(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 267 138**

(51) Int. Cl.:
G07F 7/10 (2006.01)
E05B 49/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **97915537 .1**
(86) Fecha de presentación : **21.03.1997**
(87) Número de publicación de la solicitud: **0891611**
(87) Fecha de publicación de la solicitud: **20.01.1999**

(54) Título: **Sistema de control de acceso a una función de encriptado utilizando una pluralidad de variables dinámicas.**

(30) Prioridad: **22.03.1996 US 620240**
17.04.1996 FR 96 04798

(45) Fecha de publicación de la mención BOPI:
01.03.2007

(45) Fecha de la publicación del folleto de la patente:
01.03.2007

(73) Titular/es: **ACTIVIDENTITY EUROPE S.A.**
24-28, avenue du Général-de-Gaulle
92156 Suresnes Cédex, FR

(72) Inventor/es: **Audebert, Yves**

(74) Agente: **Ungría López, Javier**

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

Venta de fascículos: Oficina Española de Patentes y Marcas. Pº de la Castellana, 75 – 28071 Madrid

DESCRIPCIÓN

Sistema de control de acceso a una función de encriptado utilizando un pluralidad de variables dinámicas.

La presente invención se refiere a un sistema electrónico de control de acceso a una función o de autentificación de una persona o de un mensaje, que permite particularmente a un usuario obtener de forma condicional un servicio u otra prestación que debe ser suministrada por una unidad de servicio especializado asociada con el sistema en cuestión.

Más particularmente, la invención se refiere a un sistema de control de acceso a un ordenador o más generalmente a una red informática cuya utilización está reservada para personas que están debidamente legitimadas. Tales redes pueden servir por ejemplo para asegurar toda clase de servicios que impliquen una transacción, lo más a menudo con contrapartida económica, tal como la tele-compra, la televisión de pago, el banco a domicilio, los juegos televisados interactivos, o igualmente el facsímile confidencial, etc.

Un ejemplo de un sistema de este tipo de la técnica anterior se describe en la patente US No. 3 806 874. Esta describe un sistema de identificación o de autentificación de personas en el cual una palabra de pase se produce por el digitalizado de datos temporales decimales codificados binarios y de dos números fijos. En este sistema, una unidad de identificación (o tarjeta) produce primeras y segundas secuencias de datos (palabras de pase) en función de un número de identificación personal, de datos secretos y de datos temporales binarios procedentes de un primer reloj. El número personal se transmite a una unidad de comprobación (o servidor). La unidad de comprobación produce primeras y segundas secuencias de datos digitalizando el número de identificación personal, los datos secretos y los datos temporales decimales codificados binarios procedentes de un segundo reloj. Los datos temporales son proporcionados independientemente por los relojes que se encuentran respectivamente en la unidad de identificación y en la unidad de comprobación.

Más particularmente, la unidad de identificación 10 comprende una memoria primaria ROM 12 en la cual se almacena un número de identificación personal, y un circuito secreto 20 que memoriza datos secretos en una memoria secreta 26 que permite producir las primeras y segundas secuencias de datos. Los datos secretos son diferentes para cada usuario y no le son conocidos. El circuito secreto 20 comprende un circuito de digitalizado que proporciona las primeras y segundas secuencias digitalizando datos de entrada compuestos por el número de identificación personal, datos secretos y datos temporales decimales codificados binarios producidos por el reloj 42.

En el servidor, un circuito secreto 31 correspondiente al circuito secreto 20 de la tarjeta comprende una memoria secreta 33 y recibe una entrada temporal de un reloj 53. El circuito secreto 31 recibe igualmente una entrada (el número de identificación personal) de la memoria primaria 12 de la unidad de identificación 10. El circuito secreto 31 comprende un circuito de digitalizado que produce primeras y segundas secuencias de datos (palabras de pase) digitalizando los datos de entrada compuestos por el número de identificación personal, los datos secretos y los datos temporales decimales codificados binarios procedentes del reloj 53.

Las primeras secuencias de datos se comparan en un comparador 30 de la tarjeta. Si existe concordancia, se produce una señal de aceptación. El comparador compara (1) la primera secuencia de datos obtenida del servidor durante el mismo intervalo de tiempo durante el cual la primera secuencia de datos ha sido producida en la unidad de comprobación con (2) la primera secuencia de datos producida durante el mismo intervalo de tiempo en la tarjeta.

En otras palabras, el comparador 30 debe recibir del servidor la primera secuencia de datos durante el mismo intervalo de tiempo durante el cual ha sido producida para que esta secuencia de datos recibida esté en concordancia con la primera secuencia de datos producida en la unidad de comprobación durante este mismo intervalo de tiempo. El mismo razonamiento se aplica a las segundas secuencias de datos confrontadas en el comparador 41.

Los circuitos secretos 20 y 31 de la patente US nº 3 806 874 generan palabras de pase (números de comprobación) mediante la digitalización del número de identificación personal, de los datos secretos y de los datos temporales decimales codificados binarios con el fin de producir las primeras y segundas secuencias de datos. Para que las secuencias de datos concuerden, es preciso que los datos temporales utilizados en la unidad de identificación y en la unidad de comprobación sean idénticos. Por consiguiente, los relojes 42 y 53 deben ser síncronos para que puedan producir aproximadamente al mismo tiempo los mismos datos temporales.

La patente US 4 601 011 describe un sistema de autentificación que genera una palabra de pase digitalizando un número fijo con una clave formada por dos partes de las cuales la primera no cambia y la segunda cambia cada vez que se utiliza la clave para la digitalización.

Este sistema comprende al menos una unidad portátil electrónica (tarjeta) y al menos una unidad de comprobación electrónica (servidor) que debe condicionalmente proporcionar autorizaciones de acceso a un ordenador. El sistema genera palabras de pase que en una primera variante son función del tiempo y en una segunda variante función del número de palabras de pase producidas por la unidad portátil. Esta comprende un módulo de digitalización que digitaliza una palabra de pase diferente para cada transmisión utilizando para ello una clave en dos partes. El servidor recibe la palabra de pase de la tarjeta y genera una palabra de pase interna por digitalización de un número fijo (que corresponde al número fijo digitalizado en la tarjeta) con la primera parte de la clave (almacenada en memoria) y la segunda parte de la clave (recibida de la tarjeta). Un comparador 50 compara la palabra de pase recibida con la palabra de pase interna y, en función del resultado de la comparación, proporciona una salida que concede o rechaza el acceso al ordenador 56.

Los sistemas de las patentes US 4 601 011 y 3 806 874 producen los dos palabras de pase idénticas ("secuencias de datos" o "números de comprobación digitalizados") en la tarjeta y en el servidor, calculando las dos unidades de forma independiente las palabras de pase ejecutando para ello un programa de digitalización sobre datos que comprenden al menos un código personal fijo y al menos un número función del tiem-

po o que varía en función del número de veces que una palabra de pase ha sido producida en la tarjeta.

