(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 420 679**

(51) Int. CI.:

G07C 9/00 (2006.01)
G07F 7/08 (2006.01)
G07F 7/10 (2006.01)
G07F 17/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **05.11.2002 E 02292756 (0)**

(97) Fecha y número de publicación de la concesión europea: **27.02.2013 EP 1308909**

(54) Título: **Procedimiento de generación de datos pseudoaleatorios en una tarjeta inteligente y procedimiento de autenticación y su sistema**

(30) Prioridad:

06.11.2001 FR 0114351

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
26.08.2013

(73) Titular/es:

COMPAGNIE INDUSTRIELLE ET FINANCIERE D'INGENIERIE (INGENICO) (100.0%)
28-32 boulevard de Grenelle
75015 Paris, FR

(72) Inventor/es:

DEBORGIES, LUC y
CHOISET, BRUNO

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Procedimiento de generación de datos pseudoaleatorios en una tarjeta inteligente y procedimiento de autenticación y su sistema.

La presente invención concierne a un procedimiento de generación de datos imprevisibles mediante un objeto que incluye capacidades de tratamiento de datos. La invención concierne en concreto a un procedimiento de este tipo que permite a un objeto que dispone de tales capacidades, por ejemplo que comprende una tarjeta inteligente o un módulo de identidad, disponer de datos imprevisibles para su usuario, pudiendo estos datos ser idénticos para varios objetos informatizados similares. La invención concierne asimismo a un procedimiento y un sistema de control de un parque de tales objetos, pudiendo servir estos objetos para autenticar a personas o para realizar un descuento de crédito de tiempo o de crédito de otra índole, o para poner en práctica juegos multijugador que incluyen una parte aleatoria común para los participantes, o un control de utilización de otro dispositivo o sistema.

Por la técnica anterior, se conocen procedimientos que utilizan algoritmos capaces de generar datos aparentemente aleatorios, especialmente partiendo de un dato base llamado semilla («seed» en inglés). Estos algoritmos permiten así proporcionar datos que no son previsibles sin el conocimiento del dato semilla y presentan una distribución de valores que obedecen aproximadamente a unas normas de distribución aleatorias.

Tales datos imprevisibles o pseudoaleatorios pueden ser utilizados para simular un sorteo aleatorio, por ejemplo para programar en un ordenador juegos que utilizan una parte de azar. Este puede ser el caso para videojuegos o juegos informáticos para sustituir un lanzamiento de dados. Esto puede permitir realizar un juego de tipo lotería que reúne a varios usuarios de un mismo ordenador o a usuarios de ordenadores enlazados entre sí.

Tales datos pseudoaleatorios pueden ser utilizados para proporcionar en cualesquiera programas unos eventos que no presentan correlación aparente con eventos en el seno del programa o acciones del usuario. Puede tratarse de generar eventos aleatorios en un programa de simulación, por ejemplo para generar condiciones meteorológicas o incidentes que manejar.

Puede tratarse asimismo de autenticar un ordenador verificando que realmente incluye una versión determinada de tal algoritmo, o una clave determinada que incluye un dato utilizable dentro de tal algoritmo. Esta verificación puede llevarse entonces a cabo comunicando tal dato semilla a ese ordenador y solicitándole que calcule un dato pseudoaleatorio, llamado firma, mediante tal algoritmo. Tal algoritmo puede incluir en concreto la utilización de una clave determinada. Comparando la firma calculada por el ordenador que ha de autenticarse con una firma de control calculada por un ordenador de referencia o de control que posee el mismo algoritmo y la misma clave, es posible así verificar que el ordenador realmente incluye esa información, sin tener que desvelar esa misma información.

La patente US 5361062 enseña por ejemplo un dispositivo portátil de identificación de una persona. Este dispositivo genera un código pseudoaleatorio a partir de un código individual que identifica a esa persona, al combinar ese código individual con un dato extraído de un reloj embarcado en el dispositivo.

La patente WO 9106926 también enseña efectuar un control de identificación de persona, disparando esa generación de código pseudoaleatorio mediante una señal recibida por el dispositivo. Esta señal es emitida entonces por la estación de control y constituye una mera señal de disparo del dispositivo del que es portadora la persona que ha de identificarse.

Estos procedimientos presentan no obstante el inconveniente de que tan sólo en determinadas condiciones de coordinación pueden generar datos pseudoaleatorios que sean los mismos en varios objetos informatizados similares. Estos objetos, por ejemplo, deben estar conectados entre sí en un momento dado para poder recibir el mismo dato semilla. De lo contrario, estos objetos pueden proporcionar datos pseudoaleatorios tomando como base un dato semilla común, proporcionado por un reloj inicialmente común, que mantiene una sincronización entre ellos. No obstante, estos objetos deben incluir entonces una función de reloj que se halle permanentemente en funcionamiento. Tal funcionamiento continuo plantea problemas de energía que limitan la autonomía y el espacio ocupado por tal objeto. Asimismo, este precisa que la sincronización a lo largo del tiempo no deje de ser perfecta entre todos los objetos interesados, lo cual puede ser difícil de obtener por un largo tiempo y para un gran número de objetos.

En tal sentido, la patente AU 6568686 enseña, por otro lado, un procedimiento que permite sincronizar nuevamente un dispositivo de este tipo en el transcurso de su utilización.

La presente invención tiene pues por objeto subsanar los inconvenientes de la técnica anterior proponiendo un procedimiento que permite a una pluralidad de objetos informatizados, dotados de capacidades de tratamiento de datos, generar datos pseudoaleatorios que sean idénticos entre los distintos objetos sin precisar de comunicación entre ellos.

Esta finalidad se consigue mediante un procedimiento de generación de un dato pseudoaleatorio por un objeto informatizado que incluye unos medios de tratamiento de datos, unos medios de memorización, así como unos

medios de presentación o unos medios de comunicación con un dispositivo de tratamiento de datos llamado terminal, permitiendo este terminal la generación del dato pseudoaleatorio a partir de un dato semilla, constantemente diferente, proporcionado mediante la recepción de una señal exterior, y el cálculo por este objeto informatizado de un dato digital pseudoaleatorio, llamado firma, a partir de esa señal, con ayuda de un algoritmo memorizado en este objeto, caracterizado porque este cálculo se efectúa en la recepción de la señal exterior, por al menos un objeto informatizado o por al menos un terminal, señal esta que varía con el paso del tiempo y que es difundida, independientemente del estado de funcionamiento del objeto informatizado, dentro de una zona determinada y que puede ser recibida o interpretada de manera idéntica por otros objetos o terminales en diferentes ubicaciones de esa misma zona.

Según una peculiaridad, la señal es una señal de radio, es decir, que utiliza ondas electromagnéticas, emitida por un transmisor de difusión, incluyendo además el procedimiento las siguientes etapas:

- recepción de la señal de radio por parte del terminal;
- extracción de datos de señal a partir de esa señal de radio;
- transmisión de esos datos de señal al objeto informatizado.

Según una peculiaridad, la señal de radio representa información que incluye características irregulares o no previsibles.

Según una peculiaridad, la señal de radio se recibe mediante la lectura de una onda subportadora, asociada a una difusión de ondas radiofónicas.

Según una peculiaridad, la señal incluye la emisión, durante una pluralidad de períodos de tiempo determinados, de una información constante o interpretable de manera constante dentro de cada uno de estos períodos determinados, información esta que varía de uno a otro de estos períodos de una manera irregular o no previsible.

Es otra finalidad proponer un procedimiento de autenticación de un objeto informatizado dotado de capacidades de tratamiento de datos o de control de su validez.

Esta finalidad se consigue mediante un procedimiento de control de un objeto informatizado, incluyendo este objeto informatizado unos medios de tratamiento de datos, unos medios de memorización, así como unos medios de presentación o unos medios de comunicación con un dispositivo de tratamiento de datos llamado terminal, caracterizado porque incluye las siguientes etapas:

- generación de un dato pseudoaleatorio, llamado firma, por parte de este objeto informatizado utilizando un procedimiento tal y como se ha descrito anteriormente;
- presentación de esta firma, o transmisión de esta firma al terminal, con fines de verificación con relación a un dato calculado por otro aparato a partir de la misma señal digital o analógica, pudiendo llevarse a cabo esta verificación en el terminal o fuera del mismo.

Según una peculiaridad, el procedimiento incluye una etapa de comparación que verifica el valor de un dato, llamado dato de validez, memorizado en el objeto informatizado, verificación esta que condiciona o modifica el cálculo, la presentación o la transmisión de la firma.

Según una peculiaridad, el procedimiento incluye una etapa de presentación, en unos medios de presentación del terminal, de la firma que el terminal recibe del objeto informatizado.

Según una peculiaridad, la firma es calculada por el objeto informatizado mediante un algoritmo, llamado algoritmo de firma, que utiliza al menos un dato, llamado clave de cálculo.

Según una peculiaridad, la clave de cálculo se calcula a partir de un dato, llamado clave de base, memorizado en el objeto informatizado.

Según una peculiaridad, en el objeto informatizado se memorizan varios datos, llamados claves múltiples de base, incluyendo el procedimiento una etapa de introducción de un dato que representa, de entre esas claves múltiples de base, el dato que ha de utilizarse como clave de base.

Según una peculiaridad, el procedimiento incluye una etapa de personalización del objeto informatizado mediante introducción de al menos un dato, llamado dato individual, siendo utilizado este dato individual por el objeto informatizado en combinación con la clave de base para calcular un dato, llamado clave hija, que se utilizará como clave de cálculo.

Según una peculiaridad, el procedimiento incluye una etapa de introducción y memorización en el objeto informatizado de al menos un dato, llamado parámetro suplementario, cuyo parámetro suplementario es combinado por el algoritmo de firma con la clave de cálculo y los datos de señal para calcular la firma.

Según una peculiaridad, el procedimiento incluye una etapa que utiliza un algoritmo, llamado algoritmo complementario, que realiza la extracción del dato individual que se ha utilizado para generar una firma, llamada firma individualizada, comparando esta firma individualizada con una firma, llamada firma de base, que ha sido generada combinando los mismos datos salvo dicho dato individual.

Es otra finalidad proponer un procedimiento de autenticación de un parque de objetos informatizados dotados de capacidades de tratamiento de datos o de control de su validez.

Esta finalidad se consigue mediante un procedimiento de autenticación de uno o varios objetos, o de su validez, perteneciendo estos objetos a un parque de objetos que, distribuidos a unos usuarios, ponen en práctica un procedimiento tal y como se ha descrito anteriormente, caracterizado porque incluye las siguientes etapas:

- activación en una estación de tratamiento de datos, llamada estación de control, de un algoritmo de control que reproduce los resultados del algoritmo de firma memorizado en los objetos que han de autenticarse;

- eventual memorización, en la estación de control, de un dato que representa la clave de base memorizada en los objetos que han de autenticarse, o aquella de las claves múltiples de base que debe ser utilizada como clave de base;

- eventual memorización, en la estación de control, de al menos un dato que representa los parámetros suplementarios que deben ser memorizados en los objetos que han de autenticarse;

- para cada objeto que ha de autenticarse que utiliza un dato individual, lectura o recepción, procedente del objeto, de un dato que representa el dato individual y memorización de este dato individual en la estación de control;

- cálculo, por parte de la estación de control, con ayuda del algoritmo de control, de un dato, llamado firma de control, en función de los datos eventualmente memorizados en lo anterior;

- lectura o recepción de la firma calculada por un objeto que ha de autenticarse y verificación de esta misma firma con relación a la última firma de control obtenida por la estación de control, o con una firma de control anterior.

Según una peculiaridad, el dato individual memorizado en el objeto informatizado tan sólo puede modificarse en unas condiciones determinadas, incluyendo además el procedimiento las siguientes etapas:

- cálculo por parte del objeto informatizado y transmisión al terminal de una firma de base sin utilización del dato individual;

- cálculo por parte del objeto informatizado y transmisión al terminal de una firma individualizada con utilización del dato individual;

- presentación de estas firmas, o transmisión de estas firmas al terminal, con fines de verificación con relación a al menos un dato calculado por otro aparato a partir de la misma señal digital o analógica, pudiendo llevarse a cabo esta verificación en el terminal o fuera del mismo.

