROM 140.

La interfaz 110 puede comprender una interfaz de comunicación con o sin contracto o una interfaz llamada dual, es decir, que comprende una interfaz de contacto.

La memoria solo de lectura 130 conserva un sistema de explotación que permite a la entidad electrónica portátil 100 funcionar, es decir, recibir y ejecutar instrucciones o comandos conforme a la norma ISO 7816, y asegurar la entidad electrónica portátil 100.

La personalización de la entidad electrónica portátil consiste, particularmente, en inicializar la memoria 140 creando ficheros y/o variables, por ejemplo en forma de una estructura conocida bajo el nombre de TLV (acrónimo de *tag length value* para tipo-longitud-valor).

Según un modo de funcionamiento, la entidad electrónica portátil 100 es de tipo esclavo, en el sentido de que la entidad electrónica no hace más que responder a comandos del terminal jefe. En una implementación de la invención en el seno de una tarjeta de microcircuito, el terminal jefe es, particularmente, un lector de tarjeta. En este caso, la entidad electrónica portátil, de microcircuito, es preferentemente conforme a la norma ISO 7816. Se trata generalmente, en este caso, de una tarjeta de microcircuito asegurada.

Se observa, en la figura 2, un sistema de personalización que comprende un servidor 200 de personalización y una estación 240 de personalización que comunica una entidad electrónica portátil 100.

El servidor 200 de personalización comprende una entrada 205 de datos de personalización, una memoria no volátil 210, por ejemplo un disco duro, que conserva un programa 220 y una unidad central CPU 230. El programa 220 es un programa de tratamiento y de control que genera grupos de instrucciones a partir de datos de personalización y, eventualmente, un identificador de la entidad electrónica portátil 100.

La unidad central CPU 230 y el programa 220 constituyen, conjuntamente, unos medios de tratamiento adaptados para tratar datos de personalización e identificadores de entidades electrónicas portátiles y para generar al menos un grupo de instrucciones de personalización de la entidad electrónica portátil. Preferentemente, un grupo de instrucciones de personalización comprende más de una instrucción de personalización.

Las instrucciones generadas por estos medios de tratamiento comprenden, preferentemente, instrucciones de personalización, instrucciones de control e instrucciones de notificación. Las instrucciones de personalización son comprensibles y ejecutables por la entidad electrónica portátil 100. Conforme a la presente invención, estas instrucciones de personalización son agrupadas, por el servidor 200 de personalización, en grupos de instrucciones de personalización, al menos un grupo de instrucciones que comprende una pluralidad de instrucciones de personalización y, de manera explícita o implícita, al menos una instrucción de control y, eventualmente, al menos una instrucción de notificación.

Las instrucciones de control pueden ser no importa qué instrucción a la consideración de la estación 240 de personalización que le permite controlar la ejecución de las instrucciones de personalización por la entidad electrónica portátil 100. Preferentemente, las instrucciones de control permiten a la estación 240 de personalización verificar la ejecución de cada instrucción de personalización por la entidad electrónica portátil 100. Así, estas instrucciones de control pueden definir una duración máxima durante la que la estación de personalización 240 puede esperar, de parte de la entidad electrónica portátil 100, una respuesta a una instrucción de personalización. En este modo de realización, dicha instrucción de control es ventajosamente la respuesta en el formato APDU esperada a una instrucción de personalización en forma de comando en el formato APDU.

Las instrucciones de notificación determinan en qué casos y cómo la estación 240 de personalización debe comunicar con el servidor 200 de personalización para indicarle la buena ejecución de al menos una parte de un grupo de instrucciones de personalización de una entidad electrónica portátil 100. Preferentemente, la instrucción de notificación es materializada implícitamente por el final de grupo de instrucción, es decir, que cada vez que la estación 240 de personalización logra el fin de un grupo de instrucción, esta emite, con destino al servidor 200 de personalización, una notificación que representa la ejecución, con éxito, de cada instrucción de control. Este tipo particular de instrucción de notificación es particularmente simple de implementar. En otras variantes, el servidor 200 de personalización inserta instrucciones de notificación explícita en el grupo de instrucciones de personalización.

Preferentemente, los medios de tratamiento y de control, es decir, la memoria no volátil 210, el programa 220 y la unidad 230 de tratamiento del servidor 200, comprenden medios de análisis de las notificaciones recibidas de la estación de personalización, estos medios de análisis comprenden, particularmente, la memoria no volátil 210 y el programa 220.

Preferentemente, los medios de tratamiento y de control están adaptados para generar al menos un grupo de instrucciones de personalización en paralelo con la ejecución, por la estación de personalización, de otro grupo de instrucciones de personalización.

Ventajosamente, los medios de tratamiento y de control del servidor 200 comprenden unos medios de definición de grupos de instrucciones tales que el servidor 200 de personalización necesita la notificación de ejecución de al menos unas de las instrucciones precedentes para generar la primera instrucción del próximo grupo de instrucciones de personalización. Así, en el transcurso de la generación de grupos de instrucciones determinan, para cada instrucción, si su generación necesita una notificación de ejecución de al menos una de las instrucciones precedentes. Si es el caso, los medios de definición de grupos de instrucciones terminan el grupo de instrucciones precedentes antes de esta instrucción a generar en función de esta notificación y definen un nuevo grupo de instrucciones de personalización que comienza con dicha instrucción. Este funcionamiento de los medios de definición de grupos de instrucciones permite minimizar los intercambios entre el servidor y la estación de personalización.

Por ejemplo, la primera instrucción del nuevo grupo de instrucciones es una instrucción que interviene en un proceso criptográfico. Según otro ejemplo, se trata de una instrucción de memorización de un elemento en la entidad electrónica (por ejemplo, una tarjeta de memoria flash), el elemento a memorizar dependiendo del espacio de memoria disponible en la entidad electrónica. La primera instrucción del nuevo grupo de instrucciones necesita por lo tanto la notificación de la ejecución de una instrucción de determinación del espacio de memoria disponible en dicha entidad 100, instrucción que se encuentra, como se expone anteriormente, en el grupo de instrucciones precedente.

En una variante, el número de instrucciones del grupo de instrucciones puede ser fijo o determinado por el tamaño esperado de dicha notificación.

Los medios de tratamiento y de control 210 a 230 comprenden unos medios de emisión de instrucciones de control de la estación 240 de personalización. Esto permite al servidor 200 de personalización controlar la estación 240 de personalización utilizando ciertos medios utilizados para los grupos de instrucciones de personalización.

Las instrucciones de control de la estación 240 de personalización comprenden, preferentemente:

- un comando de puesta en tensión de la entidad electrónica portátil,

- un comando de retirada de tensión de la entidad electrónica portátil,

- un comando de selección del temporizador aplicado de la entidad electrónica portátil,

- un comando de determinación de un protocolo de comunicación entre la estación de personalización y la entidad electrónica portátil; en un modo de realización en el que la entidad electrónica portátil es una tarjeta de microcircuito, dicho comando de selección de protocolo permite una selección del protocolo T=1 y del protocolo T=0 definido conforme a la norma ISO 7816; en un modo de realización, dicho comando de determinación de un protocolo permite negociar la velocidad de transmisión de los datos intercambiados entre la entidad electrónica portátil y la estación de personalización,

- un comando de selección de la tensión aplicada a la entidad electrónica,

- un comando de suspensión de la personalización durante un tiempo determinado,

- un comando de especificación a la estación de personalización de un tiempo de espera máximo para obtener una respuesta de parte de la entidad electrónica portátil,

- un comando de inserción de un tiempo de espera antes de cada comando sea enviado a la entidad electrónica portátil,

- un comando de inserción de dato en dicha notificación emitida a la atención del servidor (ventaja: permite facilitar los controles realizados por el servidor),

- un comando de fin de personalización y/o

- un comando de información de anomalía de personalización.

Preferentemente, los medios de emisión están adaptados para transmitir grupos de instrucciones de personalización a una pluralidad de estaciones de personalización.

El servidor 200 de personalización se comunica con cada estación 240 de personalización según un protocolo cualquiera, preferentemente encriptado, a través de medios 235 de emisión de cada grupo de instrucciones de personalización con destino a la estación 240 de personalización de la entidad electrónica portátil 100. Recíprocamente, los medios 235 de emisión constituyen unos medios de recepción, de parte de la estación 240 de personalización, de al menos un identificador de la entidad electrónica portátil 100 y de notificación de ejecución de instrucciones de personalización.

La estación 240 de personalización comprende una memoria no volátil 270 que conserva unos pilotos 265 (en inglés *driver*) de pilotaje de lector 280 de entidad electrónica portátil 100 y un programa 275 de gestión de los grupos de instrucciones de personalización. La estación 240 de personalización comprende también un generador 245 de señal de temporizador, una alimentación 250, un circuito 255 de pilotaje del lector 280 y una unidad central CPU 260.

La unidad central CPU 260 y el programa de gestión de grupos de instrucciones 275 constituyen unos medios de recepción de al menos un grupo de instrucciones de personalización de la entidad electrónica portátil.

El lector 280 está dotado de una interfaz con o sin contacto con la entidad electrónica portátil 100. El lector 280 intercambia, con la entidad electrónica portátil 100 unas instrucciones, o comandos, y respuestas, por ejemplo en el formato APDU, unas señales de temporizador y de alimentación, según técnicas conocidas en el campo de los lectores de tarjetas inteligentes. La unidad central 260, el lector 280, los pilotos 265 y el programa 275 de gestión constituyen así unos medios de transmisión de al menos una instrucción de personalización con la entidad electrónica portátil 100.