La patente US 4 720 860 describe otro sistema de autentificación en el cual, para generar las palabras de pase, se utiliza una variable estática y una variable dinámica. En esta patente, al inicio de un procedimiento de solicitud de acceso, el usuario debe introducir en la tarjeta un código fijo cada vez que deba realizarse una transacción. El código fijo es una variable estática. Una segunda variable se produce con el fin de modificar de forma dinámica en función del tiempo, en particular en función del instante en el cual el código fijo es introducido en la tarjeta por el usuario. Las dos variables de las cuales una es por consiguiente estática y la otra dinámica, se utilizan entonces como parámetros de entrada de un algoritmo secreto de digitalización que sirve para generar una palabra de pase en la tarjeta.

Esta palabra de pase se visualiza en la tarjeta y el usuario es invitado a transferirla al servidor. El código fijo se transfiere igualmente al servidor que, utilizando el mismo algoritmo de digitalización y una variable dinámica que tiene en principio el mismo valor que el utilizado en la tarjeta, calcula igualmente la palabra de pase. Esta última se compara con la palabra de pase transmitida al servidor por el usuario y si existe concordancia, una autorización de acceso a la función puede ser considerada. Este sistema de control de acceso utiliza por consiguiente una variable estática con ayuda de la cual el algoritmo de digitalización calcula la palabra de pase utilizando igualmente la variable dinámica.

En este sistema, la variable estática se almacena en una memoria de la tarjeta y se transmite al servidor, por ejemplo por mediación de una línea telefónica. Así, la misma es susceptible de ser descubierta por piratas que utilizan procedimientos electrónicos fraudulentos.

En este sistema, el algoritmo debe por consiguiente necesariamente mantenerse secreto con el fin de preservar la seguridad del sistema. Si la seguridad del algoritmo es vulnerada, la seguridad del conjunto del sistema se compromete, pues las variables estáticas pueden eventualmente ser descubiertas por procedimientos electrónicos fraudulentos. Por eso se indica, en esta patente, que se prevén medios para destruir el algoritmo en caso de tentativa de fraude en la tarjeta (por ejemplo memorizando el algoritmo en una memoria volátil).

Se debe igualmente observar que en las dos patentes US No. 3 806 874 y 4 720 860, la segunda variable es un valor dinámico en función del tiempo. Como esta variable debe necesariamente ser producida independientemente a la vez en la tarjeta y en el servidor, los relojes de las dos unidades utilizadas para generar la variable dinámica por cada lado deben sincronizarse con una precisión dada. Para no tener que proporcionar relojes demasiado precisos (lo que aumentaría considerablemente el coste del sistema), es necesario admitir un margen de tolerancia dentro del cual la palabra de pase actual es valedera. Cuanto más corto es el margen de tolerancia más se asegura la fiabilidad, pero igualmente más molesto es un defecto de sincronización de los relojes.

Habida cuenta de este margen de tolerancia, la palabra de pase calculada en cada solicitud de acceso es también valedera durante el tiempo de duración de cada intervalo que separa dos operaciones de cálculo de la variable dinámica. Dicho intervalo puede tener una duración relativamente larga (típicamente 10 minutos incluso más, por ejemplo) de forma que un defraudador amparándose subrepticiamente en la palabra de pase de una tarjeta en el momento de una solicitud de acceso, tendrá tiempo de utilizarla durante todo el intervalo anteriormente mencionado en el servidor y podrá así fácilmente obtener una autorización de acceso.

En la patente US nº 4 800 590, se describe igualmente un sistema de autentificación que utiliza una clave de digitalización dinámica en función del tiempo. Más particularmente, este sistema utiliza como parámetro de entrada de un algoritmo de digitalización, una clave de digitalización utilizada como variable dinámica que se modifica en función del tiempo. Este procedimiento necesita una actualización periódica de la clave de digitalización, por ejemplo a una frecuencia dada de un minuto. Si esta actualización puede realizarse fácilmente en la tarjeta, no sucede lo mismo en lo que respecta al servidor. En efecto, el sistema puede tener un número muy grande de usuarios teniendo cada uno una tarjeta a la cual se asigna una variable dinámica evidentemente única para esta tarjeta. Por consiguiente, en este sistema conocido de la patente US 4 800 590, el servidor debe periódicamente recalcular mediante cálculos iterativos, bien sea todas las claves de digitalización a la vez, o actualizar la clave de digitalización de la tarjeta considerada mientras que esta demanda un acceso. Se entiende que si el sistema comprende un gran número de tarjetas (típicamente 100 000, por ejemplo), la actualización de las claves de digitalización se vuelve rápidamente una carga de cálculo demasiado importante para el servidor. Esta patente describe igualmente la posibilidad de actualizar la clave en respuesta a una acción del usuario sobre una tecla; este modo de realización es desventajoso pues limita la frecuencia de modificación de la clave.

La patente US 5 060 263 describe igualmente un sistema que genera una palabra de pase dinámica. En este sistema, un generador de palabras de pase produce cada palabra de pase por la digitalización de la palabra de pase producida antes utilizada como variable. Un gran número de claves de digitalizado fijas se almacena en la tarjeta. Para aumentar la seguridad, el servidor genera un número aleatorio para designar una de las claves que se utilizará para generar la palabra de pase. La tarjeta debe repetir las secuencias de digitalizado (por medio de un algoritmo público del tipo DES) tantas veces como claves existan en la tarjeta, reiniciando la salida respecto a la entrada.

En este sistema conocido, las claves tienen por consiguiente valores fijo no obstante sean elegidos aleatoriamente. Sin embargo, pueden ser descubiertas fraudulentamente en la memoria de la tarjeta. Además, el número aleatorio generado en el servidor debe transmitirse a la tarjeta y puede por consiguiente ser interceptado fraudulentamente durante la transmisión. Otro problema de este sistema se plantea si el usuario de la tarjeta no consigue una demanda de acceso al servidor. En este caso, pueden existir serios problemas de desincronización, pues cada palabra de pase es generada sobre la base de la palabra de pase precedente, de forma que el desfase se hace cada vez más importante con el tiempo. Se debe entonces prever un mecanismo que permita restablecer la sincronización.

El documento EP 0605 996 A1 describe un sistema donde un código de seguridad se transmite por un codificador 28 que comprende una parte representada por un valor del contador de transmisión 22, una parte representada por un código de identificación 24 y una parte representada por un "rolling code" 26. Este código de seguridad es por consiguiente la yuxtaposición de tres elementos que son transmitidos por el codificador 28 al decodificador 42. Este los separa con miras a su tratamiento individual por el receptor 40.

Dos de estos elementos, el valor del contador de transmisión 22 y el "rolling code 26" son variables dinámicas pero no sirven para generar parámetros de entrada de un algoritmo de digitalización que produzca una palabra de pase.

La invención tiene por objeto proporcionar un sistema de control de acceso o de autentificación de personas y/o de mensajes que ofrece una mejor seguridad contra los fraudes.

La misma tiene por consiguiente por objeto un sistema de control de acceso o de autentificación de personas y/o de mensajes según la reivindicación 1.

Las variables dinámicas deben ser coherentes en las indicadas primera y segunda unidades; las mismas deben por consiguiente presentar una relación predeterminada, como por ejemplo la identidad.