Según una peculiaridad, la estación de control incluye un algoritmo complementario, incluyendo además el procedimiento las siguientes etapas:

- memorización en la estación de control de una firma individualizada proporcionada por el objeto informatizado;

- extracción en la estación de control, mediante el algoritmo complementario, del dato individual utilizado por el objeto informatizado para generar la firma individualizada, con fines de comparación con una identificación proporcionada o exhibida por el usuario, o el objeto informatizado, o el terminal, o un dispositivo o lugar que incluye o utiliza este objeto informatizado.

Es otra finalidad proponer un objeto informatizado que permite poner en práctica uno de los procedimientos anteriormente descritos.

Es otra finalidad proponer un procedimiento de control de un parque de objetos informatizados de descuento de crédito de tiempo cuya autenticidad y validez se pueden controlar fácilmente, por ejemplo mediante lectura óptica.

Esta finalidad se consigue mediante un procedimiento de control de un parque de objetos de descuento de crédito de tiempo, caracterizado porque utiliza objetos informatizados que ponen en práctica un procedimiento según una de las anteriores reivindicaciones, memorizando, por una parte, estos objetos informatizados un dato de saldo, que representa un valor de crédito de tiempo disponible, y un programa que incluye un algoritmo de descuento apto para modificar ese dato de saldo y, por otra, incluyendo estos un dato de validez que presenta un estado determinado cuando está activado el algoritmo de descuento y el dato de saldo representa un crédito de tiempo no nulo, llevándose a cabo esa modificación del dato de saldo en función de una o varias duraciones de activación del objeto; incluyendo este procedimiento las siguientes etapas:

- distribución de tales objetos informatizados a unos usuarios;

- autenticación y control de la validez de uno o varios de estos objetos informatizados, con ayuda de una estación de control según una de las anteriores reivindicaciones, siendo estos objetos informatizados exhibidos por los usuarios o accesibles a efectos de control.

Según una peculiaridad, la modificación del dato de saldo se lleva a cabo asimismo en función de datos que representan un dato individual, un parámetro suplementario, una elección de clave de base o una combinación de estos elementos.

Es otra finalidad proponer un sistema que pone en práctica uno de los procedimientos anteriormente descritos para controlar un parque de objetos informatizados de descuento de crédito de tiempo o de otro tipo.

Es otra finalidad de la invención proponer un procedimiento que permite controlar la utilización de un dispositivo, sistema o soporte lógico, verificando que el usuario realmente dispone de un objeto informatizado determinado que sea auténtico, válido, esté activado o que funcione según unos parámetros determinados.

Esta finalidad se consigue mediante un procedimiento de control de utilización de un dispositivo o de un sistema que incluye o utiliza un programa informático, llamado aplicación protegida, caracterizado porque al menos una parte de la aplicación protegida se ejecuta en un objeto informatizado que pone en práctica un procedimiento según una de las anteriores reivindicaciones, o utiliza un programa ejecutado en ese mismo objeto informatizado, efectuándose el cálculo de la firma o su presentación por parte del objeto informatizado o su transmisión al terminal tan sólo si la aplicación protegida está activa.

Es otra finalidad proponer un sistema que pone en práctica el procedimiento anteriormente descrito para controlar la utilización de un dispositivo, sistema o soporte lógico.

Es otra finalidad realizar el control de un parque de objetos informatizados de descuento de valor de estacionamiento.

Esta finalidad se consigue mediante la utilización de un procedimiento tal como se ha descrito anteriormente para controlar títulos de derecho de estacionamiento de vehículos, caracterizado porque los objetos informatizados son tarjetas inteligentes, prepago o de crédito, con un dato de saldo que representa un valor de tiempo de estacionamiento.

Según una peculiaridad, al menos un parámetro suplementario corresponde a una zona geográfica de estacionamiento o a un tipo de tarificación o una combinación de ambos.

Según una peculiaridad, al menos un dato individual corresponde a un dato identificador del objeto informatizado o a un dato identificador de un vehículo o de un usuario o de una cuenta de usuario, o de una combinación de estos elementos.

La invención, con sus características y ventajas, se pondrá más claramente de manifiesto con la lectura de la descripción que se hace con referencia a los dibujos que se acompañan, en los que:

la figura 1 representa un esquema simbólico de puesta en práctica de un procedimiento según la invención en una forma de realización que realiza la autenticación de un parque de tarjetas inteligentes de descuento de tiempo que funciona con una clave de base única y permanente;

la figura 2 representa un esquema simbólico de puesta en práctica de un procedimiento según la invención en una forma de realización que realiza la autenticación de un parque de tarjetas inteligentes de descuento de tiempo según una variante que integra parámetros suplementarios que pueden corresponder a varios tipos de uso de una misma tarjeta;

la figura 3 representa un esquema simbólico de puesta en práctica de un procedimiento según la invención en una forma de realización que realiza la autenticación de un parque de tarjetas inteligentes de descuento de tiempo según una variante que integra parámetros suplementarios que pueden corresponder a varios tipos de uso de una misma tarjeta, pudiendo ser personalizada cada tarjeta por el usuario antes del uso;

la figura 4 representa un esquema simbólico de puesta en práctica de un procedimiento según la invención en una forma de realización que realiza la autenticación de un parque de tarjetas inteligentes de descuento de tiempo según una variante que integra parámetros suplementarios que pueden corresponder a varios tipos de uso de una misma tarjeta, pudiendo ser personalizada cada tarjeta por el usuario antes del uso, pudiendo ser controlada esta personalización con independencia de la validez.

En la presente descripción, la invención quedará ilustrada principalmente en unas formas de realización que utilizan objetos informatizados constituidos a partir de o que comprenden una tarjeta inteligente («smart card» en inglés), en una cualquiera de las versiones y entornos de funcionamiento disponibles para este tipo de objeto informatizado. Tal

tarjeta inteligente comprende así al menos un procesador, unos medios de memorización y unos medios de comunicación con un aparato exterior, que recibe por ejemplo el nombre de terminal o lector de tarjetas.

Tal tarjeta inteligente se presta especialmente bien a un gran número de aplicaciones debido a sus reducidos coste y ocupación de espacio, entre otros factores, debido a que su funcionamiento es, en cierto modo, pasivo. Es decir, que tan sólo funciona con la energía de un terminal y cuando se enlaza con éste. Entre dos conexiones, ésta se halla en estado de funcionamiento «detenido». Este aspecto pasivo y su ausencia de consumo energético suponen no obstante un cierto número de restricciones, que la invención permite soslayar en cierto número de aplicaciones.

No obstante, pueden utilizar ventajosamente la presente invención objetos informatizados, portátiles o no, que presentan ciertas características o restricciones distintas de la tarjeta inteligente tradicional, por ejemplo por motivos de autonomía, de sencillez de puesta en práctica, de coste de puesta en práctica. Puede tratarse, por ejemplo, de encapsulados que incorporan asimismo medios más o menos austeros de presentación o de introducción, de módulos que integran la puesta en práctica de la invención junto con otras funciones, en variadas configuraciones físicas y electrónicas.

Por lo tanto, debe comprenderse perfectamente que el o los objetos que incluyen capacidades de tratamiento de datos designados en la presente descripción como objetos informatizados pueden presentar configuraciones muy diferentes de la tarjeta inteligente ilustrada en el presente documento, sin salir de la esencialidad de la invención. Puede tratarse especialmente de objetos que son solidarios físicamente de objetos o dispositivos de consideración o voluminosos o incorporados a tales dispositivos. Tales objetos pueden, por ejemplo, no ser portátiles, pero beneficiarse de una notable autonomía de funcionamiento con relación al dispositivo al que se añaden, y realizan, a instancias del mismo, tareas completas y con unos recursos cuya escasa amplitud les podría permitir estar realizados en una forma portátil.

En este sentido, hay que considerar que los objetos informatizados a los que se aplica la presente descripción incluyen dispositivos de tratamiento de datos de escasas capacidades tales como los designados de ordinario con el término de «informática embarcada», utilizado en muchas ocasiones para traducir el término inglés «embedded computer», es decir «ordenador empotrado», o «incorporado».

Tal presentación de la amplitud de los dispositivos que pertenecen a la informática embarcada se puede encontrar, por ejemplo, en la obra «Java embarqué» (Eyrolles - París, 1999).

De acuerdo con las aplicaciones, la invención podrá ser utilizada en una forma de realización que presente diferentes repartos de las funciones que a continuación se describen, en uno o varios objetos separados o separables.

Estas funcionalidades se podrán repartir especialmente según las siguientes configuraciones, las cuales se describirán de manera más completa en lo sucesivo:

«Módulo completo»: cada objeto informatizado comprende a la vez los algoritmos y datos necesarios, y medios de interfaz con el exterior.

«Objeto informatizado completo y pasivo»: cada objeto informatizado comprende los algoritmos y datos necesarios, así como medios de cálculo y de memorización. Tales objetos son utilizados con un terminal que comprende medios de interfaz con el exterior.

«Objeto informatizado múltiple»: cada objeto informatizado se compone de varios objetos cada uno de los cuales no comprende más que una parte de los algoritmos y datos necesarios. Uno o varios de estos objetos comprenden la totalidad o parte de los medios de interfaz con el exterior.

En el caso de un objeto informatizado «pasivo», para poder ser activado y utilizado, tal objeto debe estar conectado a un aparato o terminal que dispone de medios de interfaz con el usuario. El objeto informatizado, entonces, tan sólo puede comunicarse de manera puramente electrónica con el exterior, con ese terminal. Esta comunicación se lleva a cabo por ejemplo según un protocolo tal como el formato «APDU» para el caso de una tarjeta inteligente que es acorde con a la norma ISO 7816.

La segregación de las tareas entre el terminal y la tarjeta inteligente hace que las funciones específicas de una utilización y las funciones de seguridad que lleva aparejadas sean memorizadas y tratadas por completo en el interior de la tarjeta, actuando el terminal únicamente de intermediario. Debido al escaso coste de la tarjeta en sí misma, son posibles numerosas aplicaciones que dependen directamente de la tarjeta, siendo ésta el elemento seguro y conteniendo ella el valor de uso de la aplicación. El terminal no es entonces más que una herramienta intercambiable y las aplicaciones concebibles pueden incluir entonces importantes cantidades de tarjetas inteligentes a un tiempo seguras y a costes reducidos, de la misma manera que para las tarjetas telefónicas, las diversas tarjetas bancarias o toda clase de tarjetas de fidelidad u otras.

Para obtener la generación de datos imprevisibles para el usuario de una tarjeta inteligente, es posible utilizar un algoritmo, llamado algoritmo de firma, que incluye un algoritmo pseudoaleatorio, proporcionándole un dato semilla.

En concreto, para aplicaciones que incluyen un importante número de tarjetas producidas, es importante proporcionar a este algoritmo de firma un dato semilla que sea siempre diferente. En efecto, si es posible proporcionar un dato semilla que sea el mismo en varias utilizaciones, entonces es posible obtener valores que igualmente sean los mismos para los datos pseudoaleatorios que se derivarán.

Para proporcionar un dato semilla que sea constantemente diferente, la invención propone utilizar un terminal, denominado terminal en el presente documento, que incluye la capacidad de recibir una señal exterior, por ejemplo una señal radiodifundida. La tecnología de recepción de una onda de radio, es decir, electromagnética, por ejemplo las señales de transmisores radiofónicos, proporciona a día de hoy soluciones de recepción a un tiempo económicas y poco voluminosas.