El circuito 255 transmite al generador 245 unos comandos de determinación de una señal de temporizador, a la alimentación 250 unos comandos de puesta en tensión, de corte de alimentación y/o de determinación de la tensión, y al lector 280 unos comandos en el formato APDU.

Antes de describir más profundamente al menos un modo de realización particular del dispositivo y del procedimiento objetos de la presente invención, se recuerdan, después, varios detalles en la implementación del cálculo de la ATR por una tarjeta inteligente conforme a la norma ISO 7816, siendo aquí recordado que la presente invención no se limita a este tipo de tarjeta.

El programa de cálculo de la ATR forma parte de la máscara (o sistema de explotación) que es memorizado en la memoria solo de lectura ROM 130 de la entidad electrónica portátil 100. Este programa de cálculo puede utilizar informaciones de la memoria regrabable no volátil EEPROM 120 y de la memoria solo de lectura ROM 130. Se observa que, para el cálculo de la ATR, la memoria 120 no es inicializada.

El funcionamiento de la estación 240 de personalización es ilustrado en la figura 3.

En el transcurso de una etapa 300, la estación 240 de personalización envía al servidor 200 una petición de inicialización de la personalización que comprende una información de identificación del lote de entidad 100 a personalizar con el fin de inicializar los medios de tratamiento de control de personalización. En un modo de realización descrito más adelante en relación con la figura 4, esta información de identificación es un número de lote, al que estarán unidos, por el servidor 200, grupos de datos de personalización necesarios a la personalización de las entidades electrónicas portátiles del lote. Esta petición puede comprender igualmente informaciones de identificación de la estación 240 de personalización, que permiten al servidor 200 dirigirle la respuesta y, eventualmente, el tipo de estación 240 de personalización, el servidor 200 pudiendo necesitar esta información para conocer las instrucciones que puede enviar con destino a la estación 240.

El servidor 200 responde entonces a la estación 240 de personalización, ya sea por un mensaje de error, particularmente si el número de lote es inválido, ya sea por un acuse de recibo si no se ha encontrado ningún problema.

En el transcurso de una etapa 305, la estación 240 de personalización efectúa un cargo automático de una entidad electrónica portátil 100 en el lector 280, según unas técnicas conocidas en sí. Y después, en el transcurso de una etapa 310, la estación 240 de personalización detecta y pone en tensión la entidad electrónica portátil 100.

En el transcurso de una etapa 315, la estación 240 de personalización recibe el identificador de la entidad electrónica portátil 100 y comunica el identificador de esta entidad electrónica portátil 100 al servidor 200 así como una petición de grupo de instrucciones de personalización.

En el transcurso de una etapa 320, en función del identificador de la entidad electrónica portátil y de datos de personalización recibidos por otro lado, el servidor 200 de personalización genera un grupo de instrucciones de personalización y lo transmite a la estación 240 de personalización, preferentemente en forma encriptada, codificada o cifrada.

Preferentemente, en el transcurso de esta etapa 320, el servidor 200 de personalización define el primer grupo de instrucciones de personalización para que este grupo de instrucciones no se acabe más que cuando, para generar la instrucción siguiente, el servidor 200 necesite la notificación de ejecución de al menos una de las instrucciones precedentes.

El detalle de la etapa 320 es dado, más adelante, en relación con la figura 4 así como una descripción de etapas preliminares 400 y 405 implementadas por el servidor 200 de personalización o por otro ordenador (no representado) unido al servidor 200.

En el transcurso de una etapa 325, la estación 240 de personalización recibe el grupo de instrucciones de personalización y transmite cada comando en el formato APDU del grupo de instrucciones de personalización a la entidad electrónica portátil 100.

Los datos de personalización de la entidad electrónica portátil son entonces memorizados en su memoria, generalmente en una memoria no volátil regrabable, por ejemplo una memoria de tipo EEPROM, particularmente adaptada a la memorización de este tipo de datos que varían de una entidad a otra.

Preferentemente, la estación 240 de personalización realiza al menos una instrucción de control de al menos una instrucción de personalización después de haber transmitido, a la entidad electrónica portátil, otra instrucción de personalización referida por esta instrucción de control.

Si, para un comando en el formato APDU, ninguna instrucción de control integrada en el grupo de instrucciones de personalización recibido se refiere a esta instrucción en el formato APDU, la estación 240 espera, de parte de la

entidad 100, un código estándar que indica que la instrucción de personalización ha sido bien ejecutada y verifica este código estándar.

Si no, la estación 240 espera una respuesta en el formato APDU específica en un intervalo de tiempo específico, si esta respuesta y/o este intervalo de tiempo específicos son especificados en una instrucción de control incorporado en el grupo de instrucciones de personalización recibido.

En caso de problema, es decir, según los casos, en ausencia de recepción del código estándar o de la respuesta esperada durante el intervalo de tiempo específico, la personalización de la entidad 100 es interrumpida y un mensaje de interrupción de personalización es transmitido, por la estación 240 de personalización al servidor 200.

En la ausencia de problema, cada respuesta es colocada en una memoria tampón (en inglés *buffer*), en el orden cronológico con otras informaciones de notificación de desarrollo de la personalización (por ejemplo, fecha, hora, identificador de la entidad 100).

Cuando la estación 240 de personalización ha recibido de la entidad electrónica portátil todas las respuestas asociadas a las instrucciones de personalización (o que una duración predeterminada transcurre sin recepción de una respuesta esperada, signo de una anomalía), la estación 240 emite, con destino al servidor 200, un mensaje de notificación, por ejemplo que comprende el contenido de una memoria tampón que contiene las respuestas en cuestión.

Con la recepción de cada mensaje de notificación, el servidor 200 analiza la notificación, en la etapa 335 y determina si debe activar una acción en función del resultado de este análisis. El servidor determina, particularmente, si un error ha sido detectado en el transcurso de la etapa 340. Si sí, en el transcurso de una etapa 345, el error es tratado. Por ejemplo, un mensaje de expulsión de la entidad 100 hacia un rebús es transmitido a la estación 240 de personalización. Si no, en el transcurso de una etapa 350, el servidor de personalización determina si la personalización de la entidad electrónica portátil 100 es terminada. Si sí, en el transcurso de una etapa 360, se carga una nueva entidad electrónica portátil en el lector 280 y se vuelve a la etapa 310. Si no, en el transcurso de una etapa 355, en función del identificador de la entidad electrónica portátil, de la notificación o notificaciones recibidas y de los datos de personalización recibidos por otro lado, el servidor 200 de personalización genera un nuevo grupo de instrucciones de personalización y las transmite a la estación 240 de personalización, preferentemente en forma encriptada, codificada o cifrada.

Preferentemente, en el transcurso de esta etapa 355, el servidor 200 de personalización define el nuevo grupo de instrucciones de personalización para que este grupo de instrucciones no se acabe más que cuando, para la instrucción siguiente, el servidor 200 necesite la notificación de ejecución de al menos una de las instrucciones precedentes.

Después se vuelve a la etapa 325.

La figura 4 ilustra unas etapas 400 y 405 efectuadas preliminarmente a la etapa 300 y unas etapas 410 a 435 efectuadas en el transcurso de la etapa 320. Como se ilustra en la figura 4, en el transcurso de una etapa 400, se definen unos perfiles de personalización, conjunto de datos asociados a un tipo de entidad electrónica portátil y que definen las características generales de la personalización de las entidades de este tipo, tales como la estructura de los datos (incluido eventualmente el programa aplicativo) y los datos comunes para inscribir en unas memorias de entidades electrónicas, o incluso datos de personalización física (caracteres a gofrar, codificación de la banda magnética, etc.) o gráfica (logo a imprimir en la superficie de la tarjeta, por ejemplo).

Por ejemplo, los perfiles comprenden una longitud máxima del nombre del portador, preferencias lingüísticas, identificaciones de redes autorizadas y/o redes prohibidas, una duración de validez y de elecciones técnicas del distribuidor de entidades.

El resto de la descripción de la figura 4 se refiere a las entidades electrónicas portátiles conformes a la norma ISO 7816.

La definición de un perfil de personalización respecto a un conjunto de criterios unidos a la estructura y a la utilización futura de la entidad electrónica, a saber por ejemplo las normas (por ejemplo, GSM en telefonía o EMV en el campo bancario) y aplicaciones (por ejemplo, VISA, MASTERCARD, marcas registradas) existentes, y la organización interna (material) de la entidad electrónica.

Preferentemente, en el transcurso de la etapa 400, para cada perfil, se efectúan las siguientes etapas:

- elección de al menos una aplicación en una lista predefinida de aplicaciones,

- configuración de parámetros asociados a cada aplicación elegida,

- selección de una plataforma material, es decir un tipo de entidad electrónica portátil, entre una lista de plataformas compatibles determinada en función de las aplicaciones elegidas y de los parámetros configurados,

- obtención del perfil de personalización en función de las aplicaciones elegidas, de los parámetros configurados y de la plataforma seleccionada.

Se simplifica así la generación de los datos de perfil de personalización. En efecto, la elección de la aplicación permite limitar considerablemente las soluciones posibles para los otros datos de personalización, lo que simplifica la generación de datos de perfil de configuración y hace fácil su implementación en forma interactiva, por ejemplo por medio de un sistema informático.