Se desprende primeramente de estas características que las primeras unidades del sistema no contienen en su memoria para el cálculo palabra de pase ninguna variable estática susceptible de ser descubierta fraudulentamente, por ejemplo por espionaje. Otra ventaja consiste en que el algoritmo de digitalización no tiene necesariamente por qué ser secreto y si lo es así, se pueden obviar medios de destrucción de este algoritmo en caso de fraude.

Es cierto que si se utiliza un algoritmo público, al menos una de las variables dinámicas debe ser secreta, pero en caso de descubrimiento fraudulento de una variable de este tipo (que es propia de la tarjeta), solo la tarjeta en cuestión pierde su seguridad mientras que el sistema propiamente dicho la mantiene completamente.

Así, según otra característica de la invención, los indicados primeros y segundos medios generadores comprenden respectivamente terceros y cuartos medios de cálculo para producir al menos una primera de las indicadas variables dinámicas según una función que hace intervenir el número de demandas de acceso formuladas por la indicada primera unidad anteriormente a la solicitud de acceso en curso.

Sucede de esta característica particularmente ventajosa que, gracias a la invención, la actualización de una primera de las variables dinámicas, utilizadas por ejemplo como clave de digitalización, no tiene necesidad de ser realizada periódicamente y no necesita en el servidor ningún nuevo cálculo o "recuperación" del valor de la variable dinámica calculada para una solicitud de acceso anterior, con relación al valor actual de esta variable dinámica calculada que se encuentra en la tarjeta en el momento en que se formula una demanda de acceso. El trabajo de cálculo para el servidor se reduce por consiguiente al mínimo.

Desde luego, puede suceder que el número de demandas de acceso contabilizadas por la tarjeta sea superior al registrado por el servidor debido a que el usuario de la tarjeta puede no siempre conseguir una demanda de acceso. Sin embargo, en este caso, el servidor no tendrá que recuperar en el peor de los casos más que un número muy pequeño de iteraciones para calcular de nuevo la variable dinámica. Además, se podrá, por construcción, limitar de oficio la diferencia entre los números de demandas de acceso contabilizados respectivamente en las dos unidades.

Se observará igualmente que, gracias a la invención, si un individuo se apodera fraudulentamente con una palabra de pase que acaba de ser obtenida por un usuario de una tarjeta dada y es transferida legítimamente al servidor por éste, esta palabra de pase no conducirá a una autorización de acceso. En efecto, una nueva demanda de acceso, incluso formulada muy rápidamente después, generará una palabra de pase diferente de la que va a ser calculada en el servidor, pues la variable dinámica de la tarjeta habrá entonces evolucionado por el aumento del número de demandas de acceso.

En un modo de realización particular, el sistema de control de acceso puede comprender segundos medios de cálculo de la palabra de pase que descifran la palabra de pase recibida según al menos un algoritmo de desciframiento que utiliza como clave de descifrado un parámetro de entrada en función de una primera variable dinámica producida en la mencionada segunda unidad para derivar una variable dinámica que debe corresponder a una de las variables dinámicas producidas en la primera unidad. En este caso, esta segunda unidad comprende igualmente medios comparadores que comparan la variable dinámica derivada por los segundos medios de cálculo, a una segunda de las indicadas variables dinámicas producidas en la mencionada segunda unidad, y medios que, cuando los medios comparadores observan una relación predeterminada entre la variable dinámica derivada por los segundos medios de cálculo y la segunda de las indicadas variables producida en la segunda unidad, proporcionan una autorización de acceso a la mencionada función.

Otras características y ventajas de la invención aparecerán en el transcurso de la descripción que sigue, dada únicamente a título de ejemplo y realizada haciendo referencia a los dibujos adjuntos en los cuales:

- la figura 1 es un esquema general de un sistema de control de acceso según la invención;
- la figura 2 es un organigrama simplificado que ilustra el principio de desarrollo de las operaciones en el sistema según la invención, cuando se ha tratado una demanda de acceso;
- la figura 3 muestra un organigrama del modo de cálculo de una clave de digitalización utilizada para el cálculo de la palabra de pase.

En la figura 1, se ha representado un esquema muy simplificado de un sistema de control de acceso según la invención.

El sistema está supuesto para proporcionar un acceso condicional a una función que se simboliza por el rectángulo 1 en la figura 1. El término "función" debe ser tomado en una acepción muy amplia. Designa toda función en la cual el acceso está condicionado por una autorización que requiere una autentificación que implica una comprobación del útil (tarjeta) con la ayuda del cual se formula la demanda, y de preferencia igualmente una identificación de la persona que demanda el acceso a la función para saber si su demanda es legítima.

La función puede ser de cualquier naturaleza, por ejemplo una función de acceso a un local, a una red

informática o a un ordenador, a una transacción de orden pecuniario (tele-compra, banco a domicilio, juego televisado interactivo, televisión de pago), etc. Por otro lado, funciones de autentificación, bien sea de personas, o de mensajes, caen expresamente dentro del alcance de la presente invención, aunque en el conjunto de la descripción se haga más bien referencia a un procedimiento que implica demandas de acceso a una función.

En estas condiciones, se aprecia en la figura 1 que según un modo de realización particular, el sistema según la invención puede comprender al menos una primera unidad 2 llamada "tarjeta" y al menos una segunda unidad 3. Se apreciará que el sistema de control de acceso según la invención puede comprender un gran número de primeras unidades y una o varias segundas unidades, pero en todo caso en un número generalmente claramente más bajo. Los números de las unidades 2 y 3 no son por consiguiente en modo alguno limitativos de la invención.

La primera unidad o tarjeta 2 es de preferencia portátil y personalizada para ser asignada personalmente a un usuario dado. La misma se presenta por ejemplo bajo la forma de una calculadora o de una tarjeta de crédito y la misma lleva un número de identificación público 5 indicado esquemáticamente en la figura 1. Este número puede inscribirse en ella en claro y ser asignado en el momento de su inicialización. Puede igualmente estar formado por el apellido del usuario o por cualquier otra información adecuada de este. Otro número, el número de identificación personal o PIN, es secreto y normalmente conocido solamente por el usuario autorizado de la tarjeta. Para utilizar la tarjeta, el número de PIN debe ser introducido con ella por el usuario, comparando la tarjeta el número de PIN introducido con un valor que se memoriza en ella. Si el número PIN introducido y el valor memorizado concuerdan, el usuario recibe la autorización de utilizar la tarjeta; de lo contrario la tarjeta no funcionará para generar una palabra de pase. En cuanto al número de identificación público, identifica la tarjeta propiamente dicha respecto a la unidad 3 entre todas las tarjetas con las cuales el sistema está llamado a trabajar.

La tarjeta 2 comprende un teclado 6 destinado para permitir la introducción de informaciones, tales como por ejemplo los números de identificación ya mencionados, así como diversas teclas de función 7. La misma comprende igualmente una pantalla de visualización 8 y está dotada de un circuito integrado 9 que comprende particularmente un microcontrolador debidamente programado así como las memorias ROM y RAM habituales.

La tarjeta 2 comprende igualmente un dispositivo de comunicación 10 que permite comunicarse con la unidad 3, bien sea directamente, o por una conexión de transmisión a más o menos larga distancia. Este dispositivo puede presentarse bajo numerosos aspectos por ejemplo una conexión telefónica en DTMF, un dispositivo de transmisión de datos por rayos infrarrojos, un dispositivo llamado "en modalidad conectada" en el cual la tarjeta se introduce en un lector adecuado o cualquier otro dispositivo de transmisión bien conocido en la técnica.