Para las aplicaciones que utilizan objetos informatizados «completos y pasivos», la invención propone entonces un procedimiento que incluye la recepción de una onda de radio por un terminal conectado a una tarjeta inteligente. El terminal comprende medios de recepción de radio de un tipo conocido, que le permiten recibir una señal de radio, bien sea en una forma digital o bien en una forma analógica según las variantes de la invención. La señal recibida se interpreta entonces a través de un módulo de interpretación que puede comprender un convertidor analógico-digital.

Un tipo utilizado de señal de radio puede ser recibido ventajosamente según la tecnología de recepción de una onda «subportadora», tal como la utilizada para la transmisión a los receptores FM (Modulación de Frecuencia) de informaciones suplementarias según la norma «RDS», por ejemplo el nombre de la estación radiofónica captada o el título de una música difundida. Esta tecnología subportadora puede ser utilizada asimismo en modo ondas largas o AM (Modulación de Amplitud) con la ventaja de un mayor alcance de recepción, hasta 2000 km para un importante transmisor de radiodifusión pública.

La señal de radio utilizada puede ser no obstante cualquier categoría de onda electromagnética sin salir de la esencialidad de la invención, por ejemplo una señal de televisión de origen hertziano o de satélite, o una señal emitida por cualquier satélite tal como un satélite de posicionamiento GPS.

En una forma de realización, el módulo de interpretación del terminal extrae uno o varios datos digitales que a continuación se transmiten a la tarjeta para servir de dato semilla en un algoritmo de generación de datos pseudoaleatorios.

En una forma de realización de la invención, tales datos pseudoaleatorios son utilizados por un programa en el seno de la tarjeta para poner en práctica un juego de azar, que eventualmente incluye unos premios. Por ejemplo, se venden tarjetas de manera similar a boletos de juegos de rascar y el aspecto aleatorio obtenido mediante la provisión de un dato semilla externo permite afirmar sin engaño que todas las tarjetas tienen en efecto la misma oportunidad de ganar. La seguridad del proceso frente al fraude puede quedar asegurada entonces por unos medios conocidos de protección de seguridad de los datos contenidos en una tarjeta inteligente. En otra fase, la validación de una tarjeta ganadora puede comprender por ejemplo una autenticación de la tarjeta mediante comparación de una firma obtenida proporcionando un nuevo dato semilla a esa misma tarjeta. Esta firma debe ser entonces idéntica a una firma de control obtenida, a partir de ese mismo dato semilla, por una estación de control que utiliza un algoritmo idéntico o equivalente.

En una forma de realización que permite un juego con varios jugadores, la invención comprende la difusión de un cierto número de tarjetas a diferentes jugadores. Utilizando una señal que cubre una zona geográfica de una extensión determinada, es posible entonces, para todas las tarjetas que se encuentran dentro de esa zona, generar datos a la vez aleatorios y que sean los mismos en cada una de esas tarjetas.

Una forma de realización comprende entonces una lotería que utiliza un número de serie propio de cada tarjeta para obtener una o varias tarjetas ganadoras generando uno o varios números en el mismo momento en todas las tarjetas activas en ese momento.

Otra forma de realización comprende la selección para cada tarjeta, por mediación de los medios de interfaz de cualquier terminal, de una serie de números en los que apostar. Se puede realizar entonces un sorteo aleatorio en un momento dado, el cual dará unos números ganadores comunes para todas las tarjetas activadas. Las tarjetas que tengan memorizados unos números apostados correspondientes a los números resultantes del sorteo se pueden reconocer entonces como ganadoras y proporcionar un cálculo o una validación de los premios.

Numerosas aplicaciones pueden precisar de elementos aleatorios que sean comunes para varios usuarios.

En una forma de realización, un programa de realidad virtual o de simulación, lúdico o de entrenamiento, determina unas condiciones aleatorias de funcionamiento. Estas condiciones, por ejemplo de meteorología o de resultados de combates, son entonces imposibles de prever o de falsificar para los participantes en la aplicación.

En esta configuración que utiliza un «objeto informatizado completo y pasivo», el terminal puede presentar formas variadas, que interfieran poco o nada en el modo de funcionamiento y la seguridad del procedimiento. Semejante terminal puede ir integrado por ejemplo en un radioteléfono portátil, en un reproductor portátil de grabaciones

sonoras, en un televisor, en una terminal interactiva, en un ordenador portátil o de sobremesa, o enlazado con tal aparato.

En una forma de realización representada en las figuras 1 a 4, la invención propone un procedimiento y un sistema que realizan el control de un parque de objetos informatizados, tales como tarjetas inteligentes (1). En el ejemplo que se presenta, las tarjetas inteligentes son utilizadas para descontar un crédito de tiempo. En determinadas variantes, este tiempo puede corresponder a valores diferentes, mediante ponderación en función de parámetros suplementarios modificables para cada utilización.

En una utilización de la invención, estos objetos informatizados comprenden tarjetas inteligentes, por ejemplo prepago o recargables, que memorizan un saldo que representa un valor de tiempo de estacionamiento de vehículo. En una variante, este saldo se puede pagar de otras diversas maneras, por ejemplo siendo cargado a una cuenta de usuario para ulterior pago, o facturado después de un consumo o de manera periódica.

En un estadio llamado de distribución, se fabrican o personalizan o parametrizan un cierto número de tarjetas inteligentes de manera que memoricen una aplicación que gestiona la puesta en práctica del procedimiento. Esta aplicación comprende un programa, llamado programa de control (10), que utiliza un algoritmo de firma (11) apto para efectuar el cálculo de una firma (13) a partir de un dato que representa una clave, llamada clave de cálculo, y de unos datos semilla que pueden ser recibidos ulteriormente. Esta aplicación comprende asimismo unas funcionalidades que permiten activar un descuento de tiempo, descuento este que provoca la variación de una duración o de un valor de crédito de tiempo, memorizado en un dato llamado dato de saldo (17). Estas tarjetas se distribuyen entonces a unos usuarios de un servicio proporcionado por uno o varios proveedores de servicios.

Según las variantes, el algoritmo de firma (11) puede incluir un algoritmo que efectúa por ejemplo una codificación o cifrado simétrico, o de clave secreta, o una codificación o cifrado asimétrico, o de clave pública y clave privada.

Según las variantes, todas las tarjetas pueden tener memorizada una misma clave de base (12), o un juego de diferentes claves de base llamadas múltiples que permiten un ulterior cambio de la clave de base (12) que habrá de utilizarse sin reactualización de las tarjetas ya distribuidas.

En una utilización típica, la o las claves de base pueden variar según el proveedor de servicio que emite o distribuye esas tarjetas. Estas claves de base pueden variar asimismo según el fabricante de la tarjeta o el prestador de personalización. Por supuesto, estas claves de base pueden variar según el tipo de servicio que ha de descontarse, o una categoría dentro de un mismo tipo de servicio. La tarjeta puede llevar inscrita o codificada de manera legible una información, llamada código de clave, identificadora de la clave de base o del juego de claves de base memorizado en esa tarjeta. Tal información permite entonces a un agente de control parametrizar una estación de control (14) introduciendo ese código de clave. Si el valor de la o las claves de base correspondiente a ese código ya está memorizado en la estación de control, la introducción de ese código de clave permite entonces a la estación de control utilizar como clave de cálculo la misma clave de base que la tarjeta del usuario, sin que ni el usuario ni el agente de control conozcan el valor de ninguna de estas claves. La elección de la clave de base o de las claves de base que se utilizarán puede quedar definida asimismo mediante un código de clave contenido en los datos de señal extraídos de la señal.

En una utilización de control de estacionamiento, se venden tarjetas prepago o recargables, por ejemplo a los automovilistas, que contienen un dato de saldo que representa, bien sea una duración, o bien una cuantía monetaria.

En una forma de realización representada más en particular en la figura 1, la invención utiliza una única y misma clave de base como clave de cálculo para un conjunto de tarjetas distribuidas.

En una fase de activación, el usuario del servicio activa su tarjeta (1) insertándola en un terminal (2) que incluye medios de comunicación (21) con esa tarjeta, por ejemplo mediante conexión eléctrica o mediante antena de radio de corto alcance. Este terminal incluye asimismo unos medios de presentación (22), por ejemplo una pantalla de cristal líquido, unos medios de alimentación de energía y unos medios de recepción radio (23) de un tipo conocido. Estos medios de recepción le permiten recibir una señal de radio (3), por ejemplo mediante decodificación de una onda subportadora emitida por un transmisor radiofónico de amplitud modulada. El terminal incluye asimismo un módulo de interpretación (24) apto para generar datos digitales llamados datos de señal (32) a partir de la señal (3) recibida por los medios de recepción (23).

En una fase de funcionamiento, el usuario deja la tarjeta (1) en el terminal (2) todo el tiempo que desee activar el descuento de tiempo, por ejemplo como pago del servicio, o como medio de control de una duración máxima de utilización de ese servicio. Durante toda esta fase de funcionamiento, el terminal recibe la señal de radio (3) e interpreta esta señal para extraer de ella unos datos de señal (32). Por lo tanto, estos datos de señal son generados mientras el terminal se encuentre dentro de la zona cubierta por la difusión de esa señal con una calidad suficiente para que la interpretación digital de esa señal pueda llevarse a cabo de manera no ambigua.

La señal utilizada puede estar basada por ejemplo en la recepción de una señal indicativa de la hora universal, por

ejemplo la emitida por el transmisor de Fráncfort. La utilización de una señal no previsible permite no obstante disminuir todavía más los riesgos de fraudes. En efecto, para un estafador es más difícil prever las firmas que deben ser generadas en un momento futuro si no dispone de la naturaleza de la señal que será difundida en el momento en cuestión.

De manera ventajosa, el módulo de interpretación (23) extrae los datos digitales a partir de una onda subportadora de manera conocida, por ejemplo según la tecnología RDS utilizada para transmitir el nombre de determinadas estaciones radiofónicas.

En una variante en la que la señal utilizada no incluye información prevista específicamente para este uso, esta señal se interpreta siguiendo un período de muestreo determinado. Los datos de señal (32) son calculados entonces estableciendo una media de determinadas características de la señal a lo largo de ese período de muestreo. Estas características se escogen de manera que su interpretación dependa poco o nada de la potencia de recepción de la señal, de manera que los datos de señal extraídos sean independientes de la ubicación del terminal (2).

A partir de una señal analógica, es posible por ejemplo interpretar determinadas características de la señal poco dependientes de la calidad de recepción, por ejemplo una función de los tiempos de silencio en el seno de los sonidos radiodifundidos. El valor de la función obtenida se puede comparar entonces con una lista predeterminada de márgenes de valores para obtener un dato digital no ambiguo en el tiempo y constante de una ubicación de recepción a otra.

En el transcurso de la fase de funcionamiento, es decir, mientras la tarjeta (1) esté activada, un programa (16), llamado programa protegido, memorizado en esa tarjeta, efectúa el descuento del tiempo que transcurre y modifica el dato de saldo (17) en función de este descuento. Cuando se agota el crédito de tiempo, el programa (16) modifica el estado de un dato llamado dato de validez (18), o eventualmente interrumpe su propio funcionamiento. El programa puede prever otros casos en los que se modifica el dato de validez, por ejemplo en caso de error o de intento de fraude. El dato de validez puede comprender asimismo información relativa a la cantidad o a la cuantía de crédito de tiempo restante, o a los motivos por los que deja de ser válido el funcionamiento. Este dato de validez puede memorizar asimismo el tiempo transcurrido desde el momento en que el funcionamiento deja de ser válido. En caso de invalidez, esta información de invalidez puede ser transmitida al terminal (2) con fines de presentación o transmisión a otro aparato.

De manera reiterada a todo lo largo de la fase de funcionamiento, la tarjeta (1) recibe nuevos datos de señal (32). Combinando estos datos de señal con una clave de cálculo, por ejemplo la clave de base (12), el algoritmo de firma (11) del programa de control (10) calcula la firma (13). Esta firma se transmite al terminal (2), el cual la presenta en sus medios de presentación (22). Este cálculo de la firma, o su transmisión al terminal, tan sólo se lleva a cabo mientras esté activo el programa protegido (16), o el dato de validez (18) indique que se autoriza el funcionamiento y, especialmente, no se haya sobrepasado el crédito-tiempo concedido.