Se obtiene igualmente un acercamiento más funcional que permite concentrarse en las elecciones del cliente de la prestación de personalización, es decir, del distribuidor de entidades electrónicas portátiles, por ejemplo un banco, un operador de telefonía o una administración, limitando al mínimo los conocimientos técnicos (particularmente en el campo de la tarjeta de microcircuito) necesarios para la generación del perfil de personalización. En definitiva, se asegura la coherencia del conjunto de los elementos que entran en línea de cuenta para la definición del perfil ya que la compatibilidad de las aplicaciones, de su configuración y de la plataforma utilizada deriva de la solución propuesta.

La etapa 400 empieza por la elección de al menos una aplicación que las entidades electrónicas portátiles a personalizar deberán poder implementar. La elección de cada aplicación se efectúa en una lista predefinida, por ejemplo presentada al usuario del sistema en forma interactiva, por medio de un menú desplegable.

Se verifica entonces la coherencia de las aplicaciones elegidas. Cuando las aplicaciones elegidas no generan incoherencia, se configuran parámetros relativos a cada una de las aplicaciones elegidas. Por ejemplo, se configura la agenda telefónica (en inglés *phonebook*) de un teléfono móvil introduciendo los parámetros de la agenda tales como los definidos en la norma de telefonía móvil correspondiente. Se define así, por ejemplo, un número máximo de entradas en la agenda telefónica (en inglés *max number of entries*) igual a 250, una longitud máxima de nombres (en inglés *max length of name*) igual a 16 octetos. Esta configuración permite por lo tanto definir particularmente el tamaño de los ficheros para la memorización regrabable de la entidad electrónica portátil. Igualmente pueden ser definidas unas configuraciones por defecto para cada aplicación. La etapa de configuración comprende igualmente una etapa de verificación de la coherencia de las informaciones introducidas o seleccionadas, particularmente con el fin de asegurar la conformidad a las normas correspondientes.

En otro ejemplo adaptado al campo de las tarjetas bancarias, se determina la lengua preferida del futuro portador de la tarjeta seleccionándola en una lista de lenguas posibles.

Las elecciones de aplicaciones y de configuración de estas pueden entonces ser memorizadas, por ejemplo en forma de una base de datos, que da, por consiguiente, una descripción funcional del perfil de personalización, independientemente de la plataforma material (es decir, componentes y sistema de explotación) de la entidad electrónica portátil. Tal base de datos puede así ser reutilizada para la introducción de funcionalidades idénticas en otra plataforma material. La base de datos utiliza por ejemplo una estructura de tipo objeto en el seno de la cual cada elección del usuario es memorizada como una instancia de un objeto de una de las clases predefinidas.

Gracias, particularmente, al mecanismo de herencia, se evita duplicar códigos inútiles, definiendo clases generales que describen un perfil de configuración y unas funcionalidades comunes a numerosas aplicaciones, y definiendo clases que describen funcionalidades específicas a una aplicación dada que hereda atributos de clases más generales.

Una vez determinada la definición funcional, se selecciona la plataforma a la que está destinada la personalización, en una lista de plataformas compatibles con la definición funcional definida a las etapas precedentes (por ejemplo debido a una capacidad de memoria suficiente y a una capacidad para implementar una aplicación particular, tal como JavaCard).

Las plataformas son por ejemplo definidas por la asociación de un componente (en general circuito integrado de la entidad a personalizar) y de un sistema de explotación (generalmente denominado “máscara” en el campo de las tarjetas de microcircuito).

Se puede prever visualizar, en asociación con cada plataforma compatible, informaciones que permiten facilitar la elección de una plataforma, tales como por ejemplo, informaciones de coste, de fiabilidad de aprovisionamiento, de referencias de utilización precedente.

Una vez validada la elección de la plataforma, se genera, en la base de los elementos dados precedentemente, la imagen de memoria de la tarjeta (en inglés IC *card image*), que define los datos de la memoria EEPROM, fuera de los elementos propios al futuro portador de la entidad, por ejemplo en forma de un objeto. Esta imagen representa, particularmente, la estructura de fichero de la memoria EEPROM (conforme a la norma ISO 7816), así como el

contenido y el tamaño de los ficheros que han sido determinados durante la generación del perfil de personalización. Además de la descripción de los ficheros y de su estructura, la imagen de memoria contiene todas las otras informaciones que definen la memoria EEPROM de la entidad electrónica portátil tales como las zonas de memorias que contienen variables, así como su valor, fuera de los datos específicos al futuro portador.

Estas variables son, por ejemplo, memorizadas en forma TLV (acrónimo de *Tag Lengh Value*), es decir, sucesivamente identificador, longitud, valor. Las etapas de configuración precitadas pueden en efecto generar datos en esta forma, siendo fijado el valor a esta etapa o para definir ulteriormente según es común o no al conjunto de los futuros portadores de entidades electrónicas portátiles.

La estructura de dos imágenes puede así ser diferente aunque los servicios dados por las entidades que las implementan sean idénticos. Los datos para los que el valor es desconocido son posicionados, sin valor, en estas imágenes de circuito integrado.

Eventualmente, se realiza una tarjeta de prueba con un lector de mesa y después se efectúa la personalización evocada anteriormente y, en definitiva, la personalización que implementa el procedimiento y/o el dispositivo objeto de la presente invención, completando, para cada entidad, los valores de los campos o datos incluso vírgenes.

Preferentemente, cada grupo de datos de personalización es asociado a un identificador llamado “segundo”, el término de “identificador primero” estando reservado, en toda la descripción, a un identificador de entidad electrónica portátil generado a partir de datos conservados en la memoria no regrabable ROM 130 de tal entidad. El identificador segundo es típicamente la cadena de caracteres utilizada para designar la plataforma.

Los grupos de datos comprenden, preferentemente, instrucciones de personalización, personalización que puede referirse, además de al contenido de las memorias de la entidad electrónica portátil 100, su apariencia física, como, por ejemplo, su gofrado o la impresión de su superficie, o incluso el registro en una banda magnética. En lo que se refiere a la personalización del contenido de la memoria EEPROM, se recorren unos perfiles de personalización (grupos de datos de personalización que forman el conjunto de los datos de personalización comunes a todas las entidades electrónicas portátiles del mismo tipo, definido por una máscara o una máscara y un circuito integrado) para formar y memorizar estas instrucciones. Estas instrucciones son, en un modo de realización, comandos en el formato APDU. Se puede, por ejemplo, formar todos los comandos en el formato APDU para la creación de la estructura de fichero de la memoria de una tarjeta inteligente. Se puede, de hecho, generar todos los comandos de inicialización que se llaman también “comando de pre-personalización”. El lector podrá remitirse a la patente US 6196459 para el detalle de esta pre-personalización.

En unos modos de funcionamiento, los medios de personalización generan las instrucciones de personalización a partir de los datos contenidos en el grupo de datos de personalización seleccionado. Por ejemplo, si, durante el recorrido de un grupo de datos de personalización, se encuentra una palabra clave que define un fichero, se forma la instrucción de fichero correspondiente. En unos modos de funcionamiento, se integran unos comandos APDU en la imagen. En unos modos de funcionamiento, se prepara el cuerpo de los comandos en el formato APDU que comprende una parte variable que es completada por datos de personalización. Se integra así, en el grupo de datos de personalización, los cuerpos de comandos APDU que serán completados por los datos propios de cada portador en el momento de la personalización.

Como se ha expuesto anteriormente, en unos modos de realización particulares, los grupos de datos de personalización comprenden al menos una imagen de la estructura de al menos una parte de la memoria de la entidad electrónica portátil.

Así, en el transcurso de la etapa 400, en la figura 4, se produce una imagen de la memoria de la tarjeta (esencialmente la estructura de fichero y las variables en forma TLV), a partir de la selección de una aplicación y se producen preferentemente las instrucciones de personalización a partir de esta imagen, lo que permite adaptarse a la plataforma, a la máquina, y por lo tanto mejorar la flexibilidad de la personalización. Eventualmente, las instrucciones de personalización están en la imagen.

En el transcurso de una etapa 405, el servidor 200 de personalización recibe y memoriza una pluralidad de grupos de datos de personalización.

En el momento de la preparación de la inicialización del lote, etapa 410, se asocian al lote entidades electrónicas portátiles a personalizar, una pluralidad de grupos de datos de personalización, en la memoria del servidor 200 de personalización.

Se señala que, en unos modos de realización, las etapas 400 y 405 son efectuadas en otro ordenador, por ejemplo portátil, los perfiles o grupos de datos de personalización siendo después cargados en el servidor 200.

Se observa que en este estado, los grupos de datos no poseen ni los valores específicos a los futuros portadores de entidades.

En el transcurso de la etapa 320, se efectúa, primero, una etapa 410, en el transcurso de la cual se utiliza el perfil de personalización, formado por ejemplo por la imagen de memoria y eventualmente por otros parámetros unidos por ejemplo al aspecto físico de la entidad electrónica portátil, para la personalización de cada entidad del lote, integrando en la imagen de memoria precedentemente definida, los datos propios de cada futuro portador.