La segunda unidad 3 abarca primeramente medios de interfaz que permiten asegurar la comunicación con la tarjeta 2 por medio del dispositivo de comunicación 10. En el modo de realización representado en las figuras 1 y 2, estos medios de interfaz se simbolizan por un rectángulo 12; pueden presentarse bajo numerosas formas. Puede tratarse por ejemplo de un lector dedicado especialmente, pero puede igualmente presentarse en forma de un terminal de ordenador introducido por ejemplo en una red, o también un ordenador personal equipado con una interfaz de rayos infrarrojos, etc. Su particularidad es que puedan comunicar bajo una forma apropiada con la o las tarjetas que le es o son asociada(s).

Los medios de interfaz 12 pueden comprender un teclado 13 y una pantalla de visualización 14 para permitir a un usuario introducir informaciones a comunicar a una parte 15 de la segunda unidad 3, tales como por ejemplo palabras de pase o datos para autentificar relativos a la función 1. Sin embargo, la introducción de estos datos puede ser realizada de otras maneras, particularmente de forma automática sin intervención manual del usuario, por ejemplo por la simple introducción de la tarjeta en la interfaz 12 o por uno de los botones de función 7 que provocan por ejemplo la emisión de rayos infrarrojos modulados.

La interfaz 12 comunica con otra parte 15 de la unidad 3 llamada "servidor" en la presente descripción. Esta comunicación simbolizada por la conexión 16 puede hacerse a corta o a larga distancia por cualquier medio adecuado. Las informaciones que circulan por esta conexión son particularmente la palabra de pase a controlar en el servidor 15 y eventualmente datos a autentificar y a explotar en el servidor.

El servidor 15 comprende en particular un procesador 17 y una memoria 18. El procesador es capaz de liberar condicionalmente las funciones 1, consideradas por las demandas de acceso formuladas por las diversas tarjetas, pudiendo estas funciones ser aseguradas en el interior o en el exterior. Hay que observar que el servidor coopera generalmente con un gran número de tarjetas por mediación de interfaces tales como la interfaz 12.

La figura 2 representa un organigrama simplificado de las diversas operaciones que se desarrollan cuando una demanda de acceso a una función se formula por el usuario de una tarjeta. La figura 2 se divide en dos partes, la parte a la izquierda con trazos interrumpidos 19 que representa las operaciones realizadas en la tarjeta 2 y la parte a la derecha de este trazo que muestra las que se desarrollan en la parte 15 o servidor de la unidad 3.

Para iniciar el procedimiento, el número de identificación público 5 debe ser comunicado al servidor 15. Esta operación puede realizarse de diversas maneras. Por ejemplo, puede comunicarse directamente al servidor desde que se introduce la tarjeta en la interfaz 12. Puede teclearse directamente en el teclado 13 de este por el usuario mismo, o bien en el teclado 6 de la tarjeta 2 y transferido por el dispositivo de comunicación 10. La comunicación puede igualmente realizarse por una conexión a distancia, tal como una línea telefónica o por vía hertziana.

El usuario debe igualmente dar su legitimización tecleando en 20 su código de identificación personal o código PIN almacenado en la memoria de la tarjeta. En caso de no concordancia, la demanda de acceso es de entrada rechazada en 22, pudiendo el usuario permitirse eventualmente varias tentativas consecutivas antes que le sea presentado un rechazo definitivo, si todas siguen siendo infructuosas.

Si por el contrario el código PIN introducido en el código PIN memorizado concuerdan, el programa desencadena en 23 la operación de cálculo de la palabra de pase.

Este cálculo consiste en una digitalización con la ayuda de un algoritmo de digitalización que puede ser secreto o público (bloque 24). En este último caso, puede tratarse de un algoritmo llamado DES (Data Encryption Standard) por los especialista de esta técnica.

Según la invención, el algorítmo en cuestión utiliza parámetros de entrada en función de variables dinámicas que, en el caso representado, se encuentran en número de tres. Dos de entre ellas son una variable Nn almacenada en un registro 25 y que representa el número de demandas de acceso realizadas por la tarjeta, y una variable T que está constituida por la posición actual de un contador 26. Cuando se inicializa cada tarjeta, estas variables pueden fijarse con valores iniciales, N0 y/o T0 respectivamente que no son necesariamente iguales a cero y que puede ser secretas o públicas. De igual modo, Nn y T pueden variar según funciones que hacen intervenir parámetros tales como entre otros el número de demandas de acceso, una función del número de demandas de acceso y el tiempo actual.

Cada una de las dos variables Nn y Tn puede comprender 32 bitios y previamente ser sometida a una operación de concatenación en 27 ofreciendo así un parámetro de entrada de 64 bitios en total. La operación en 27 realizada sobre las variables Nn y Tn puede igualmente estar constituida por cualquier otro tratamiento o combinación como el entrelazado, la interrupción, una operación OU-EXCLUSIF ó ET etc. En otras palabras, la operación en 27 no se limita a estas diversas variantes, sino que puede consistir en cualquier operación realizada con el fin de producir una salida (de 64 bitios) por combinación o tratamiento de Nn y Tn.

La tercera variable dinámica es una clave de digitalización Kn utilizada por el algoritmo en 24 para digitalizar el parámetro de entrada procedente de la operación de concatenación en 27. La clave de digitalización Kn se memoriza en un registro 28 y la misma se actualiza en cada demanda de acceso, como se explica más adelante. Según unas variantes, el algorítmo realizado en 24 puede calcular una palabra de pase en función de los valores actuales de Nn, Tn y Kn, o Kn puede cifrarse según una clave que comprende un valor producido por la concatenación de Nn y Tn en 27.

La digitalización realizada en 24 da lugar a la producción de una palabra de pase A en 29 y al incremento de una unidad en 30 de la posición del registro 25 de demandas de acceso que memoriza Nn. El número incrementado Nn+1 es almacenado en el registro 25 y sometido a una operación de cálculo en 31 destinada para elaborar el nuevo valor Kn+1 de la tercera variable dinámica o clave de digitalización secreta. En variante, la salida del bloque 30 puede provocar el incremento del registro 25 por un valor diferente de la unidad, por ejemplo se puede incrementarlo en dos unidades a la vez (o de cualquier otro valor). De igual modo, el número de unidades de incremento puede variar de una demanda de acceso a la siguiente. Bien entendido, el incremento debe entonces sincronizarse con el realizado en el servidor 15.

Un ejemplo de las operaciones que pueden ser realizadas para el cálculo del nuevo valor de Kn se representa en la figura 3. Estas operaciones son realizadas de común acuerdo tanto en la tarjeta 2 como en el servidor 15. Los valores de Nn+1 y Kn se someten en 32 a una operación de combinación lógica, por ejemplo una combinación OU-EXCLUSIF. La variable intermediaria resultante Z se somete a una digitalización en 33 con la ayuda de un algoritmo conocido o público que puede eventualmente ser el mismo que el utilizado en 24. La digitalización puede realizarse con la ayuda de una clave de digitalización que es de preferencia el valor de la variable dinámica actual Kn, aunque otra clave secreta Q cualquiera (bloque 34) pueda igualmente ser utilizada.