Se comprende perfectamente que, así, todas las tarjetas activadas y válidas dentro de una zona cubierta por una misma señal (3) van a generar firmas que serán todas ellas idénticas entre sí, a la vez que varían con el paso del tiempo de manera imprevisible sin el conocimiento del algoritmo de firma ni de la clave de cálculo, en su caso la clave de base (12) o una de las claves múltiples de base.

Cuando la señal incluye una característica regular que permite una sincronización de los períodos de muestreo o de cálculo de la firma, es posible para cada tarjeta efectuar su cambio de firma en el mismo instante. Si para calcular la firma es necesario un período completo, una tarjeta recién activada podrá presentar entonces una firma determinada, o firma de inicio, en espera del próximo período completo. El conjunto de las tarjetas de la zona podrán cambiar entonces de firma en el mismo instante.

Cuando la señal no incluye características de sincronización, tarjetas diferentes podrán efectuar su cambio de firma en momentos diferentes, la mayoría de las veces espaciados en menos de un período de cambio de firma.

En una variante (no representada), el terminal o la tarjeta recibe asimismo una segunda señal indicativa de la hora universal y utiliza esa segunda señal para sincronizar los períodos de cálculo de sus datos de señal o de su firma.

Para realizar un control de las tarjetas de crédito de tiempo del parque en una zona cubierta por la señal, un operador humano o automático, llamado agente de control, que opera por cuenta del proveedor de servicio, puede utilizar entonces una estación de control (4) apta para generar los mismos datos de señal (324) que una tarjeta (1) que recibe esa misma señal (3). Esta estación de control memoriza un programa que utiliza un algoritmo (41) capaz de obtener, cuando dispone de los mismos elementos, los mismos resultados que el propio de las tarjetas que han de controlarse.

Al hallarse ajustada a la misma señal (3) y al utilizar la misma clave de base (12) que las tarjetas que han de controlarse, la estación de control podrá presentar por lo tanto una firma de control (43) idéntica a la firma (13) de las tarjetas que han de controlarse. En las variantes en las que las tarjetas efectúan su cambio de firma de manera no síncrona, la estación de control puede memorizar las firmas anteriores y presentar varias firmas al mismo tiempo, por

ejemplo todas las firmas con validez vigente en un momento dado.

Al comparar la firma (13) presentada por una tarjeta (1) controlada con la firma de control (43) presentada por la estación de control (4), el agente de control puede saber entonces si esa tarjeta contiene realmente un algoritmo de firma (11) y una clave de cálculo válida y si su funcionamiento está activado correctamente. Así, el agente de control tiene la posibilidad de saber si el usuario cumple unos requisitos de control, que pueden ser presentados en el mismo lugar o conocidos de otra manera, y tomar medidas en consecuencia.

Según las aplicaciones, el terminal puede ser propio de cada usuario, de cada tarjeta, ser prestado al usuario o venir integrado en un aparato que cumple otras funciones similares o no.

En una utilización en control de estacionamiento, los conductores de vehículo que deseen estacionar pueden utilizar así un terminal ubicado de manera visible dentro de su vehículo para acreditar la compra de una tarjeta de estacionamiento y probar que ésta está activada el tiempo que dure el estacionamiento. Un agente de control puede ser entonces una persona equipada con una estación de control que verifica ante cada vehículo que la tarjeta está activada y válida, mediante comparación de la firma de la tarjeta con la firma de control.

En una variante, el cálculo de la firma o su transmisión tan sólo se efectúa bajo petición del agente de control, mediante disparo de un comando. Este disparo puede llevarse a cabo, por ejemplo, pulsando un botón en el terminal, o enviando un comando al terminal desde la estación de control, por ejemplo por vía eléctrica, o radio, o magnética, mediante un transpondedor magnético o exhibiendo una pieza metálica en la proximidad de sensores magnéticos enlazados con el terminal.

En una variante, la firma es comunicada o transmitida directamente a la estación de control por medios conocidos.

En otra variante, la firma es presentada en una forma legible de manera automática por la estación de control, por ejemplo mediante lectura de códigos de barras. La estación de control dispone entonces de medios de lectura automatizada que le permiten leer automáticamente la firma presentada por el terminal, por ejemplo en forma de códigos de barras. Estos medios de lectura automatizada también pueden estar previstos para leer automáticamente otras informaciones inscritas o presentadas en la tarjeta o en el terminal, como por ejemplo datos individuales o parámetros suplementarios según se describen posteriormente.

En una forma de realización representada más en particular en la figura 2, la invención permite al usuario de la tarjeta (1) utilizar unos parámetros suplementarios (14) que condicionan el modo de funcionamiento de esta tarjeta una vez activada. Estos parámetros suplementarios pueden ser introducidos o modificados por el usuario, por ejemplo en cada activación. Esta introducción o modificación puede llevarse a cabo, por ejemplo, con ayuda del terminal (2), el cual incluye entonces unos medios de introducción (25). Estos parámetros pueden repercutir por ejemplo en la velocidad de descuento del crédito de tiempo o en el valor de una unidad de tiempo. Estos parámetros suplementarios (14) pueden comprender asimismo una información identificadora del servicio o del proveedor de servicio para el cual se utiliza la tarjeta (1), o de la zona de utilización, o de la señal (3) a la cual está ajustada, o de un modo de recepción de dicha señal.

En la fase de funcionamiento, la tarjeta calcula la firma (13) que ha de presentarse combinando estos parámetros suplementarios (14) con los datos de señal (32) y la clave de cálculo, en su caso la clave de base (12) o una de las claves múltiples de base.

Para el control, el agente de control memoriza estos parámetros suplementarios (14) en la estación de control (4), por ejemplo mediante unos medios de introducción (45). Esta estación de control utiliza entonces esos parámetros suplementarios (14) para calcular y presentar la firma de control. En una variante, esos parámetros se hallan previamente programados en la estación de control y se activan mediante unos medios de selección, como por ejemplo mediante acción sobre una tecla o un cursor.

Se comprende perfectamente que, al introducir estos parámetros suplementarios (14), el usuario efectúa una parametrización del funcionamiento de la tarjeta. Al ser tomados en cuenta estos parámetros en el cálculo de la firma (13), esta firma tan sólo concordará con la firma de control (43) si los parámetros suplementarios memorizados en la tarjeta (1) son acordes con los memorizados en la estación de control (4). Así, cuando el modo de funcionamiento obtenido mediante estos parámetros suplementarios es una condición de utilización del servicio que motiva el control, la invención permite controlar que el usuario exhibe realmente una tarjeta auténtica, válida, activada y que funciona según los parámetros correctos.

En una utilización en control de estacionamiento, esos parámetros suplementarios podrán ser conocidos por el usuario o presentados en el lugar de estacionamiento. Puede tratarse de introducir una información condicionante del coste del estacionamiento o del tiempo máximo permitido de estacionamiento. Esta indicación puede corresponder a una zona geográfica o tarifaria, a un tipo de vehículo o de estacionamiento, a un nivel de servicio que incluye por ejemplo la vigilancia. Esos parámetros son introducidos entonces por el agente de control cada vez que cambia de tipo de zona o servicio que ha de controlar.

En una forma de realización representada más en particular en las figuras 3 y 4, la invención permite al usuario de la tarjeta (1) utilizar datos individuales (15) que son propios de su configuración de utilización, por ejemplo de su persona, de su tarjeta o su terminal, o de una cuenta de usuario.

En el caso de una personalización después de la distribución (figura 4), estos datos individuales (15) son introducidos y memorizados en la tarjeta (1), por ejemplo por el usuario, con ayuda del terminal (2) o con ayuda de una terminal de distribución automatizada. En la tarjeta, estos datos individuales (15) se combinan con la o las claves de base (12) ya memorizadas para dar otra clave, llamada clave hija (121). Esta clave hija se memoriza en la tarjeta y será utilizada como clave de cálculo en el cálculo de la firma (13) en la fase de funcionamiento.

En una variante (no representada) en la que se efectúa una personalización antes de la distribución, estos datos individuales se combinan con una clave madre para dar otra clave, llamada clave hija, que se memoriza en la tarjeta. Esta personalización la puede llevar a cabo, por ejemplo, el proveedor de servicio o un distribuidor o una terminal de distribución automatizada. Según las aplicaciones, estos datos individuales pueden estar eventualmente memorizados en la tarjeta, inscritos en la tarjeta, o ambos.

En la forma de realización representada más en particular en la figura 3, la personalización se realiza en varios tiempos, a la vez antes de la distribución al usuario y después de esta distribución. Antes de la distribución, una clave madre (120), combinada con un dato de personalización (151), da entonces la clave de base (12), que será la única memorizada en la tarjeta distribuida. La clave madre se memoriza en la máquina de personalización (5) o en otra tarjeta (50) que sirve de clave en la personalización. De manera ventajosa, la clave madre (120) no se memoriza en la tarjeta (1) distribuida, lo cual limita los riesgos de difusión ilegítima de esta clave madre. Después de la distribución, esa clave de base (12) se puede combinar entonces con el dato individual (15) para dar la clave hija que será utilizada en el cálculo de la firma.

En una variante, los datos individuales (15) se memorizan en la tarjeta de manera que no puedan ser modificados por el usuario.

En una variante, los datos individuales (15) y los datos de personalización (151) tienen al menos una parte común, o son idénticos.

En una variante, estos datos individuales condicionan o modifican el funcionamiento del programa de descuento (16) de crédito de tiempo. Puede tratarse de efectuar este descuento a partir de una cuenta determinada, cuando la tarjeta incluye varias de estas. Puede tratarse de utilizar una tarifa o un modo de cálculo individualizado, o por categoría.

Para el control, el agente de control se informa de estos datos individuales (15) o de los datos de personalización (151) o de ambos, frente al usuario o mediante lectura en la tarjeta, el terminal o el aparato que los porta. En una variante, estos datos individuales o de personalización son transmitidos directamente del terminal a la estación de control, por medios conocidos. En otra variante, estos datos individuales o de personalización son presentados por el terminal y leídos automáticamente mediante unos medios de lectura de la estación de control, por ejemplo en forma de códigos de barras.

Se comprende perfectamente que la invención permite así efectuar un control individualizado. En el caso de una parametrización individualizada del funcionamiento del descuento de crédito de tiempo, la invención permite así controlar que el usuario realmente exhibe una tarjeta auténtica, válida, activada y que funciona según los parámetros correspondientes a su identidad o a su categoría. En el caso de una parametrización individualizada de una vez, la invención permite así controlar que el usuario realmente exhibe una tarjeta auténtica, válida, activada y personalizada de manera coherente con la identificación o la categoría que exhibe. Este aspecto permite especialmente disminuir los riesgos de utilización de una tarjeta robada.

En una variante representada más en particular en la figura 4, el programa de la estación de control comprende un algoritmo, llamado algoritmo complementario (410), apto para combinar la firma, firma individualizada (130), de una tarjeta que incluye datos individuales (15) con una firma (43) obtenida sin esos mismos datos individuales, combinación esta que da como resultado el valor de los datos individuales utilizados por la tarjeta. El terminal puede incluir entonces la presentación combinada de la firma individualizada (130), es decir, obtenida con esos datos individuales (15), y de la firma de base (13), es decir, obtenida sin esos mismos datos individuales.