El servidor 200 elige entonces, entre las imágenes de circuito integrado, la que corresponde a cada entidad electrónica portátil del lote. Después los comandos en el formato APDU son preparados como se describe anteriormente. En el transcurso de una etapa 415 correspondiente a la etapa 310 de la figura 3, la estación 240 de personalización pone en tensión o pone a cero la entidad electrónica portátil 100 y obtiene, en respuesta, de la entidad 100, datos llamados ATR (acrónimo de *Answer to Reset* para respuesta a la puesta en tensión). Se recuerda que el programa de cálculo de la ATR forma parte de la máscara (o sistema de explotación) que es memorizada en la memoria solo de lectura ROM 130 de la entidad electrónica portátil 100. Este programa de cálculo puede utilizar informaciones de la memoria regrabable no volátil EEPROM 120 y de la memoria solo de lectura ROM 130.

En una variante que no forma parte de la invención, la estación 240 de personalización emite una petición de identificador primero con destino a la entidad electrónica portátil 100 y recibe, de vuelta, el identificador primero.

En el transcurso de una etapa 420 correspondiente a la etapa 315 de la figura 3, la estación 240 de personalización transmite el identificador primero de la entidad electrónica portátil 100 al servidor 200 de personalización. Este identificador primero es, eventualmente, completado por un identificador de la estación de personalización con el fin de que el servidor de personalización pueda dirigir mensajes específicos a esta estación.

En el transcurso de una etapa 425, el servidor 200 de personalización asocia el identificador primero, de la entidad electrónica portátil, a al menos un identificador segundo, de grupo de datos de personalización, por ejemplo implementando una tabla de correspondencia.

Estos grupos de datos son memorizados, en el servidor 200, en asociación con los identificadores segundos, los octetos históricos que corresponden respectivamente a las máscaras, a las máscaras asociadas a circuitos y/o a los circuitos de las entidades electrónicas portátiles 100.

Cuando se obtienen dichos octetos históricos de la entidad electrónica portátil que lo va a personalizar, se comparan con esos asociados a los grupos de datos de personalización y se elige cada grupo de datos para el que la comparación es positiva (este puede ser la igualdad, la inclusión, etc.).

En el transcurso de una etapa 430, se efectúa la creación, o formación, de grupos de instrucciones de personalización a partir de los datos o perfiles de personalización, que comprenden, eventualmente, comandos APDU y cuerpos de comandos APDU. Si los comandos APDU son, al menos en parte, generados durante la etapa 400, en el transcurso de la etapa 430, se completan los que deben ser completados por datos específicos a los futuros portadores de las entidades electrónicas portátiles.

En el transcurso de una etapa 435, el servidor 200 de personalización efectúa la decodificación y/o análisis necesario, y transmite cada comando en el formato APDU del grupo de instrucciones a la estación de personalización.

La figura 6 ilustra, en detalle, la etapa 325. En primer lugar, en el transcurso de una etapa 605, la estación 240 de personalización recibe un grupo de instrucciones de personalización de parte del servidor 200. Y después, en el transcurso de una etapa 610, la estación 240 de personalización efectúa una extracción de la próxima instrucción del último grupo de instrucciones de personalización recibido. Durante la primera iteración de la etapa 610, la próxima instrucción es la primera instrucción.

En el transcurso de una etapa 615, la estación 240 de personalización determina si la instrucción extraída es asociada a una instrucción de control, es decir, aquí, identifica una respuesta a esperar de la entidad electrónica portátil.

Si sí, en el transcurso de una etapa 625, la estación 240 de personalización extrae, del grupo de instrucciones de personalización, la identificación de la respuesta a esperar. Si no, en el transcurso de una etapa 620, la estación 240 de personalización memoriza, como respuesta esperada, una respuesta estándar, independiente de la instrucción de personalización.

A continuación de una de las etapas 620 ó 625, la estación de personalización extrae el comando en el formato APDU de la instrucción extraída y la transmite a la entidad electrónica portátil 100, en el transcurso de una etapa 630. Por ejemplo, esta instrucción permite la inscripción, por la entidad electrónica portátil 100, de datos en la memoria no volátil EEPROM 140 de la entidad electrónica portátil 100.

Y después, en el transcurso de una etapa 635, la estación 240 de personalización espera una respuesta de la

entidad 100. Durante la recepción de una respuesta de parte de la entidad 100 o al final de la duración máxima de espera, la estación de personalización inscribe el contenido del comando y de la respuesta, eventualmente vacía, en una memoria tampón de notificación, de manera cronológica en el transcurso de una etapa 640.

En el transcurso de una etapa 645, la estación 240 de personalización determina si la respuesta obtenida es idéntica a la respuesta esperada. Si no, en el transcurso de una etapa 650, la estación 240 envía un mensaje de error al servidor 200 así como el contenido de la memoria tampón de notificación. Si sí, en el transcurso de una etapa 655, la estación 240 de personalización determina si el último grupo de instrucciones recibido comprende incluso al menos una instrucción. Si no, la etapa 325 se acaba. Si sí, se vuelve a la etapa 610.

Se observa, en la figura 5A, que una petición 500 de inicialización de personalización, enviada por la estación 240 al servidor 200, puede comprender un código 502 de inicialización, por ejemplo en 2 octetos, un número de lote 504, por ejemplo en 2 octetos, y un número de estación 506, por ejemplo en 2 octetos.

La petición de inicialización es enviada una sola vez por lote como se indica en relación con la etapa 300, en la figura 3.

Un ejemplo de respuesta 508, del servidor 200 es dado en la figura 5B. Comprende un código 510 de acuse de recibo. Otro ejemplo de respuesta 512 es dado en la figura 5C. Comprende un código 514 de fallo de recepción y un número 516 de error.

Cuando el lote se termina (la detección del final del lote es generalmente realizada por un sensor de la estación 240, o por un descuento de las entidades electrónicas portátiles), la estación 240 envía un mensaje de fin de personalización al servidor. Este mensaje 518, ilustrado en la figura 5D, comprende un código 520 de fin de lote y puede comprender informaciones de identificación del lote y/o de la máquina 522 de personalización.

Una vez que el acuse de recibo al comando de inicialización de la personalización es recibido, tras la detección de una nueva entidad 100 en el lector 280, la estación 240 comunica al servidor 200, en un solo comando, el identificador, por ejemplo la ATR (el acrónimo de *Answer to Reset* para respuesta a la inicialización), de la entidad 100 y una petición de grupo de instrucciones de personalización. Un ejemplo de tal comando 524 es ilustrado en la figura 5E. Este comando 524 comprende un código de comunicación ATR 526, un número de lote 528, un identificador de estación de personalización, por ejemplo un número de estación de personalización, un dato de longitud de identificador ATR 532 y el identificador ATR 534, de longitud variable.

Se recuerda que la ATR, cuyo contenido es definido por la norma ISO 7816, es la primera respuesta de una tarjeta después de la puesta a cero (típicamente en la puesta en tensión). La ATR puede contener, en unos octetos llamados históricos, informaciones en la plataforma (circuito y máscara o circuito o máscara) comunicadas al lector 280. Son particularmente estas informaciones las que son utilizadas por el servidor 200 para formar los grupos de instrucciones de personalización.

Un ejemplo de respuesta 536 del servidor 200 es ilustrado en la figura 5F. Esta respuesta 536 comprende un encabezamiento de grupo de instrucciones de personalización 538 y un grupo de instrucciones de personalización 540, de longitud variable.

En otro modo de realización, la etapa de comunicación del identificador ATR es remplazada por una simple petición de grupo de instrucciones de personalización enviada por la estación 240 al servidor 200, en detección de una nueva entidad 100 o, más generalmente, en el momento del lanzamiento de un nuevo lote de entidades 100. Un ejemplo de tal petición 542 es ilustrado en la figura 5G y comprende un código 544 de petición, un código 546 de lote y un número 548 de estación.

En este modo de realización, el primer grupo 550 de instrucciones, enviado por el servidor 200 a la estación 240 de personalización, comprende un comando de puesta en tensión de la entidad electrónica portátil 100. Un ejemplo de primer grupo 550 de instrucciones es ilustrado en la figura 5H. Comprende un número de instrucción 552, un tipo 554 de instrucción a la atención de la estación 240 de personalización y un código 556 de instrucción de puesta en tensión.

La estación 240 de personalización recupera e inserta después el identificador ATR de la entidad electrónica portátil en una notificación 558, cuyo ejemplo es ilustrado en la figura 5I. Comprende un número 560 de notificación, una longitud 562 de identificador ATR y un identificador ATR 564, de longitud variable.

El servidor 200 define después cada grupo de instrucciones de personalización para que un grupo de instrucciones no se acabe más que cuando, para la instrucción siguiente, el servidor necesite la notificación de ejecución de al menos una de las instrucciones precedentes.

Por ejemplo, la primera instrucción del nuevo grupo de instrucciones es una instrucción que interviene en un proceso criptográfico. Por ejemplo, la última instrucción del grupo de instrucciones precedente puede ser un comando en el

formato APDU denominado *get challen*ge según la norma ISO 7816, que permite obtener de la tarjeta un *challenge*, es decir, un nombre aleatorio, para permitir al servidor 200 autentificarse calculando un código de autentificación calculado encriptando el *challenge* a partir de una clave, por el sesgo de un módulo asegurado externo material llamado HSM (acrónimo de *Hardware Security Module*, y enviando este código de autentificación, por un comando en el formato APDU denominado *external authenticate* (para autentificación externa) según la norma ISO 7816, a la entidad electrónica portátil 100, que lo compara entonces con el código de autentificación que esta misma ha calculado a partir de la misma clave, del *challenge*, y utilizando medios criptográficos que le son propios, y que acepta la autentificación en el caso de que los dos códigos sean iguales.