El resultado de la operación de digitalización en 33 es el nuevo valor Kn+1 de la clave de digitalización que va a ser utilizada en la próxima demanda de acceso. Este valor se memoriza en el registro 26.

Después de la obtención de la palabra de pase A que se visualiza en la pantalla 8 de la tarjeta, el usuario es invitado a comunicarla a la unidad 3. Hay que observar que esta palabra de pase puede ser el resultado completo de la operación de digitalización en 24 (con una longitud de 64 bitios) o bien solamente una parte de este resultado, por ejemplo una palabra de 32 bitios. Esta comunicación (simbolizada por líneas de trazo interrumpido 35) puede realizarse por ejemplo tecleando la palabra en el teclado 13 de la interfaz 12. Esta comunicación puede igualmente realizarse de forma automática por medio del dispositivo de comunicación 10 o por cualquier otro medio de comunicación apropiado, como se ha descrito anteriormente.

Durante la introducción en la unidad 3 del número de identificación público 5, el programa del servidor 15 ejecuta, de común acuerdo con la tarjeta y con la ayuda de variables dinámicas producidas independientemente con relación a la tarjeta 2, operaciones de cálculo idénticas a las realizadas en esta. Estas operaciones han sido por consiguiente indicadas en la figura 2 por las mismas referencias numéricas seguidas de la letra “a”, como lo son los registros y el contador que sirve para producir las variables dinámicas Nna, Ta y Kna. La variable Kna es extraída de la memoria 18 del servidor 15 en respuesta a la demanda de acceso, por ejemplo por transferencia del número de identificación 5 hacia la interfaz 12. La memoria 18 almacena las variables Kna de todas las tarjetas con las cuales el servidor está llamado a cooperar.

Por consiguiente, el servidor 15 produce por su parte y sin que le sean comunicadas las variables dinámicas producidas en la tarjeta 2, una palabra de pase Aa que se comparará con la palabra de pase A comunicada al servidor 15 por el usuario. Si la tarjeta es auténtica, las palabras de pase A y Aa deben ser idénticas o al menos concordar según normas predeterminadas. Si el ensayo en 36 conduce a una respuesta afirmativa, la función en 1 queda liberada. En el caso contrario, el acceso se rechazará en 37.

Se debe apreciar que en un sistema según la invención, algunos problemas pueden plantearse cuando una de las variables es el tiempo o es una función del tiempo, como se ha descrito anteriormente, pues la deriva de los relojes utilizados tanto en la tarjeta como en el servidor no puede evitarse. Una solución ventajosa de estos problemas se describe en la solicitud de patente presentada este día a nombre de la firma solicitante de la presente solicitud y titulada “Sistema de control de acceso a una función que comprende un dispositivo de sincronización de relojes”.

Se observa pues que, según la invención, el proceso de autentificación de la tarjeta que conduce a la liberación de la función en 1 se realiza con la ayuda de al menos dos variables dinámicas de las cuales una es la clave de digitalización Kn (Kna) y la otra puede ser bien sea el número Nn (Nna) de demandas de acceso ya realizadas, o el tiempo T (Ta), o también de los números calculados según una función predeterminada de estas variables. Como se ha descrito anteriormente, tres variables pueden ser utilizadas tales como Kn, (Kna), Nn (Nna) y T (Ta), siendo las variables Nn (Nna) y T (Ta) combinadas por ejemplo por una operación de concatenación.

La clave de digitalización Kn (Kna) propiamente dicha se deriva de una demanda de acceso a otra y es dinámicamente variable en función al valor Nn (Nna) con la cual puede combinarse lógicamente, luego digitalizada para dar lugar a la clave de digitalización Kn+1 (Kna+1) utilizada durante la próxima demanda de acceso.

Según una variante de la invención, se puede considerar una transferencia de datos de la tarjeta 2 a la unidad 3 y el servidor 15, con el fin de que los datos puedan ser tratados en el cumplimiento de la función 1 en la medida naturalmente en que la autorización haya sido dada para ello como continuación del ensayo en 36.

El usuario al formular su demanda de acceso introduce en 38 los datos en la tarjeta con la ayuda de su teclado 6. Estos datos se combinan lógicamente en 39 con el valor concatenado de las dos variables Nn y T, siendo el resultado utilizado como parámetro de entrada del procedimiento de digitalización realizado en 24. En variante, los datos pueden igualmente directamente combinarse con el resultado de la operación de digitalización en 24. Es esencial que la entrada para la operación 24 sea una función de los datos a transferir.

Los datos son igualmente transferidos al servidor 15 por ejemplo por medio del teclado 13 de la interfaz 12 o automáticamente por mediación de las conexiones 10 y 16.

Los datos así recibidos en 38a en el servidor son tratados en él de la misma forma que en la tarjeta 2. En efecto, los datos pueden combinarse mediante una operación lógica en 39a con el valor concatenado de Nn y de T, siendo utilizado el resultado como parámetro de entrada para el proceso de digitalización en 24a. En variante, los datos pueden combinarse directamente con el resultado de la operación de digitalización en 24a o bien los datos pueden constituir otra clave para la operación de cálculo en 24a. Los datos son también comunicados claramente al dispositivo encargado de ejecutar la función 1.

Así, la autenticidad de los datos puede comprobarse comparando las palabras de pase A y Aa que son las dos funciones del valor que representan los datos. La realización de la función 1 recibirá por consiguiente igualmente un rechazo si no existe concordancia entre los datos presentados por los dos lados.

Otros diversos modos de realización serán ahora descritos, haciéndose para algunos de ellos referencia a cambios que se producen en la tarjeta 2, pero se comprenderá que estos mismos cambios se aplican igualmente al servidor 15, pues la tarjeta 2 y el servidor 15 deben poder producir palabras de pase idénticas o concordantes.

La operación 31 ilustrada en las figuras 1 y 3 puede variar en función de T. De igual modo, el algoritmo 33 puede ser cambiado con cada nueva derivación de Kn, como puede serlo el algoritmo utilizado para el cálculo en 24. Por ejemplo, los módulos 24, 24a y 33, 33a pueden almacenar varios algoritmos utilizados de forma distinta en el transcurso de las diferentes operaciones de cálculo de las palabras de pase. Cambios sincronizados deben entonces ser realizados en el servidor en lo que respecta a la función en 31a, y los algoritmos en 24a y 33a.

Además, la función 32 (Figura 3) puede ser diferente de una función OU-EXCLUSIF, tal como una operación ET o cualquier otra operación lógica. La función 32 no es indispensable, pudiendo Nn+1 directamente ser utilizado por el algoritmo en 33 de forma que sea digitalizado por Kn o Q. Por otro lado, Q puede ser sometido con Nn+1 a una operación OU-EXCLUSIF en 32, siendo Kn o Q utilizado como clave de digitalización para la digitalización de la salida producida por la operación lógica en 32.