En tal variante, la firma individualizada (130) de la tarjeta (1) puede, por ejemplo, ser presentada por el terminal (2) en una forma legible automáticamente, por ejemplo incluyendo un código de barras. El agente de control, cuando ha efectuado un primer control de la validez de la tarjeta, según se ha descrito anteriormente, puede efectuar entonces un segundo control que recae sobre los datos individuales (15) memorizados en esa tarjeta. En ese segundo control, la estación de control (4) lee la firma individualizada (130) mediante unos medios de lectura automatizada y la ingresa en el algoritmo complementario (410). Este algoritmo complementario combina esa firma individualizada con una firma de base, la propia (13) de la tarjeta o la suya (43) propia si son idénticas, y de ello extrae el valor de los datos individuales (15) utilizados por la tarjeta. El agente de control puede comparar entonces estos datos individuales con la identificación exhibida por el usuario para verificar que ese usuario utiliza esa tarjeta de manera

legítima.

En una variante (no representada), la estación de control combina la firma individualizada con una firma obtenida a partir de la clave madre (121; figura 3) para extraer el valor de los datos individuales (15) o de los datos de personalización (151) o de uno de los dos.

Se comprende que la invención permite así, a un tiempo, realizar un control no individualizado, que precisa poco o nada de introducción de datos para cada control de tarjeta, y tener la posibilidad de comparar, sin introducción suplementaria, unos datos individuales memorizados en la tarjeta con una identificación exhibida por el usuario. Así, es posible disminuir los riesgos de utilización ilegítima de una tarjeta, sin gravar seriamente el trabajo del agente de control.

En una utilización en control de estacionamiento, esos datos individuales pueden ser presentados o inscritos en el terminal, en la tarjeta o en el vehículo. Puede tratarse de introducir una información individual o por categoría condicionante del coste del estacionamiento o del tiempo máximo permitido de estacionamiento. Esta indicación puede corresponder a una zona geográfica o tarifaria, a un tipo de vehículo o de estacionamiento, a un nivel de servicio que incluye por ejemplo la vigilancia.

Esos datos son leídos entonces en el vehículo, la tarjeta o el terminal, e introducidos por el agente de control cada vez que controla un nuevo vehículo.

Esos datos individuales pueden representar asimismo el número de serie de la tarjeta o del terminal, o el número de matrícula del vehículo, o cualquier otra identificación visible en el estacionamiento. El hecho de depender de tal identificación la firma proporcionada por la tarjeta permite entonces que la tarjeta tan sólo sea utilizable con esa identificación.

En una variante del control de estacionamiento que utiliza un algoritmo complementario, el agente de control realiza un primer control, de validez de la tarjeta, mediante lectura de la firma de base en el terminal. Puede efectuar entonces un segundo control, para verificar que la tarjeta no es robada o que corresponde realmente al vehículo. Para ello, la estación de control lee automáticamente la firma individualizada en el terminal y extrae de ella los datos individuales utilizados por la tarjeta para generar esa misma firma individualizada. El agente de control puede comparar entonces con facilidad esos datos individuales extraídos por su estación de control con la identificación visible en el vehículo.

En una variante, el programa protegido (16) realiza un descuento de un crédito que representa unidades independientes que no dependen forzosamente del tiempo. Puede tratarse entonces de un número de unidades telefónicas descontadas como pago de un servicio, de un número de partidas de juego, o de cualquier tipo de unidades o de fichas.

En una forma de realización (no representada), la invención propone un procedimiento y un sistema que realizan el control de un parque de objetos informatizados, tales como tarjetas inteligentes, utilizados para autenticar a una persona o un dispositivo por medio de su posesión de tal objeto informatizado. Tal forma de realización puede ser utilizada igualmente para condicionar el funcionamiento de un dispositivo o de un soporte lógico informático. Es decir, que un sistema o soporte lógico o dispositivo que utiliza una aplicación, llamada aplicación protegida, tan sólo puede ser utilizado si el usuario dispone de tal objeto informatizado.

El procedimiento y el sistema tal y como se describen anteriormente se proponen entonces en una configuración en la que el programa memorizado en la tarjeta inteligente efectúa el cálculo y la transmisión solamente cuando otro programa, llamado aplicación protegida, funciona igualmente, aunque esta aplicación no incluya descuento de crédito de tiempo. Esta aplicación protegida se halla memorizada entonces, al menos en parte, en la tarjeta y puede incluir una función que gobierna la modificación del estado o del valor del dato de validez.

La invención puede permitir así limitar el acceso de un lugar o la utilización de un dispositivo o de un servicio sólo a las personas que disponen de una tarjeta inteligente distribuida por el proveedor de ese servicio o el titular de la explotación de ese lugar o dispositivo. Esta utilización puede entonces quedar condicionada igualmente a la presencia activada y controlable de tal tarjeta. Esta utilización puede además quedar condicionada a la activación de otro programa memorizado en esa tarjeta, por ejemplo por razones de seguridad. Puede tratarse, por ejemplo, de la utilización de una sala de billar, de un ordenador, de un automóvil o de un ingenio cualquiera. Puede tratarse asimismo de un lugar, dispositivo o sistema que precisa del funcionamiento de un soporte lógico específico para ser utilizado con total seguridad, tal como un soporte lógico de protección antivirus o un sistema de control de alcoholemia.

En el caso de un objeto informatizado «como módulo completo», el terminal y la tarjeta antes descritos van agrupados en un mismo módulo. Este objeto informatizado, o módulo, agrupa entonces los medios de recepción de la señal, los medios de interpretación de la señal, los medios de presentación o de transmisión de la o de las firmas, y los oportunos medios de introducción.

Tal módulo completo puede realizarse en forma de un objeto informatizado, portátil o no, o ir integrado en otro dispositivo o sistema.

Una utilización de tal módulo informatizado puede comprender, por ejemplo, el hecho, para una persona o un ordenador, de autenticarse frente a otro sistema que utiliza o incluye una estación de control. Esta autenticación puede llevarse a cabo comunicando en un momento dado la firma individualizada indicada por el módulo informatizado, incluso a través de los medios de comunicación que presentan pocas garantías de confidencialidad.

En el caso de un «objeto informatizado múltiple», una parte de los algoritmos y datos se memoriza en un objeto pasivo, otra parte se memoriza en el lector o terminal.

En una forma de realización de este tipo, representada en la figura 5, la invención incluye un objeto pasivo que comprende una tarjeta inteligente (1a) que cumple únicamente funcionalidades llamadas de «monedero electrónico», por ejemplo según el estándar «Moneo» (marca registrada). Esta tarjeta memoriza entonces un saldo (17), por ejemplo correspondiente a un valor monetario, e incluye algoritmos que le permiten recibir comandos de verificación (191) y de decremento (192) de ese saldo. Tal tarjeta (1a) puede ser así compatible con varios tipos de servicios al no incorporar más que funciones de gestión de un saldo monetario.

El programa de control (10) así como las funcionalidades de introducción de datos complementarios (114, 15) se memorizan y ejecutan entonces en el terminal (2a). En un control, el agente de control realiza entonces el control de validez y de actividad del terminal (2a).

En el caso de un control de crédito de tiempo, el terminal (2a) es el que incluye un programa de descuento de tiempo (16a) y de decremento del valor (1) memorizado en esa tarjeta (1a). Este programa de descuento de tiempo (16) es el que tan sólo autoriza el control o se mantiene activado mientras ese valor no sea nulo. En un control, lo que controla entonces el agente de control es la validez y la actividad del terminal.

Una utilización de tal objeto informatizado múltiple puede comprender, por ejemplo, el hecho, para una persona o un ordenador, de conectar una tarjeta (1a) monedero multiservicio a un terminal de identificación (2a) específico del servicio que exige un control.

En otra forma de realización según la configuración de «objeto informatizado múltiple», la invención incluye un terminal (2b) que se comunica, por una parte, con una tarjeta inteligente (1c) de monedero electrónico y, por otra, con un objeto informatizado pasivo (1b), llamado objeto de identificación.

Las funcionalidades de cálculo de firmas se memorizan y ejecutan entonces en el objeto de identificación (1b). La presentación o la transmisión de las firmas, la recepción y la interpretación de la señal, así como las introducciones de datos complementarios son realizadas por el terminal (2b). El programa de control (10) del objeto de identificación tan sólo devuelve la firma si está en funcionamiento un programa protegido (16b), memorizado igualmente en el objeto de identificación (1b), y le indica que el saldo (17a) de la tarjeta (1c) monedero es suficiente. Este programa (16b) puede realizar operaciones de verificación (191) y de decremento (192) de ese saldo (17b) comunicándose con esa tarjeta (1c) por intermedio del terminal (2b).

En el caso de un control de crédito de tiempo, el programa protegido (16b) del objeto de identificación es el que incluye un programa de descuento de tiempo y de decremento del valor memorizado en la tarjeta monedero, y tan sólo se mantiene activado mientras ese valor no sea nulo. En un control, el agente de control realiza entonces el control de autenticidad y de actividad del objeto de identificación y de validez del saldo de la tarjeta monedero.

Una utilización de tal objeto informatizado múltiple puede comprender, por ejemplo, el hecho, para una persona o un ordenador, de conectar una tarjeta monedero multiservicio a un terminal, juntamente con un objeto de identificación específico del servicio que exige un control.

La presente descripción expone la invención en unas formas de realización que incluyen un reparto determinado de las tareas y operaciones entre los diferentes algoritmos y programas implicados. La flexibilidad de la organización de una aplicación informática por supuesto permite presentar de otro modo este reparto, especialmente cuando las distinciones entre los diferentes algoritmos y sus denominaciones son nociones abstractas que no influyen en las características principales de su funcionamiento. Es evidente por tanto que el procedimiento según la invención se puede llevar a la práctica igualmente en otras formas de realización no descritas en el presente documento, sin salir de la esencialidad de la invención, especialmente combinando de otro modo las diversas variantes expuestas para cada variable o algoritmo. Asimismo, el reparto abstracto de las tareas entre programas o aplicaciones memorizados en un mismo lugar y tiempo se puede combinar en diversas variantes no descritas en el presente documento sin salir de la esencialidad de la invención.

Debe ser evidente para las personas peritas en la materia que la presente invención permite formas de realización en numerosas otras formas específicas sin apartarse del campo de aplicación de la invención según se reivindica. Consecuentemente, las presentes formas de realización deben ser tomadas a título de ilustración, pero pueden ser modificadas dentro del ámbito definido por el alcance de las reivindicaciones adjuntas, y la invención no debe quedar limitada a los detalles dados anteriormente.

REIVINDICACIONES

1. Utilización de al menos un objeto informatizado (1) para la generación de un dato pseudoaleatorio, incluyendo este objeto informatizado unos medios de tratamiento de datos, unos medios de memorización, así como unos medios de presentación o unos medios de comunicación con un dispositivo de tratamiento de datos, llamado terminal (2), caracterizada porque esta utilización para la generación del dato pseudoaleatorio incluye las siguientes etapas:

- recepción de al menos una señal (3) exterior, por parte del objeto informatizado (1) o por parte del terminal (2), señal (3) esta que varía con el paso del tiempo, que es difundida dentro de una zona determinada sin precisar de direccionamiento de la señal ni de información prevista específicamente para esta utilización;

- generación, por parte de un módulo de interpretación (24), de datos de señal (32), a partir de la señal (3) exterior recibida, para proporcionar un dato, llamado semilla, constantemente diferente;

- cálculo, por parte del objeto informatizado (1) con ayuda de un algoritmo memorizado en este objeto (1), del dato digital pseudoaleatorio, llamado firma (13), a partir de dicho dato semilla.

2. Utilización de un objeto informatizado (1) según la anterior reivindicación, caracterizada porque la señal (3) exterior es una señal de radio, es decir, que utiliza ondas electromagnéticas, emitida por un transmisor de difusión, incluyendo además el procedimiento las siguientes etapas:

- recepción de la señal de radio por parte del terminal (2);

- generación de los datos de señal (32), por parte del módulo de interpretación (24), a partir de esa señal de radio;

- transmisión de esos datos de señal (32) al objeto informatizado (1).

3. Utilización de un objeto informatizado (1) según una de las anteriores reivindicaciones, caracterizada porque la señal de radio representa información que incluye características irregulares o no previsibles.