Se ilustran, en la figura 7A, detalles de un grupo 700 de instrucciones de personalización. Comprende una instrucción primera 702, una instrucción segunda 704, y así seguido hasta las últimas instrucciones 706 y 708, teniendo cada instrucción una longitud variable.

Se observa, en la figura 7B, que una instrucción 710 con destino a la entidad electrónica portátil 100 comprende un número de instrucciones 712 y un tipo de instrucción 714 que indica si una respuesta esperada es especificada. La instrucción 710 comprende también una longitud 716 de instrucción, un comando 718 en el formato APDU, una longitud 720 de respuesta esperada y, opcionalmente, en función del tipo de instrucción, un contenido 722 de respuesta esperada.

Dos tipos de instrucciones de control con destino a la estación 240 de personalización son representadas en las figuras 7C y 7D. El tipo de instrucción 724 de control comprende un número 726 de instrucción, un tipo 728 de instrucción y un código 730 de instrucción. El tipo 732 de instrucción de control comprende un número 734 de instrucción, un tipo 736 de instrucción, un código 738 de instrucción y datos 740. Los tipos 728 y 736 de instrucción indican que la instrucción tiene destino a la estación 240. Los códigos 730 y 738 de instrucción indican, por ejemplo, que se trata de una instrucción de puesta en tensión, de una instrucción de retirada de tensión, de una instrucción de modificación del temporizador o de una instrucción de selección de protocolo. Los datos 740 indican, por ejemplo, una frecuencia de temporizador o una tensión a suministrar a la entidad 100. En estos últimos casos, las instrucciones de notificación están implícitas.

La figura 7E ilustra un ejemplo de notificación 742 emitida por la estación 240 de personalización con destino al servidor 200. Esta notificación 742 comprende un código 744 de notificación, una información primera 746 de rendimiento, una información segunda 748 de notificación y así seguido hasta una última información 750 de notificación, teniendo cada una de las informaciones de notificación una longitud variable.

Un ejemplo de información 752 de notificación es dada en la figura 7F. Esta instrucción 752 de notificación comprende un número 754 de instrucción, una longitud 756 de respuesta y una respuesta 758 de longitud variable.

En la recepción de la notificación, el servidor 200 analiza dicha notificación, trata las anomalías eventuales (por ejemplo, parando la personalización) y envía un nuevo grupo de instrucciones de personalización a la estación 240 de personalización con el fin de proseguir el desarrollo de la personalización. Cuando la personalización de una entidad electrónica portátil es terminada, el servidor 200 envía una instrucción específica a la estación 240 de personalización. La estación 240 de personalización puede entonces descargar automáticamente la entidad electrónica portátil 100 del lector 280 con el fin de que la estación 240 prosiga el proceso de personalización, por ejemplo, por una etapa de gofrado en la misma estación o en una estación diferente, y cargar automáticamente una nueva entidad 100 en el lector 280 con el fin de iniciar la personalización eléctrica de esta entidad 100.

Un ejemplo de instrucción específica de fin de personalización 760 es ilustrado en la figura 7G. En unos modos de realización, la instrucción específica representativa de fin de personalización es la sola instrucción de personalización de un grupo de instrucciones de personalización. Esta disposición es ventajosa porque permite al servidor analizar todas las notificaciones que conciernen a una entidad electrónica portátil antes de transmitir la instrucción representativa de fin de personalización. Esta instrucción específica 760 comprende un número 762 de instrucción, un tipo 764 de instrucción que precisa que esta instrucción tiene destino a la estación 240 y un código 766 de instrucción de fin de personalización sin anomalía.

Cuando la personalización es terminada, pero comprende anomalías, el servidor 200 envía una instrucción específica 768 para informar a la estación 240 de personalización, y por lo tanto al operador de esta estación 240 de personalización. Un ejemplo de tal instrucción específica 786 es ilustrado en la figura 7H y comprende un número 770 de instrucción, un tipo 772 de instrucción que precisa que esta instrucción es destinada a la estación 240 de personalización y un código 774 de instrucción de fin de personalización con anomalía.

La instrucción de fin de personalización, con o sin anomalía, puede encontrarse al final de un grupo de instrucciones de personalización. Preferentemente, esta instrucción es colocada en un grupo sin ninguna otra instrucción. Se puede prever igualmente un mensaje análogo enviado por el servidor 200 para señalar el fin de personalización de un lote de entidades electrónicas portátiles 100.

Preferentemente, la estación 240 de personalización comprende unos medios de transmisión, en el servidor 200, de

un mensaje de anomalía y, en caso de detección de anomalía, el servidor 200 de personalización para la personalización (que puede así ser retomada a continuación, etc.). Un ejemplo de instrucción 776 de anomalía de estación es ilustrado en la figura 7I. Esta instrucción 776 comprende un código 778 de instrucción de anomalía, un número 780 de estación y un código 782 de anomalía.

Por supuesto, los datos intercambiados entre el servidor 200 y la estación 240 pueden ser codificados según un protocolo o algoritmo criptográfico cualquiera.

Numerosas variantes o mejoras pueden ser consideradas para el sistema de personalización. Por ejemplo:

- Se puede prever hacer realizar unas instrucciones de control más complejas en la estación de personalización. Así, esta puede ser eventualmente de forma directa unida a un HSM, y una instrucción de control puede consistir en intercambiar informaciones con este HSM para efectuar una autentificación tal como la descrita más arriba.

- Se pueden igualmente prever unas instrucciones de notificación más complejas, por ejemplo que no permiten poner más que una parte de las respuestas de la entidad electrónica en la notificación, o insertar el resultado de un tratamiento, por ejemplo en parte aritmético, realizada por la estación a partir de las respuestas de la entidad electrónica.

- Con el fin de mejorar la cadencia de personalización, las instrucciones de controles realizados por la estación de personalización pueden ser ejecutados en paralelo intercambios con la entidad electrónica portátil. Así, esperando la respuesta de la entidad electrónica a una instrucción de personalización, la estación de personalización puede analizar la respuesta de la instrucción de personalización precedente e insertar las informaciones necesarias en dicha notificación.

- Con el fin igualmente de mejorar la cadencia de personalización, la preparación de los grupos de instrucción por el servidor puede ser realizada en paralelo con la ejecución de los grupos de instrucciones por la estación de personalización. En efecto, una parte de las instrucciones de un nuevo grupo de instrucciones es independiente de la notificación del grupo de instrucciones precedente. El servidor puede así preparar esta parte de las instrucciones de un nuevo grupo de instrucciones durante la ejecución del grupo de instrucciones precedente por la estación de personalización.

REIVINDICACIONES

1.- Dispositivo de personalización de una entidad electrónica portátil (100) que comprende:

- unos medios (200, 270, 405) de memorización de una pluralidad de grupos (275) de datos de personalización,

- unos medios (200, 255, 260, 280) de comunicación con una memoria no regrabable de dicha entidad electrónica portátil, adaptados para recibir (315, 415, 420) un identificador primero conservado en dicha memoria no regrabable,

- unos medios (200, 260, 320, 420, 425) de selección de al menos un grupo de datos de personalización en función del identificador primero, y

- unos medios (255, 260, 280, 325) de personalización de dicha entidad electrónica portátil a partir de cada grupo de datos de personalización seleccionado;

caracterizado porque dicho identificador primero es al menos una parte de un mensaje suministrado por la entidad electrónica portátil durante su puesta en tensión.

2.- Dispositivo según la reivindicación 1, caracterizado porque los medios de memorización están adaptados a que cada grupo de datos de personalización esté asociado a un identificador segundo, porque comprende medios de asociación de un identificador segundo a dicho identificador primero, y porque los medios de selección están adaptados para seleccionar (425) al menos un grupo de datos de personalización en función del identificador segundo correspondiente al identificador primero.

3.- Dispositivo según una cualquiera de las reivindicaciones 1 ó 2, caracterizado porque:

- los medios (200, 255, 260, 280) de comunicación están adaptados a que dicha entidad electrónica (100) esté conforme al menos en parte a la norma ISO 7816 y a que dicho mensaje sea una ATR (acrónimo de *Asnwer to Reset* para respuesta a la puesta en tensión), y

- los medios de comunicación están adaptados para efectuar una puesta a cero de la entidad electrónica portátil y para recibir el identificador primero en al menos una parte de un mensaje suministrado por la entidad electrónica portátil durante su puesta a cero.

4.- Dispositivo según una cualquiera de las reivindicaciones 1 a 3, caracterizado porque los medios (200, 255, 260, 280) de comunicación están adaptados para recibir el identificador primero que comprende al menos un octeto llamado “históricos” según la norma ISO 7816 (octetos T1, T2,…T9) de la ATR.

5.- Dispositivo según una cualquiera de las reivindicaciones 1 a 4, caracterizado porque:

- los medios (200, 270, 405) de memorización están adaptados a que dichos grupos de datos de personalización comprendan al menos una imagen (400) de la estructura de la memoria no volátil de la entidad electrónica portátil, representativa del contenido y del tamaño de fichero de la entidad electrónica portátil y de las zonas de memoria de la entidad electrónica portátil que contiene variables, así como su valor, fuera de los datos específicos al futuro portador de la entidad electrónica portátil, y

- los medios (255, 260, 280, 325) de personalización están adaptados para completar los campos vírgenes de dicha imagen de estructura con datos de personalización.