Otro modo de realización consiste en prever una puerta ET entre los módulos 29 y 30 de la figura 1, constituyendo la salida del módulo 29 una de las entradas de esta puerta ET, estando la otra entrada formada por una señal procedente del servidor 15 y que solo se produce si el módulo 29a crea una salida. Esta señal del servidor 15 puede ser de un tipo cualquiera de señal de comunicación que pasa por una línea telefónica o en modulación por rayos infrarrojos. De esta forma, el módulo 25 en la tarjeta 2 y el módulo 25a en el servidor 15 se incrementarán de forma síncrona. No existirá entonces ninguna pérdida de sincronización de los valores Nn y Nna. Sin embargo, en algunas aplicaciones de la presente invención, una comunicación en retorno del servidor de este tipo a la tarjeta puede no ser deseable.

Otra variante consiste en almacenar los datos en 38 en la memoria de la tarjeta. Por ejemplo, si la tarjeta 2 es una tarjeta bancaria, los datos en 38 podrían ser la situación de una cuenta bancaria, un número de cuenta etc.

La derivación de Kn según las funciones 31 y 31a puede igualmente ser ejecutada como sigue. Kn puede derivarse dos veces para cada cálculo de palabra de pase. Se puede hacerlo por ejemplo antes y después del cálculo de la palabra de pase. Kn puede igualmente rederivarse en paralelo con el cálculo de la palabra de pase. En otras palabras, Kn puede rederivarse durante el cálculo de la palabra de pase, siendo las salidas del módulo 24 y del módulo 24a entonces directamente utilizadas como entradas de los módulos 33 y 33a, respectivamente.

En variante, los valores Nn y T pueden ser directamente introducidos en el módulo 24. Los datos pueden combinarse lógicamente directamente con Nn ó T o también los datos pueden escindirse en dos partes respectivamente combinadas con Nn ó T.

REIVINDICACIONES

1. Sistema de control de acceso o de autentificación de personas y/o de mensajes mediante el cual al menos un usuario puede ser autorizado a acceder a una función de acceso o de autentificación de personas y/o de mensajes, que comprende al menos una primera unidad personalizada (2) para el indicado usuario y al menos una segunda unidad de verificación (3) que controla el acceso a la función;

• la indicada primera unidad (2) comprende:

primeros medios generadores (25, 26, 31) para generar al menos dos variables dinámicas (Nn, T);

primeros medios de cálculo (24) para generar una primera palabra de pase (A) con la ayuda de al menos un primer algoritmo de digitalización que utiliza parámetros de entrada en función de las variables dinámicas generadas en la primera unidad; y

medios (10, 12, 35) para transmitir la indicada primera palabra de pase a la segunda unidad (3);

• comprendiendo la indicada segunda unidad (3):

segundos medios generadores (25a, 26a, 31a) para, en respuesta a una demanda de acceso realizada con la ayuda de una determinada de las indicadas primeras unidades, generar al menos dos variables dinámicas (Nna, Ta) asignadas a esta misma primera unidad determinada;

segundos medios de cálculo (24a) para generar una segunda palabra de pase (Aa) con la ayuda de al menos un segundo algoritmo de digitalización utilizando parámetros de entrada en función de las variables dinámicas (Nna, Ta) generadas en la segunda unidad;

medios (36) para comparar las primera y segunda palabras de pase;

medios para, si existe una coherencia predeterminada entre las palabras de pase, proporcionar una autorización de acceso a la indicada función (1)

caracterizado porque en cada una de las indicadas unidades:

• los indicados primero y segundo algoritmos de digitalización son algoritmos públicos y una al menos de las indicadas variables dinámicas es secreta,

• una al menos de las indicadas variables dinámicas es independiente del tiempo, y

• los indicados primeros y segundos medios generadores (25, 26, 31, 25a, 26a, 31a) están dispuestos para generar sus variables dinámicas de común acuerdo, pero de forma independiente.

2. Sistema de control según la reivindicación 1, **caracterizado** porque los indicados primeros y segundos medios generadores (25, 26, 31, 25a, 31a) comprenden respectivamente terceros y cuartos medios de cálculo (33) para generar al menos una primera de las indicadas variables dinámicas (Kn, Kna) según una función que implica un número de demandas de acceso formuladas por la indicada primera unidad (2) antes de la demanda de acceso en curso.

3. Sistema de control según la reivindicación 2, **caracterizado** porque los indicados terceros y cuartos medios de cálculo (33) generan respectivamente una variable dinámica intermediaria (Z) por combinación lógica de dicho número de demandas de acceso formuladas antes y el valor actual de la indicada primera variable dinámica (Kn, Kna).

4. Sistema de control según la reivindicación 3, **caracterizado** porque los indicados terceros y cuartos medios de cálculo (33) realizan respectivamente, por medio del tercer y cuarto algoritmos, una digitalización de la mencionada variable dinámica intermediaria (Z), constituyendo el resultado de esta digitalización un nuevo valor (Kn+1, Kna+1) de la indicada primera variable dinámica.

5. Sistema de control según la reivindicación 4, **caracterizado** porque los indicados terceros y cuartos medios de cálculo (33) comprenden respectivamente medios para digitalizar la mencionada variable dinámica intermediaria (Z) utilizando la indicada primera variable (Kn, Kna) como clave de digitalización secreta para los indicados tercero y cuarto algoritmos.

6. Sistema de control según la reivindicación 4, **caracterizado** porque los indicados terceros y cuartos medios de cálculo (33) comprenden respectivamente medios para digitalizar la indicada variable dinámica intermediaria con una clave de digitalización (Q) que difiere de la indicada primera variable dinámica y que se utiliza para los indicados tercero y cuarto algoritmos, respectivamente.

7. Sistema de control según la reivindicación 4, **caracterizado** porque los indicados terceros y cuartos medios de cálculo (33) transfieren el resultado de dicha digitalización por los indicados tercero y cuarto algoritmos de digitalización a los indicados primeros y segundos medios de cálculo (24, 24a) respectivamente, como clave de digitalización para los indicados primero y segundo algoritmos.

8. Sistema de control según una cualquiera de las reivindicaciones 2 a 7, **caracterizado** porque los indicados primeros y segundos medios generadores (25, 25a) generan respectivamente una segunda de las indicadas variables dinámicas en función de dicho número de demandas de acceso formuladas (Nn, Nna) y transfieren la indicada segunda variable dinámica a los indicados primeros y segundos medios de cálculo (24, 24a) respectivamente, y porque los indicados primeros y segundos medios de cálculo (24, 24a) digitalizan un dato de entrada que comprende la indicada segunda variable dinámica respectivamente, con la ayuda de los indicados primero y segundo algoritmos de digitalización.

9. Sistema de control según la reivindicación 8, **caracterizado** porque los indicados primeros y segundos medios generadores (26, 26a) generan respectivamente una tercera de las indicadas variables dinámicas en función del tiempo actual (T, Ta) y transfieren la indicada tercera variable dinámica a los indicados primeros y segundos medios de cálculo (24, 24a) respectivamente, y porque los indicados primeros y segundos medios de cálculo (24, 24a) incorporan respectivamente la mencionada tercera variable dinámica (T, Ta) en el mencionado dato de entrada.