4. Utilización de un objeto informatizado (1) según una de las anteriores reivindicaciones, caracterizada porque la señal de radio se recibe mediante la lectura de una onda subportadora, asociada a una difusión de ondas radiofónicas.

5. Utilización de un objeto informatizado (1) según una de las anteriores reivindicaciones, caracterizada porque la señal (3) incluye una pluralidad de períodos de tiempo determinados, siendo la información proporcionada por esta señal constante o interpretable de manera constante dentro de cada uno de estos períodos determinados, pero variando de manera irregular o no previsible de un período a otro.

6. Utilización de un objeto informatizado (1) para el control de un dato pseudoaleatorio generado por este objeto informatizado (1) que incluye unos medios de tratamiento de datos, unos medios de memorización, así como unos medios de presentación o unos medios de comunicación (21) con un dispositivo de tratamiento de datos llamado terminal (2), caracterizada porque esta utilización para el control del dato pseudoaleatorio incluye las siguientes etapas:

- generación de un dato pseudoaleatorio, llamado firma (13), mediante utilización de este objeto informatizado (1) según una de las anteriores reivindicaciones;

- presentación de esa firma (13), o transmisión de esa firma al terminal (2), con fines de verificación con relación a un dato (43) calculado por otro aparato (4), llamado estación de control, a partir de la misma señal (3) digital o analógica, pudiendo llevarse a cabo esta verificación en el terminal (2) o fuera del mismo.

7. Utilización de un objeto informatizado (1) según la anterior reivindicación, caracterizada porque incluye una etapa de comparación que verifica el valor de un dato, llamado dato de validez (18), memorizado en el objeto informatizado (1), verificación esta que condiciona o modifica el cálculo, la presentación o la transmisión de la firma (13).

8. Utilización de un objeto informatizado (1) según una de las reivindicaciones 6 a 7, caracterizada porque incluye una etapa de presentación, en unos medios de presentación (22) del terminal (2), de la firma (13) que el terminal recibe del objeto informatizado (1).

9. Utilización de un objeto informatizado (1) según una de las reivindicaciones 6 a 8, caracterizada porque la firma (13) es calculada por el objeto informatizado (1) mediante un algoritmo, llamado algoritmo de firma (11), que utiliza al menos un dato, llamado clave de cálculo.

10. Utilización de un objeto informatizado (1) según una de las reivindicaciones 6 a 9, caracterizada porque la clave de cálculo se calcula a partir de un dato, llamado clave de base (12), memorizado en el objeto informatizado

(1).

11. Utilización de un objeto informatizado (1) según una de las reivindicaciones 6 a 10, caracterizada porque en el objeto informatizado (1) se memorizan varios datos, llamados claves múltiples de base, incluyendo esta utilización una etapa de introducción de un dato que representa, de entre esas claves múltiples de base, el dato que ha de utilizarse como clave de base (12).

12. Utilización de un objeto informatizado (1) según una de las reivindicaciones 6 a 11, caracterizada porque incluye una etapa de personalización del objeto informatizado (1) mediante introducción de al menos un dato, llamado dato individual (15), siendo utilizado este dato individual por el objeto informatizado en combinación con la clave de base (12) para calcular un dato, llamado clave hija (121), que se utilizará como clave de cálculo.

13. Utilización de un objeto informatizado (1) según una de las reivindicaciones 6 a 12, caracterizada porque incluye una etapa de introducción y memorización en el objeto informatizado (1) de al menos un dato, llamado parámetro suplementario (14), cuyo parámetro suplementario es combinado por el algoritmo de firma (11) con la clave de cálculo (12, 121) y los datos de señal (32) para calcular la firma (13, 130).

14. Utilización de un objeto informatizado (1) según una de las reivindicaciones 6 a 13, caracterizada porque incluye una etapa que utiliza un algoritmo, llamado algoritmo complementario (410), que realiza la extracción del dato individual que se ha utilizado para generar una firma, llamada firma individualizada (130), comparando esta firma individualizada con una firma, llamada firma de base (13), que ha sido generada combinando los mismos datos salvo dicho dato individual (15).

15. Utilización de al menos un objeto informatizado (1) para la autenticación de uno o varios objetos (1), o de su validez, en virtud de una utilización de estos objetos informatizados (1) según una de las anteriores reivindicaciones, perteneciendo estos objetos (1) a un parque de objetos (1) distribuidos a unos usuarios, caracterizada porque esta utilización para la autenticación incluye las siguientes etapas:

- activación en una estación de tratamiento de datos, llamada estación de control (4), de un algoritmo de control (41) que reproduce los resultados del algoritmo de firma (11) memorizado en los objetos (1) que han de autenticarse;

- eventual memorización, en la estación de control, de un dato que representa la clave de base (12) memorizada en los objetos que han de autenticarse, o aquella de las claves múltiples de base que debe ser utilizada como clave de base;

- eventual memorización, en la estación de control, de al menos un dato que representa los parámetros suplementarios (14) que deben ser memorizados en los objetos (1) que han de autenticarse;

- para cada objeto que ha de autenticarse que utiliza un dato individual, lectura o recepción, procedente del objeto, de un dato (15) que representa el dato individual y memorización de este dato individual en la estación de control (4);

- cálculo, por parte de la estación de control (4), con ayuda del algoritmo de control (41), de un dato, llamado firma de control (43), en función de los datos eventualmente memorizados en lo anterior;

- lectura o recepción de la firma (13) calculada por un objeto (1) que ha de autenticarse y verificación de esta misma firma con relación a la última firma de control (43) obtenida por la estación de control (4), o con una firma de control anterior.

16. Utilización de al menos un objeto informatizado (1) según la anterior reivindicación, caracterizada porque el dato individual (15) memorizado en el objeto informatizado (1) tan sólo puede modificarse en unas condiciones determinadas, incluyendo además la utilización del objeto (1) para la autenticación las siguientes etapas:

- cálculo por parte del objeto informatizado (1) y transmisión al terminal (2) de una firma de base (13) sin utilización del dato individual (15);

- cálculo por parte del objeto informatizado y transmisión al terminal de una firma individualizada (130) con utilización del dato individual;

- presentación de esas firmas (13, 130), o transmisión de esas firmas al terminal (2), con fines de verificación con relación a al menos un dato (43) calculado por otro aparato (4), a partir de la misma señal (3) digital o analógica, pudiendo llevarse a cabo esta verificación en el terminal o fuera del mismo.

17. Utilización de al menos un objeto informatizado (1) según una de las reivindicaciones 15 a 16, caracterizada porque la estación de control (4) incluye un algoritmo complementario (410), incluyendo además la utilización del objeto (1) para la autenticación las siguientes etapas:

- memorización en la estación de control (4) de una firma individualizada (130) proporcionada por el objeto informatizado (1);

- extracción en la estación de control, mediante el algoritmo complementario (410), del dato individual (15) utilizado por el objeto informatizado (1) para generar la firma individualizada (130), con fines de comparación con una identificación proporcionada o exhibida por el usuario, o el objeto informatizado, o el terminal, o un dispositivo o un lugar que incluye o utiliza este objeto informatizado.

18. Utilización de al menos un objeto informatizado (1) para el control de un descuento de crédito, caracterizada porque este control incluye una utilización de objetos informatizados (1) según una de las anteriores reivindicaciones, memorizando, por una parte, estos objetos informatizados un dato de saldo (17), que representa un valor de crédito disponible, y un programa (16) que incluye un algoritmo de descuento apto para modificar ese dato de saldo y, por otra, incluyendo estos un dato de validez (18) que presenta un estado determinado cuando está activado el algoritmo de descuento y el dato de saldo representa un crédito no nulo, llevándose a cabo esa modificación del dato de saldo en función de una o varias duraciones de activación del objeto, incluyendo esta utilización para el control las siguientes etapas:

- distribución de tales objetos informatizados a unos usuarios;

- autenticación y control de la validez de uno o varios de estos objetos informatizados, con ayuda de una estación de control según una de las reivindicaciones 6 a 16, siendo estos objetos informatizados exhibidos por los usuarios o accesibles a efectos de control.

19. Utilización de al menos un objeto informatizado (1) según la anterior reivindicación, caracterizada porque la modificación del dato de saldo (17) se lleva a cabo asimismo en función de datos que representan un dato individual (15), o un parámetro suplementario (14), o una elección de clave de base (12) o una combinación de al menos dos de estos elementos.

20. Utilización de al menos un objeto informatizado (1) para el control de utilización de un dispositivo o de un sistema que incluye o utiliza un programa informático, llamado aplicación protegida, caracterizada porque al menos una parte de la aplicación protegida se ejecuta en virtud de la utilización de un objeto informatizado (1) según una de las anteriores reivindicaciones, o utiliza un programa ejecutado en ese mismo objeto informatizado (1), efectuándose el cálculo de la firma (13) o su presentación por parte del objeto informatizado o su transmisión al terminal (2) tan sólo si la aplicación protegida está activa.

21. Objeto informatizado (1) que incluye unos medios de tratamiento de datos, unos medios de memorización, así como unos medios de presentación o unos medios de comunicación con un dispositivo de tratamiento de datos, llamado terminal (2), caracterizado porque incluye al menos un algoritmo de cálculo que permite generar un dato pseudoaleatorio a partir de un dato semilla generado por un módulo de interpretación (24) a partir de datos proporcionados mediante la recepción de una señal (3) exterior por parte del objeto informatizado (1) o por parte del terminal (2), señal (3) esta que varía con el paso del tiempo y que es difundida dentro de una zona determinada sin precisar de direccionamiento de la señal ni de información prevista específicamente para proporcionar ese dato semilla.

22. Sistema de control de un parque de objetos informatizados que comprende al menos un objeto informatizado (1) que incluye unos medios de tratamiento de datos, unos medios de memorización, así como unos medios de presentación o unos medios de comunicación con un dispositivo de tratamiento de datos, llamado terminal (2), caracterizado porque dicho objeto informatizado (1) incluye al menos un algoritmo de cálculo que permite generar un dato pseudoaleatorio a partir de un dato semilla generado por un módulo de interpretación (24) a partir de datos proporcionados mediante la recepción de una señal (3) exterior por parte del objeto informatizado (1) o por parte del terminal (2), señal (3) esta que varía con el paso del tiempo y que es difundida dentro de una zona determinada sin precisar de direccionamiento de la señal ni de información prevista específicamente para proporcionar ese dato semilla, permitiendo el dato pseudoaleatorio la utilización del objeto informatizado (1) según una de las reivindicaciones 6 a 19.

23. Sistema de control de utilización de un dispositivo o de un sistema que incluye o utiliza un programa informático, llamado aplicación protegida, que incluye al menos un objeto informatizado (1) que incluye unos medios de tratamiento de datos, unos medios de memorización, así como unos medios de presentación o unos medios de comunicación con un dispositivo de tratamiento de datos, llamado terminal (2), caracterizado porque dicho objeto informatizado (1) incluye al menos un algoritmo de cálculo que permite generar un dato pseudoaleatorio a partir de un dato semilla generado por un módulo de interpretación (24) a partir de datos proporcionados mediante la recepción de una señal (3) exterior por parte del objeto informatizado (1) o por parte del terminal (2), señal (3) esta que varía con el paso del tiempo y que es difundida dentro de una zona determinada sin precisar de direccionamiento de la señal ni de información prevista específicamente para proporcionar ese dato semilla, permitiendo el dato pseudoaleatorio la utilización del objeto informatizado (1) según la reivindicación 20.

24. Sistema de control de objetos informatizados o de control de utilización de un dispositivo o sistema según

una de las reivindicaciones 22 y 23, caracterizado porque incluye varios objetos informatizados en los cuales se reparten los algoritmos y datos necesarios para su utilización.

25. Utilización de al menos un objeto informatizado (1) para el control de títulos de derecho de estacionamiento de vehículos, caracterizada porque el control de estos títulos pone en práctica la utilización de al menos un objeto informatizado (1) según una de las reivindicaciones 1 a 20 y porque los objetos informatizados (1) son tarjetas inteligentes, prepago o de crédito, con un dato de saldo (17) que representa un valor de tiempo de estacionamiento.