6.- Dispositivo según una cualquiera de las reivindicaciones 1 a 5, caracterizado porque la entidad electrónica (100) es una tarjeta de microcontrolador asegurado conforme al menos en parte a la norma ISO 7816.

7.- Dispositivo según una cualquiera de las reivindicaciones 1 a 6, caracterizado porque comprende:

- unos medios (200, 230) de tratamiento adaptados para tratar dichos datos de personalización y para generar al menos un grupo de instrucciones de personalización de la entidad electrónica portátil, al menos un grupo de instrucciones de personalización que comprende al menos una instrucción de control de personalización que permite a una estación (240) de personalización controlar la buena ejecución de al menos una instrucción de personalización, al menos una instrucción de personalización de un grupo de instrucciones de personalización que permite la inscripción, por la entidad electrónica portátil, de datos en la memoria de la entidad electrónica portátil, y

- unos medios de emisión de cada grupo de instrucciones de personalización.

8.- Dispositivo según la reivindicación 7, caracterizado porque los medios (200, 230) de tratamiento están, además, adaptados para generar al menos una instrucción de notificación de personalización que permite a la estación (240) de personalización confirmar al dispositivo la buena ejecución de al menos una parte de un grupo de instrucciones

de personalización, y para insertar al menos una instrucción de notificación en al menos un grupo de instrucciones de personalización, estando adaptados los medios de emisión para emitir al menos una instrucción de notificación con destino a la estación de personalización, comprendiendo el dispositivo, además, unos medios de recepción de al menos una notificación que proviene de la estación de personalización.

9.- Dispositivo según una cualquiera de las reivindicaciones 7 u 8, caracterizado porque comprende, además, unos medios (200, 230) de análisis capaces de analizar al menos una notificación recibida y de activar una acción en función del resultado de dicho análisis.

10.- Dispositivo según una cualquiera de las reivindicaciones 7 a 9, caracterizado porque los medios (200, 230) de tratamiento comprenden unos medios de definición de grupos de instrucciones tales que el dispositivo necesita la notificación de ejecución de al menos una de las instrucciones precedentes para generar la primera instrucción del próximo grupo de instrucciones de personalización.

11.- Dispositivo según una cualquiera de las reivindicaciones 7 a 10, caracterizado porque los medios (200) de comunicación están adaptados para recibir, además, al menos un identificador de dicha estación (240) de personalización.

12.- Dispositivo según una cualquiera de las reivindicaciones 7 a 11, caracterizado porque los medios (200, 230) de tratamiento están adaptados para generar al menos un grupo de instrucciones de personalización en paralelo con la ejecución de un grupo de instrucciones de personalización por la estación (240) de personalización.

13.- Dispositivo según una cualquiera de las reivindicaciones 1 a 6, caracterizado porque comprende:

- unos medios (260) de recepción de al menos un grupo de instrucciones de personalización de la entidad electrónica portátil (100), comprendiendo al menos un grupo de instrucciones al menos una instrucción de control de personalización que permite controlar la buena ejecución de al menos una instrucción de personalización, permitiendo al menos una instrucción de personalización de un grupo de instrucciones de personalización la inscripción, por la entidad electrónica portátil, de datos en la memoria de la entidad electrónica portátil,

- unos medios (255, 260, 280) de transmisión de al menos una instrucción de personalización a la entidad electrónica portátil, y

- unos medios (260) de tratamiento adaptados para tratar cada instrucción de control para controlar la buena ejecución de al menos una instrucción de personalización por la entidad electrónica portátil.

14.- Dispositivo según la reivindicación 13, caracterizado porque los medios (260) de tratamiento están adaptados para realizar al menos una instrucción de control de al menos una instrucción de personalización después de que los medios de transmisión hayan transmitido, a la entidad electrónica portátil, otra instrucción de personalización no referida por dicha instrucción de control.

15.- Dispositivo según una cualquiera de las reivindicaciones 13 ó 14, caracterizado porque los medios (260) de recepción están adaptados, además, para recibir al menos una instrucción de notificación de personalización y los medios (260) de tratamiento están adaptados, además, para preparar una notificación de ejecución de al menos un grupo de instrucciones de personalización, comprendiendo el dispositivo, además, unos medios de emisión de notificación con destino a un servidor (200) de personalización.

16.- Dispositivo según una cualquiera de las reivindicaciones 13 a 15, caracterizado porque los medios de recepción están adaptados para extraer al menos una instrucción de notificación de al menos un grupo de instrucciones de personalización.

17.- Procedimiento de personalización de una entidad electrónica portátil, que comprende:

- una etapa (405) de memorización, en un dispositivo de personalización, de una pluralidad de grupos de datos de personalización,

- una etapa (420) de comunicación con una memoria no regrabable de dicha entidad electrónica portátil (100) para recibir un identificador primero conservado en dicha memoria no regrabable,

- una etapa (430) de selección, por dicho dispositivo de personalización, de al menos un grupo de datos de personalización en función del identificador primero, y

- una etapa (435) de personalización de dicha entidad electrónica portátil a partir de cada grupo de datos de personalización seleccionado;

caracterizado porque dicho identificador primero es al menos una parte de un mensaje suministrado por la entidad

electrónica portátil durante su puesta en tensión.