10. Sistema de control según la reivindicación 9, **caracterizado** porque los indicados primeros y segundos medios de cálculo (24, 24a) ejecutan respectivamente una concatenación de la mencionada tercera variable y el indicado dato de entrada.

11. Sistema de control según una cualquiera de las reivindicaciones 5 a 10, **caracterizado** porque los indicados tercero y cuarto algoritmos de digitalización son idénticos a los mencionados primero y segundo algoritmos de digitalización.

12. Sistema de control según una cualquiera de las reivindicaciones, 5 a 11, **caracterizado** porque los indicados primeros y segundos medios generadores (25, 25a, 26, 26a, 31, 31a) transfieren respectivamente una primera de las indicadas variables dinámicas

(Kn, Kna) a los mencionados primeros y segundos medios de cálculo (24, 24a) como clave de digitalización para los mencionados primero y segundo algoritmos y generan un dato de entrada (Nn, Nna) que comprende una segunda de las mencionadas variables que representan el número de demandas de acceso formuladas por la indicada primera unidad ante la demanda de acceso en curso, siendo el indicado dato de entrada transferido a los mencionados primeros y segundos medios de cálculo (24, 24a) respectivamente para ser digitalizado por la indicada primera variable dinámica.

13. Sistema de control según la reivindicación 12, **caracterizado** porque los indicados primeros y segundos medios generadores (25, 26, 31, 25, 26a, 31a) comprenden respectivamente terceros y cuartos medios de cálculo para generar una clave de cifrado (Kn, Kna) en función del número de demandas de acceso formuladas.

14. Sistema de control según la reivindicación 13, **caracterizado** porque los indicados terceros y cuartos medios de cálculo (33) comprenden respectivamente medios de memoria (28) y generan, a partir del valor actual (Kn, Kna) de la indicada clave de digitalización, un nuevo valor (kn+1, Kn+1) de esta y memorizan el indicado nuevo valor en los mencionados medios de memoria (28) en lugar del indicado valor actual.

15. Sistema de control según una cualquiera de las reivindicaciones anteriores, **caracterizado** porque la mencionada primera unidad (2) comprende medios (6, 38) para memorizar datos destinados para ser transferidos a la indicada segunda unidad (3) con el fin de poder ser utilizados para realizar la indicada función, porque la mencionada segunda unidad (3) comprende medios (12, 38) para recibir los indicados datos y porque los indicados primeros y segundos medios generadores comprenden medios (39) para transferir los indicados datos respectivamente en los mencionados primeros y segundos medios de cálculo (24, 24a) con el fin de que puedan ser utilizados como una componente de al menos una de las indicadas variables dinámicas a digitalizar.

16. Sistema según una cualquiera de las reivindicaciones 1 a 15, **caracterizado** porque la indicada primera unidad (2) se presenta en forma de un dispositivo electrónico portátil.

17. Sistema de control según la reivindicación 16, **caracterizado** porque comprende medios de comunicación (10) en las indicadas primera y segunda unidades, comprendiendo los mencionados medios de comunicación una conexión telefónica del tipo DTMF y/o una conexión que funciona por rayos infrarrojos.

18. Sistema de control según una cualquiera de las reivindicaciones 1 a 15, **caracterizado** porque comprende un lector de tarjetas previsto en la mencionada segunda unidad (3) y porque la indicada primera unidad (2) se presenta en forma de una tarjeta que puede ser leída por dicho lector con el fin de permitir el intercambio de informaciones entre la mencionada primera unidad (2) y la indicada segunda unidad (3).

19. Sistema de control según una cualquiera de las reivindicaciones 1 a 18, **caracterizado** porque la indicada relación predeterminada entre las palabras de pase es la igualdad.

20. Sistema de control según la reivindicación 9, **caracterizado** porque los indicados primeros y segundos medios de cálculo (24, 24a) aseguran respectivamente el tratamiento de las indicadas segunda y tercera variables (Nn, T, Nna, Ta) para generar el indicado dato de entrada.

21. Sistema de control según una cualquiera de las reivindicaciones 1 a 10, **caracterizado** porque los indicados primero y segundo algoritmos de digitalización son diferentes, pero presentan una relación predeterminada que se refleja en la relación entre las indicadas primera y segunda palabras de pase (A, Aa).

22. Sistema de control de acceso o de autentificación de personas y/o de mensajes mediante el cual particularmente, al menos un usuario puede ser autorizado para acceder a una función de acceso o de autentificación de personas y/o de mensajes, que comprende al menos una primera unidad personalizada para el indicado usuario y al menos una segunda unidad de comprobación que controla el acceso a la función,

comprendiendo la primera unidad:

primeros medios generadores para generar al menos dos variables dinámicas;

primeros medios de cálculo para generar una palabra de pase con la ayuda de al menos un algoritmo de digitalización que utiliza parámetros de entrada de función de las variables; y medios para transmitir la indicada palabra de pase a la segunda unidad;

comprendiendo la indicada segunda unidad:

segundos medios generadores para, en respuesta a una demanda de acceso realizada con la ayuda de una determinada de las indicadas primeras unidades, generar al menos dos variables dinámicas asignadas a esta misma primera unidad determinada;

segundos medios de cálculo para descifrar la indicada palabra de pase con la ayuda de al menos un algoritmo de descifrado que utiliza como clave de descifrado un parámetro de entrada en función de una primera de las indicadas variables dinámicas generadas en la segunda unidad para derivar una variable dinámica que debe corresponder a una de las variables dinámicas generadas en la mencionada primera unidad;

medios de comparación para comparar la indicada variable dinámica derivada por los mencionados segundos medios de cálculo con una segunda de las mencionadas variables dinámicas generadas en la indicada segunda unidad;

medios que, cuando los mencionados medios de comparación observan que existe una relación predeterminada entre la mencionada variable dinámica derivada por los indicados segundos medios de cálculo con la mencionada segunda variable dinámica entre las mencionadas variables dinámicas generadas en la indicada segunda unidad, proporcionan una autorización de acceso a dicha función;

caracterizado porque

los indicados primeros y segundos medios generadores previstos respectivamente en las indicadas primera y segunda unidades están configurados con el fin de proporcionar las mencionadas variables dinámicas de común acuerdo, pero de forma independiente.