26. Utilización de al menos un objeto informatizado (1) según la anterior reivindicación, caracterizada porque al menos un parámetro suplementario (14) corresponde a una zona geográfica de estacionamiento o a un tipo de tarificación o una combinación de ambos.

27. Utilización de al menos un objeto informatizado (1) según una de las reivindicaciones 24 y 25, caracterizada porque al menos un dato individual (15) corresponde a un dato identificador del objeto informatizado (1) o a un dato identificador de un vehículo o de un usuario o de una cuenta de usuario, o de una combinación de estos elementos.

Fig. 1

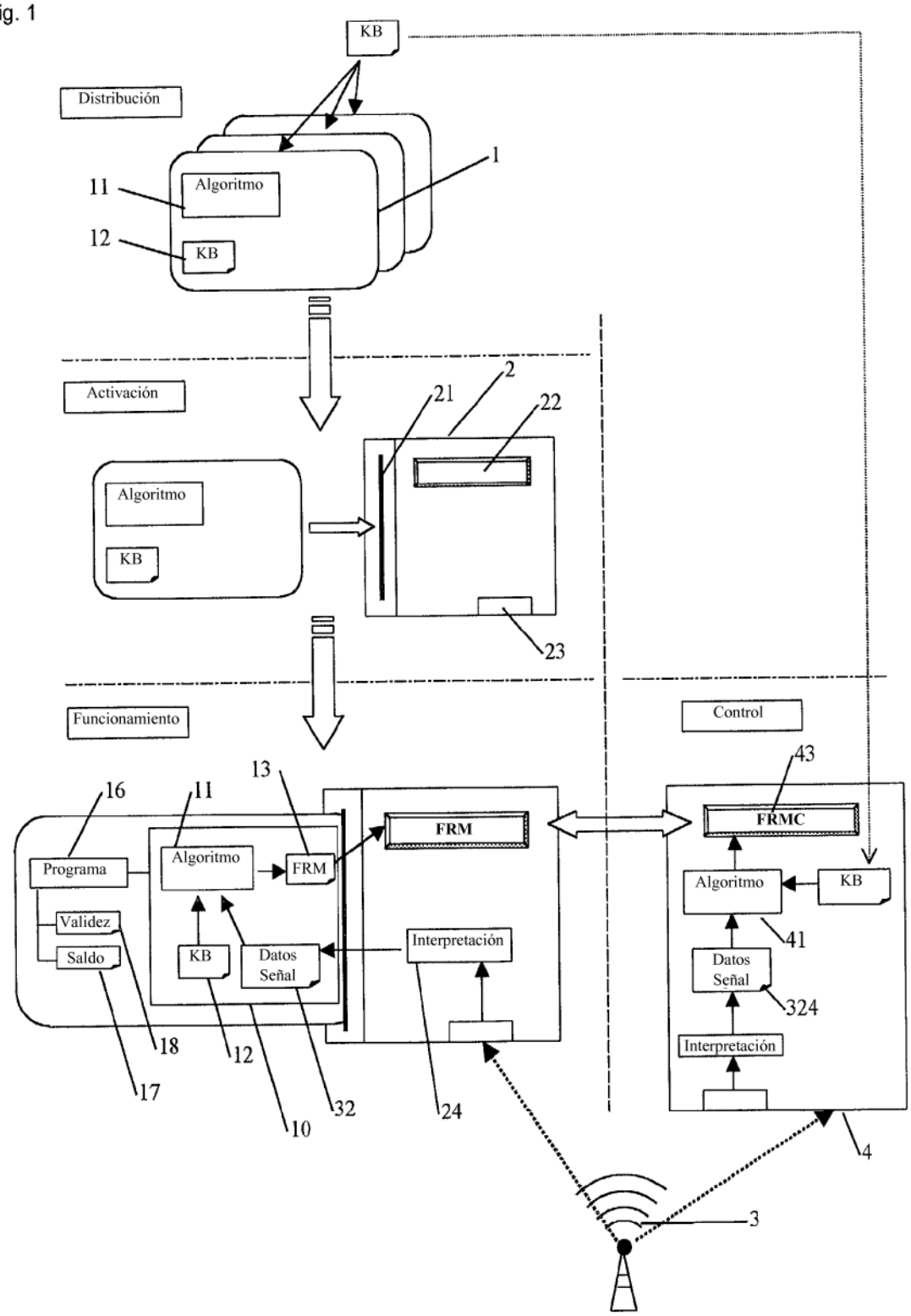

KB
Distribución
1
11
Algoritmo
12
KB
Activación
2
21
22
Algoritmo
KB
23
Funcionamiento
Control
43
13
16
11
FRM
FRMC
Programa
Algoritmo
FRM
Algoritmo
KB
Validez
Saldo
KB
Datos Señal
Interpretación
41
Datos Señal
324
Interpretación
18
12
17
10
32
24
4
3

Fig. 2

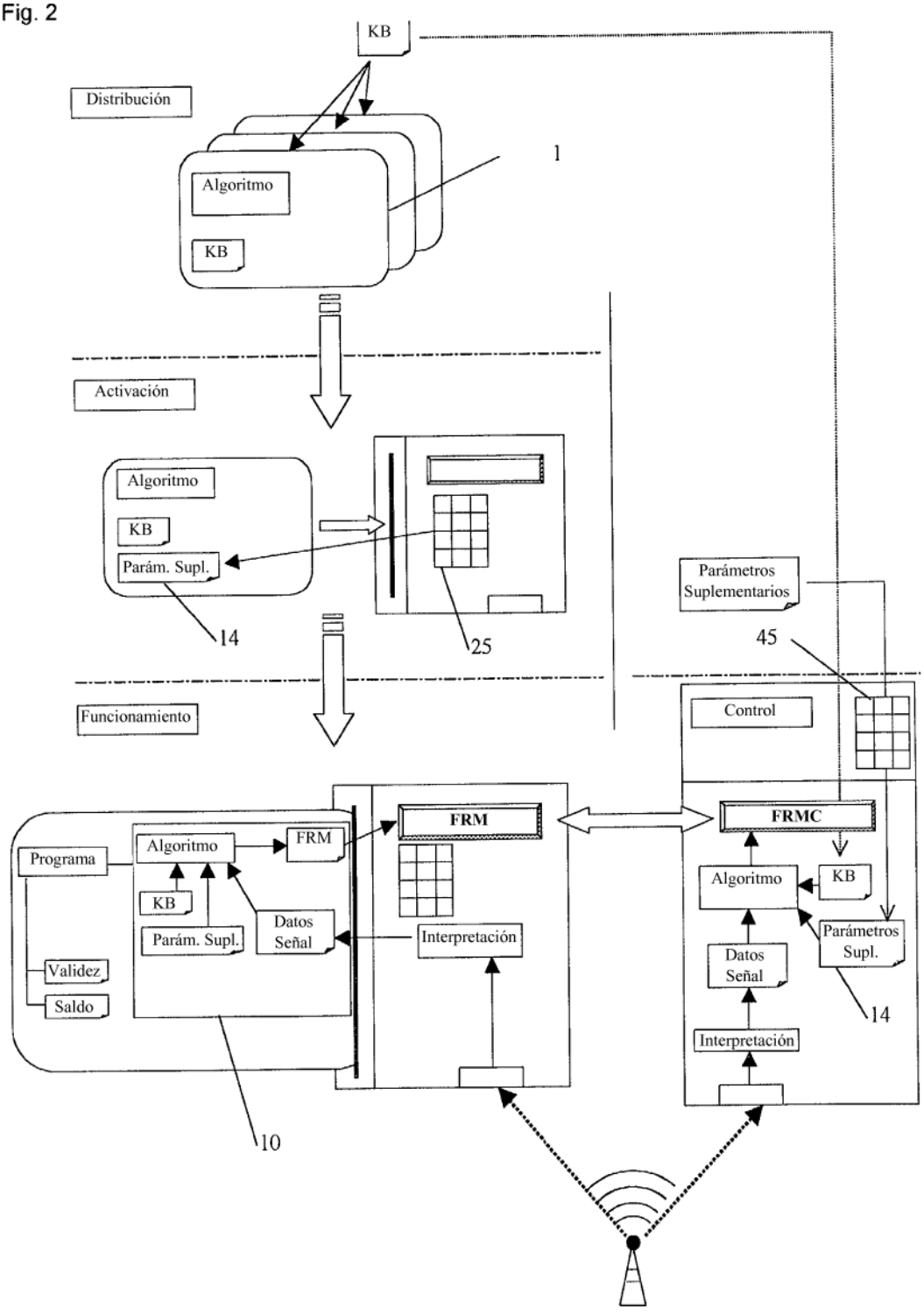

KB
Distribución
1
Algoritmo
KB
Activación
Algoritmo
KB
Parám. Supl.
14
25
Parámetros Suplementarios
45
Funcionamiento
Control
FRM
FRMC
Programa
Algoritmo
FRM
KB
Parám. Supl.
Datos Señal
Interpretación
Validez
Saldo
Algoritmo
KB
Parámetros Supl.
Datos Señal
14
Interpretación
10

Fig. 3

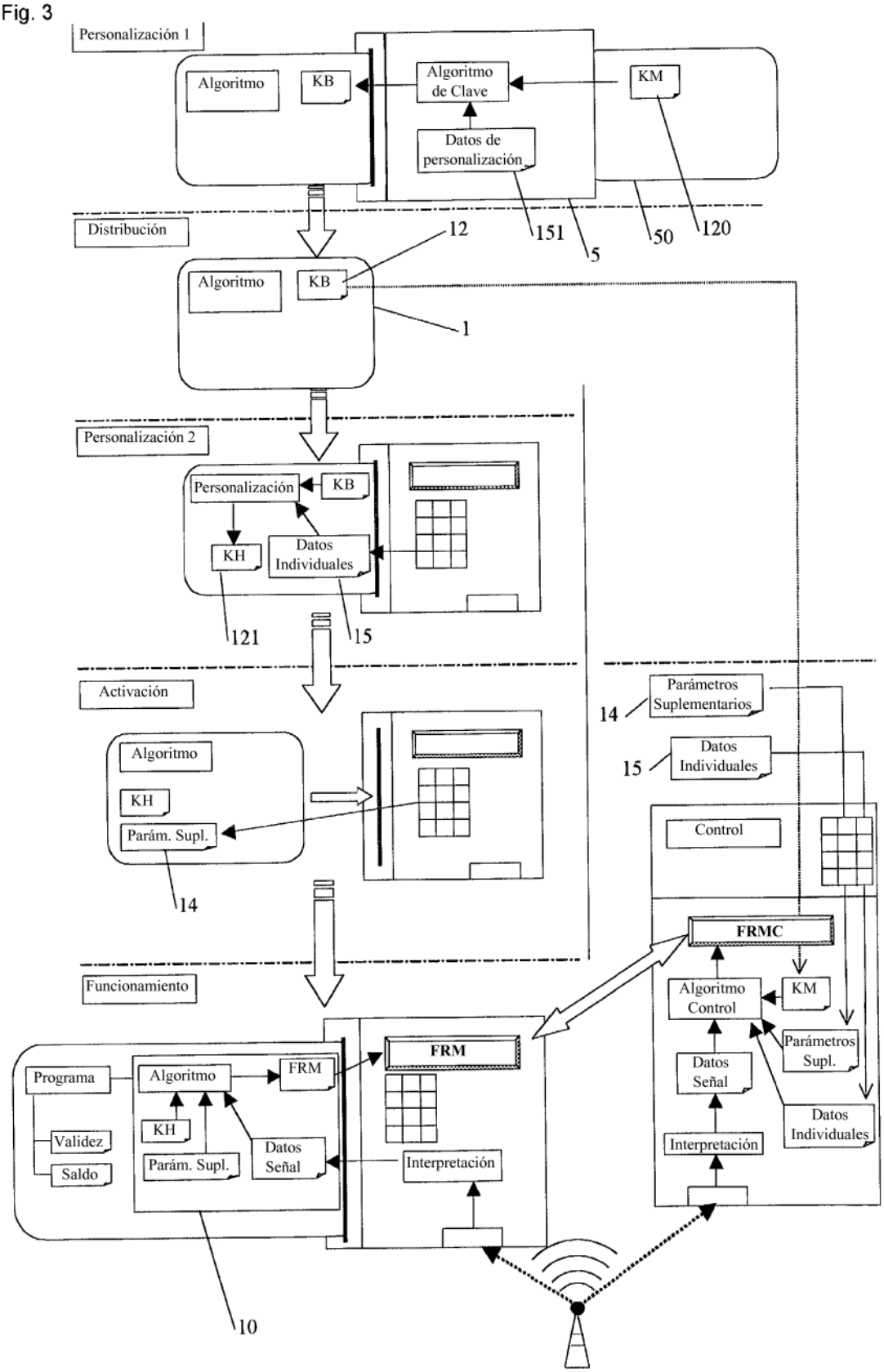

Personalización 1
Algoritmo
KB
Algoritmo de Clave
KM
Datos de personalización
Distribución
12
151
5
50
120
Algoritmo
KB
1
Personalización 2
Personalización
KB
KH
Datos Individuales
121
15
Activación
Algoritmo
KH
Parám. Supl.
14
Parámetros Suplementarios
14
Datos Individuales
15
Control
FRMC
Algoritmo Control
KM
Parámetros Supl.
Datos Señal
Datos Individuales
Interpretación
Funcionamiento
FRM
Programa
Algoritmo
FRM
Validez
Saldo
KH
Parám. Supl.
Datos Señal
Interpretación
10