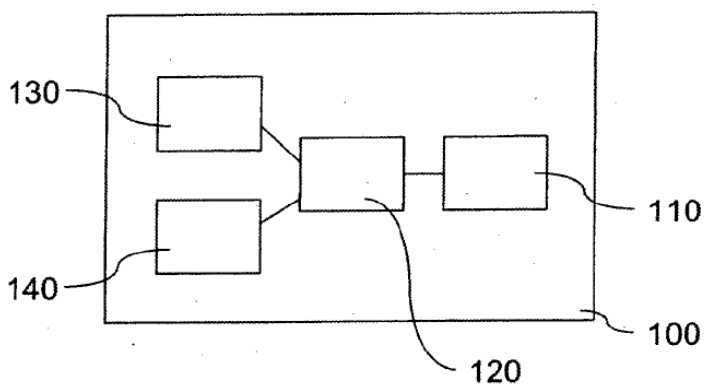

Figura 1

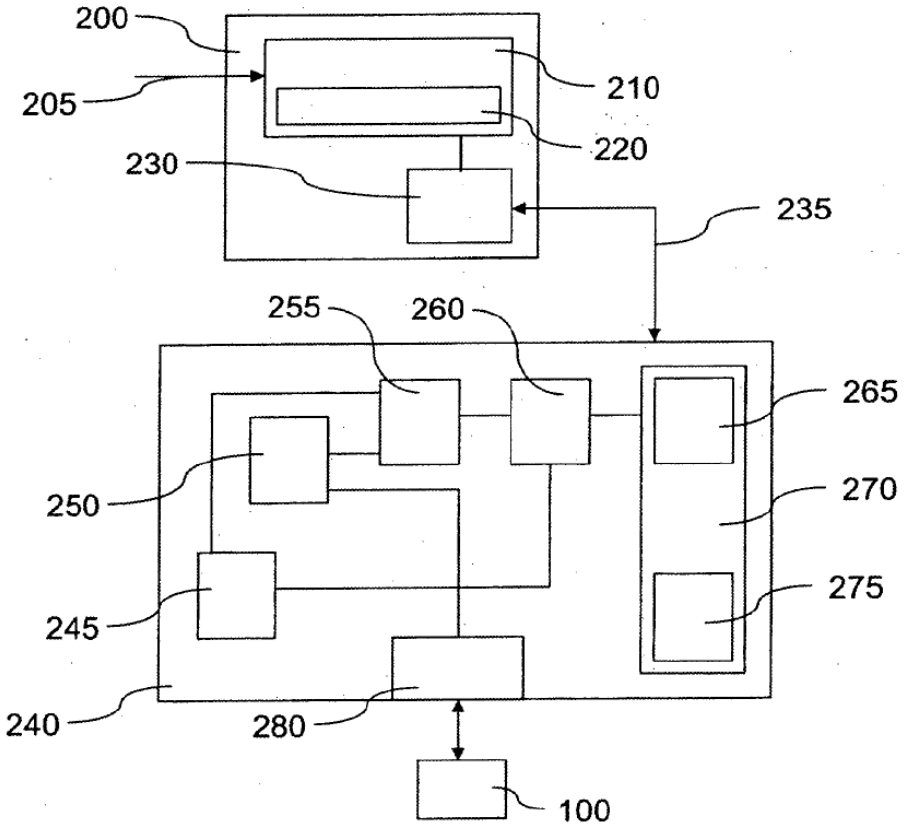

Figura 2

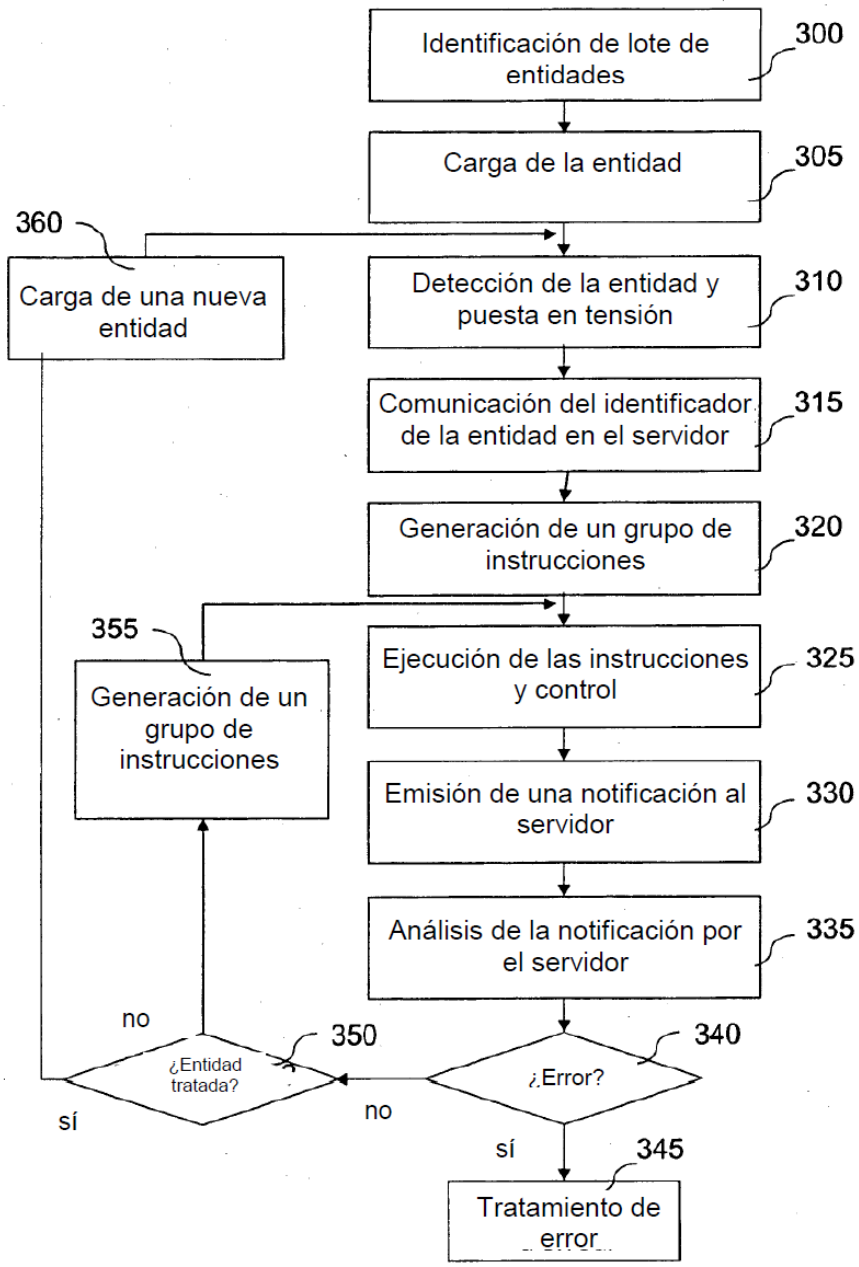
Identificación de lote de entidades
300
Carga de la entidad
305
360
Carga de una nueva entidad
Detección de la entidad y puesta en tensión
310
Comunicación del identificador de la entidad en el servidor
315
Generación de un grupo de instrucciones
320
355
Generación de un grupo de instrucciones
Ejecución de las instrucciones y control
325
Emisión de una notificación al servidor
330
Análisis de la notificación por el servidor
335
no
350
¿Entidad tratada?
sí
340
¿Error?
no
sí
345
Tratamiento de error

Figura 3

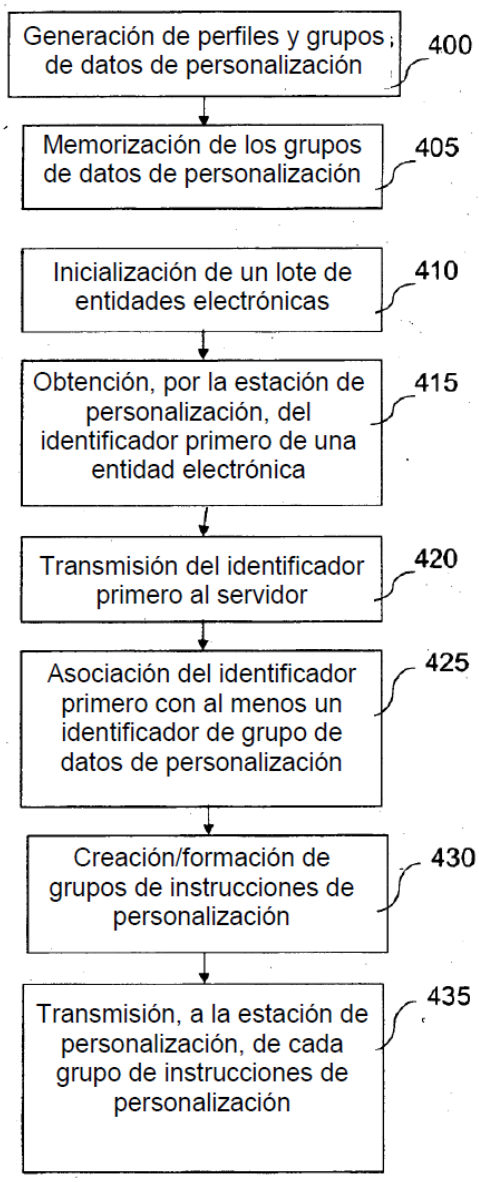
Generación de perfiles y grupos de datos de personalización
400
Memorización de los grupos de datos de personalización
405
Inicialización de un lote de entidades electrónicas
410
Obtención, por la estación de personalización, del identificador primero de una entidad electrónica
415
Transmisión del identificador primero al servidor
420
Asociación del identificador primero con al menos un identificador de grupo de datos de personalización
425
Creación/formación de grupos de instrucciones de personalización
430
Transmisión, a la estación de personalización, de cada grupo de instrucciones de personalización
435

Figura 4

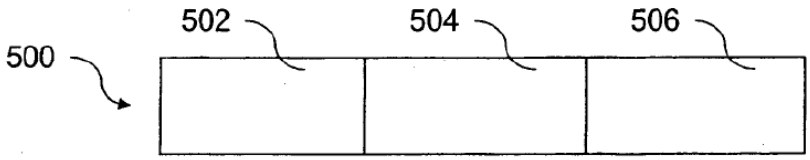

Figura 5A

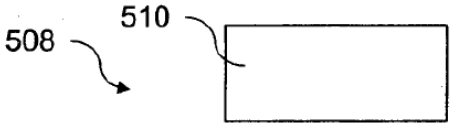

Figura 5B

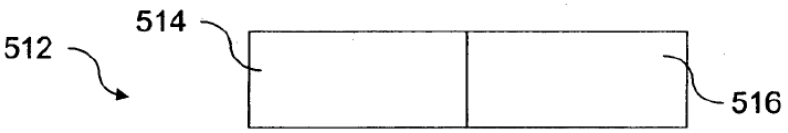

Figura 5C

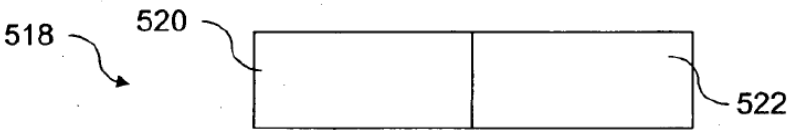

Figura 5D

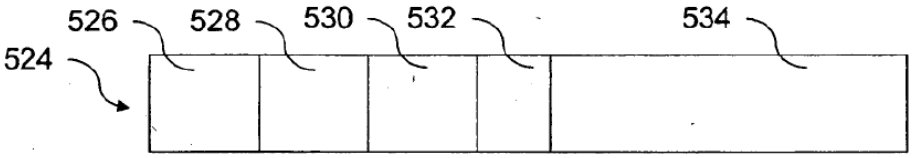

Figura 5E

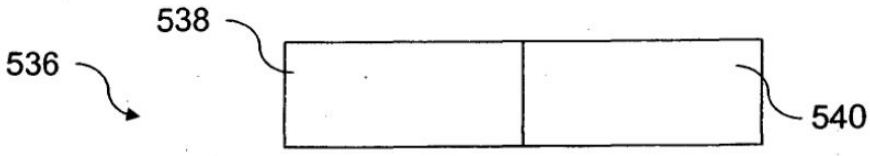

Figura 5F

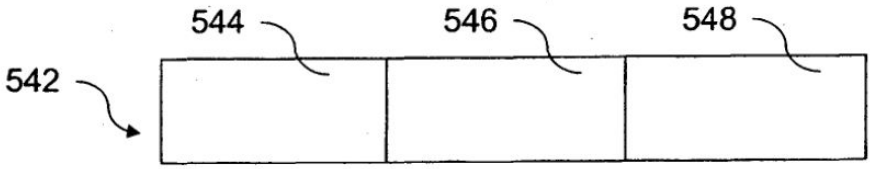

Figura 5G

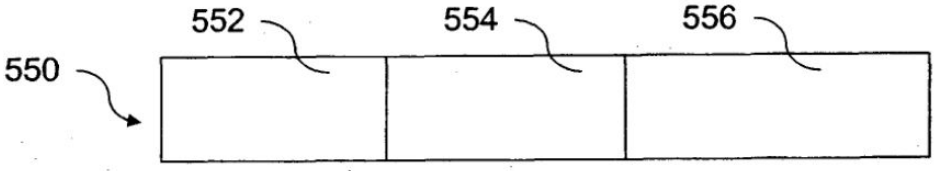

Figura 5H

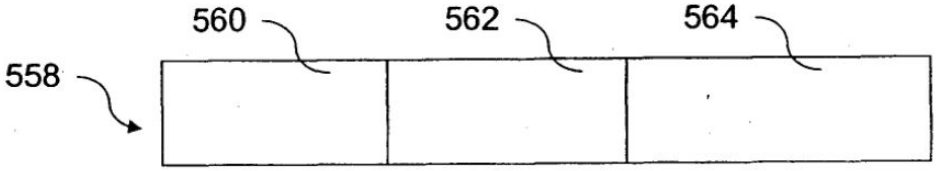

Figura 5I

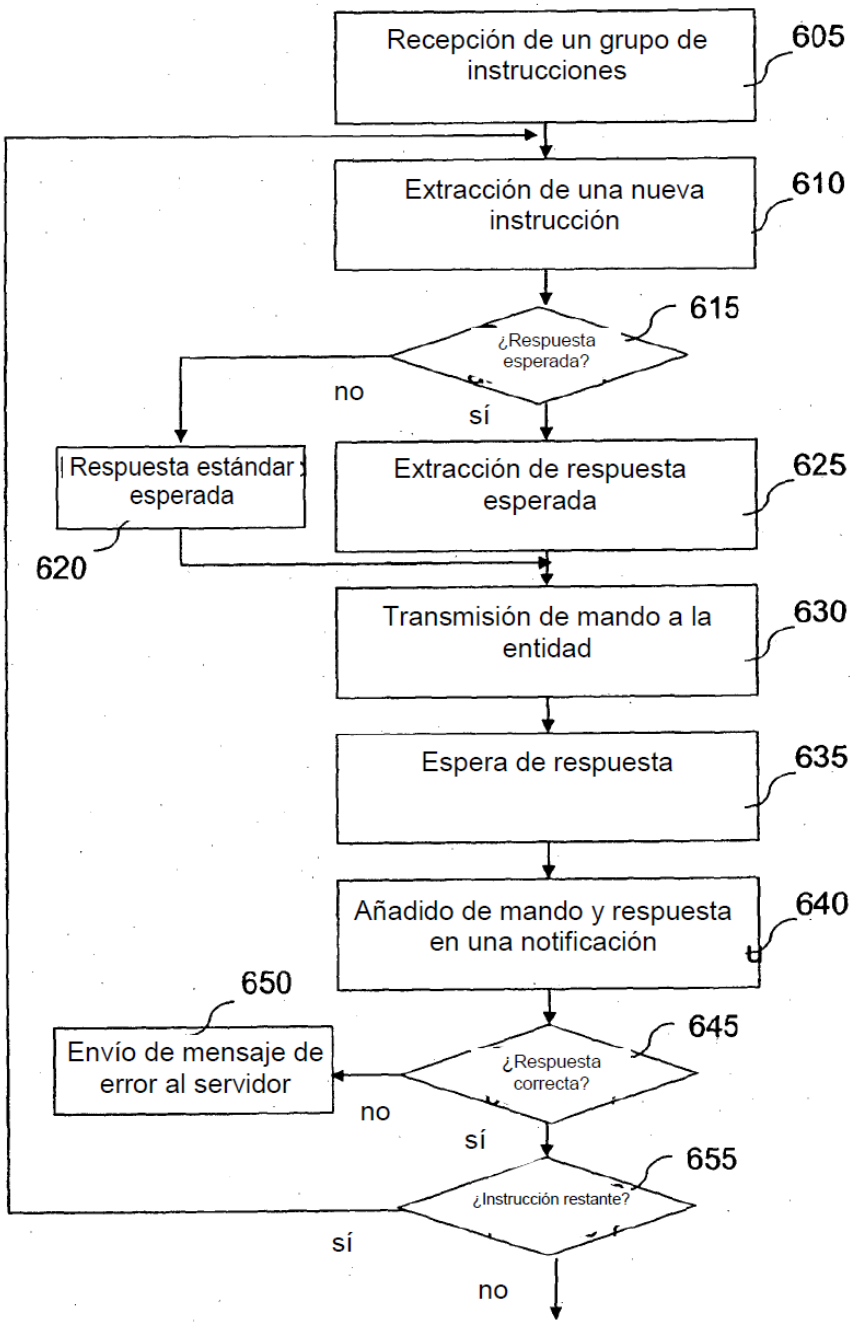
Recepción de un grupo de instrucciones
605
Extracción de una nueva instrucción
610
¿Respuesta esperada?
615
no
sí
Respuesta estándar esperada
620
Extracción de respuesta esperada
625
Transmisión de mando a la entidad
630
Espera de respuesta
635
Añadido de mando y respuesta en una notificación
640
¿Respuesta correcta?
645
650
Envío de mensaje de error al servidor
no
sí
¿Instrucción restante?
655
sí
no

Figura 6

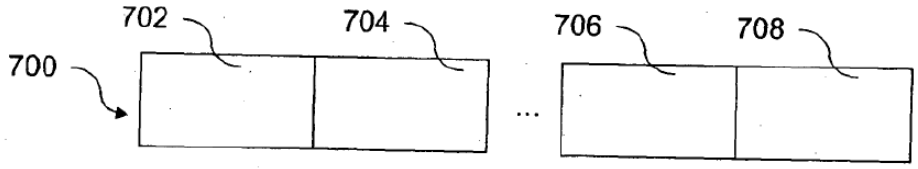

Figura 7A

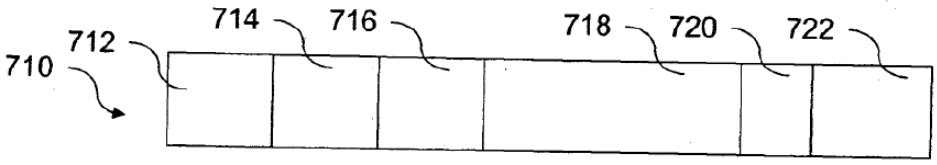

Figura 7B

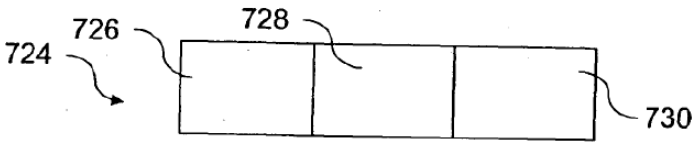

Figura 7C

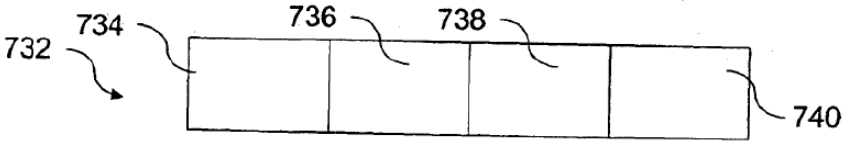

Figura 7D

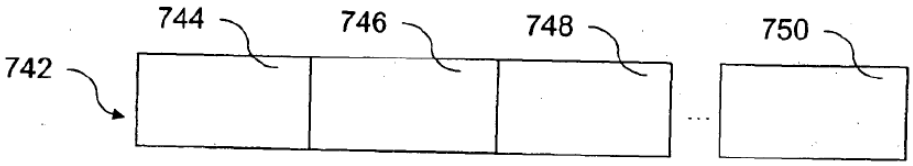

Figura 7E

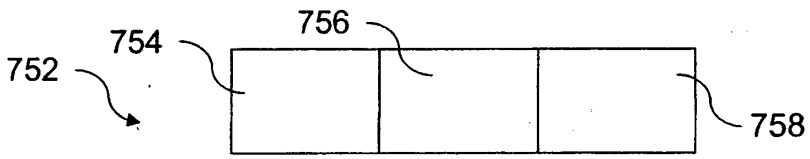

Figure 7F

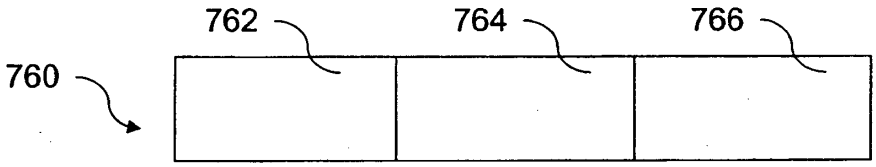

Figure 7G

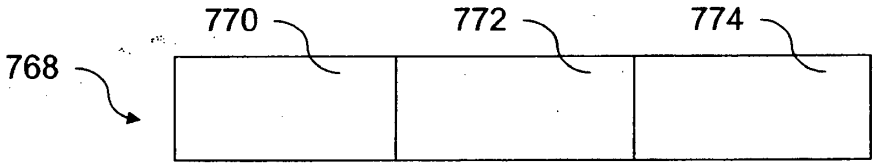

Figure 7H

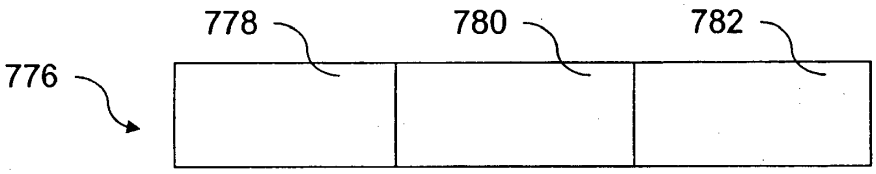

Figure 7I