Fig. 4

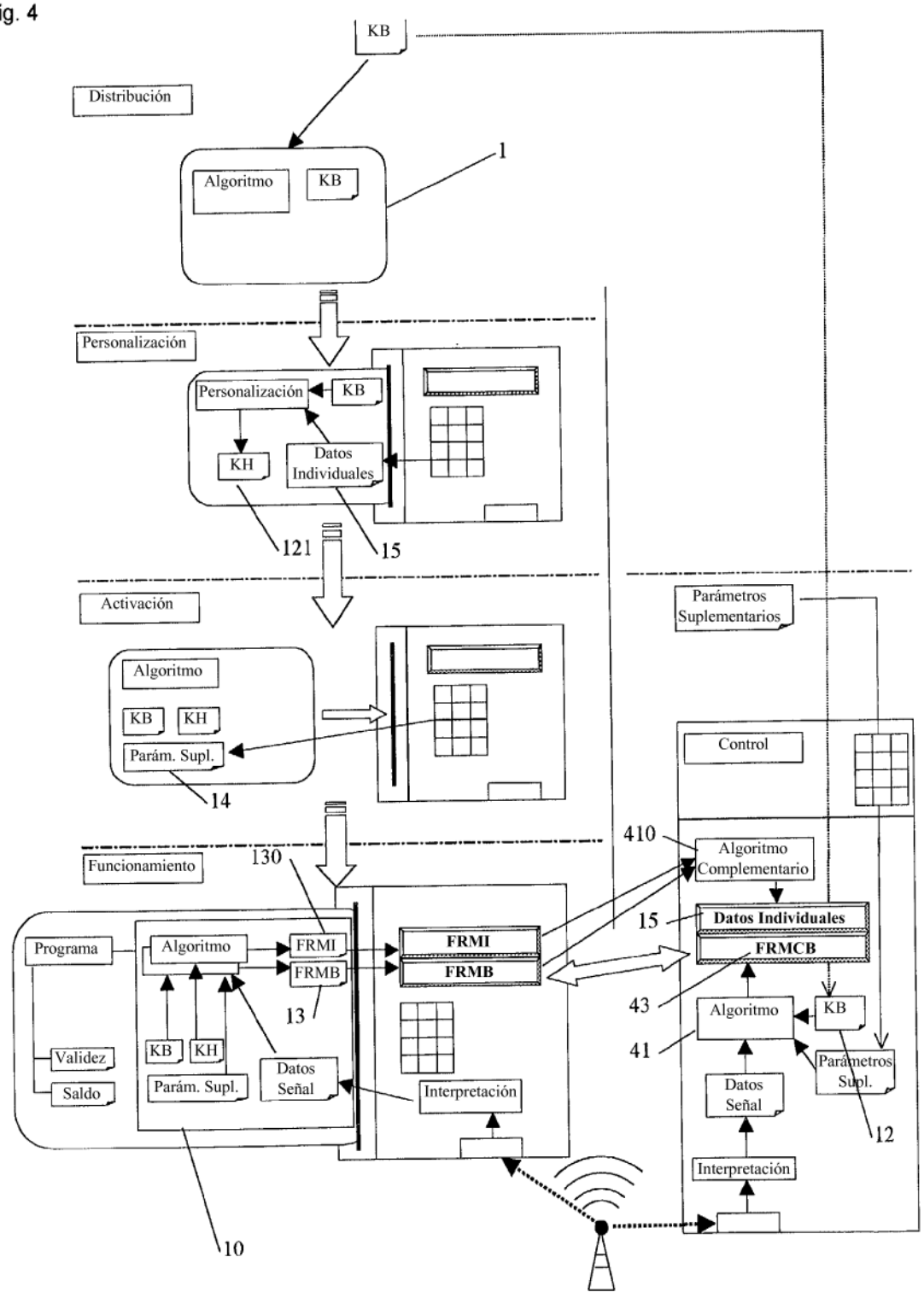

KB
Distribución
Algoritmo
KB
1
Personalización
Personalización
KB
KH
Datos Individuales
121
15
Activación
Algoritmo
KB
KH
Parám. Supl.
14
Parámetros Suplementarios
Control
410
Algoritmo Complementario
Funcionamiento
130
Programa
Algoritmo
FRMI
FRMB
13
Validez
Saldo
KB
KH
Parám. Supl.
Datos Señal
FRMI
FRMB
Interpretación
10
15
Datos Individuales
FRMCB
43
Algoritmo
KB
41
Parámetros Supl.
Datos Señal
12
Interpretación

Fig. 5

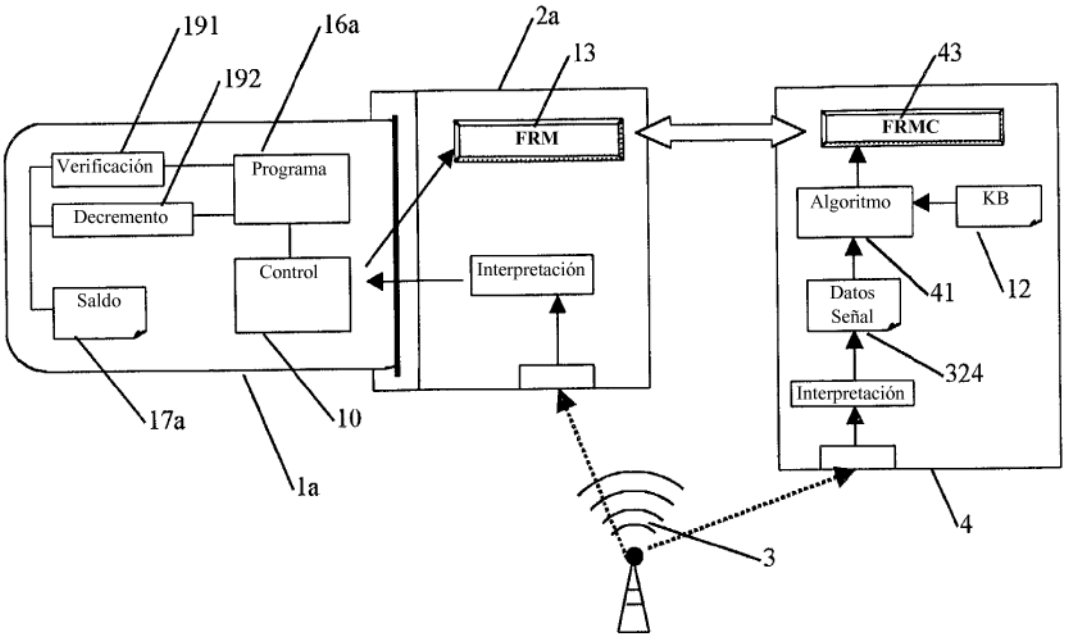
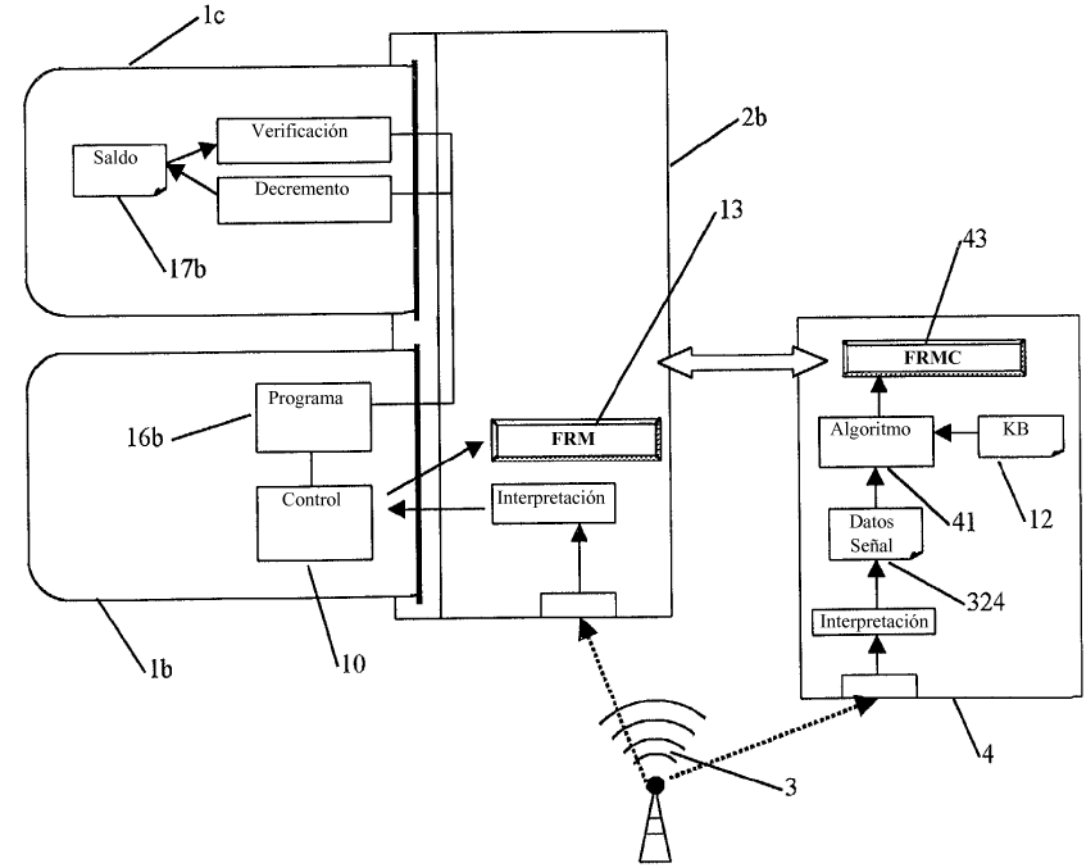

191
16a
2a
13
43
192
Verificación
Programa
FRM
FRMC
Decremento
Algoritmo
KB
Control
Interpretación
Saldo
Datos
Señal
41
12
324
Interpretación
17a
10
1a
4
3

Fig. 6


1c
2b
Verificación
Saldo
Decremento
13
43
17b
FRMC
Programa
16b
FRM
Algoritmo
KB
Control
Interpretación
41
12
Datos
Señal
324
Interpretación
1b
10
4
3