FIG. 1

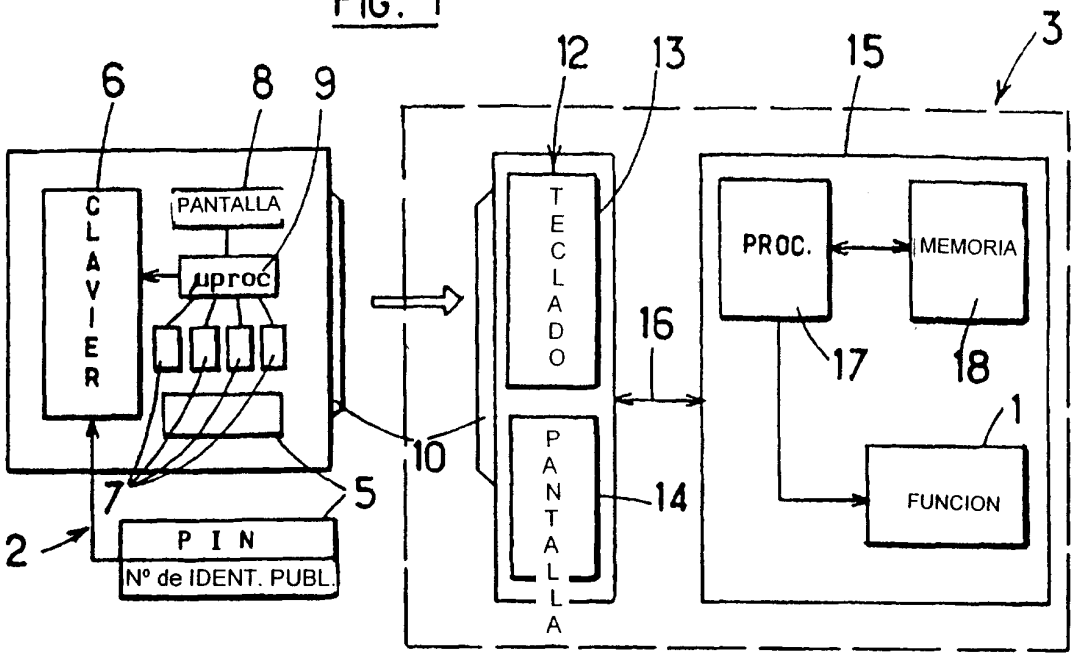

6
8
9
12
13
15
3
CLAVIER
PANTALLA
µproc
TECLADO
PROC.
MEMORIA
16
17
18
1
FUNCION
10
7
5
14
2
PIN
Nº de IDENT. PUBL.
PANTALLA

FIG. 3

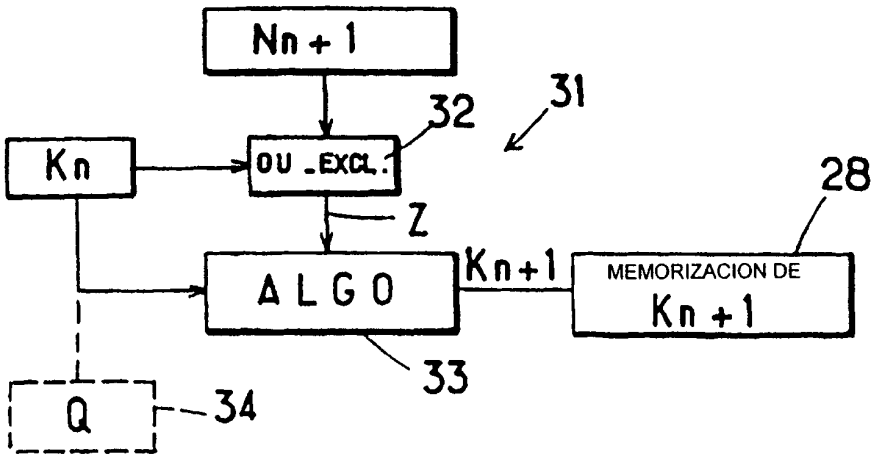
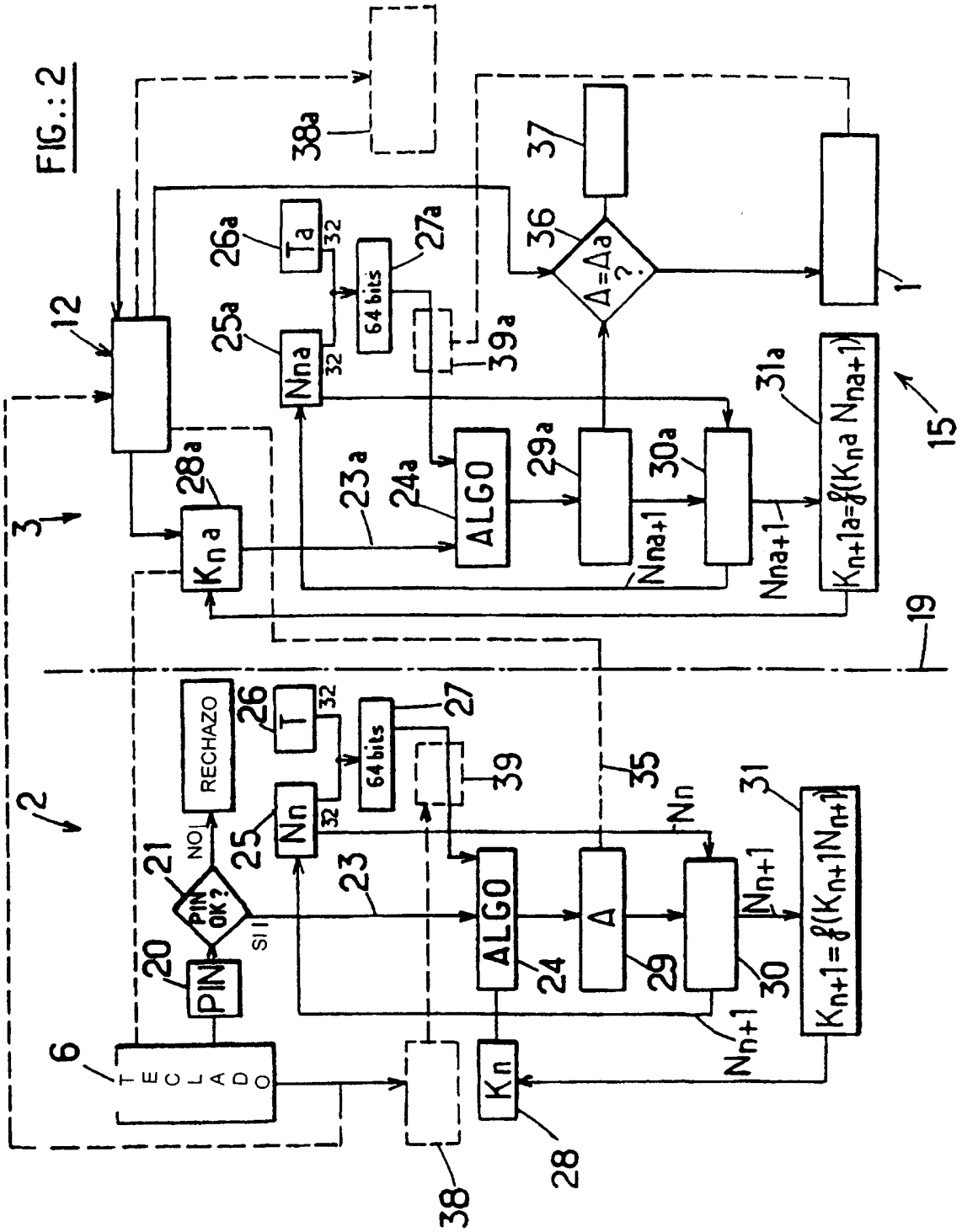

Nn + 1
31
32
Kn
OU - EXCL.
28
Z
Kn+1
ALGO
MEMORIZACION DE
Kn + 1
33
Q
34

FIG.: 2


TECLADO
PIN
PIN OK?
NO
SI
RECHAZO
64 bits
ALGO
Δ
Δ=Δa ?
Kn
Kn+1=f(Kn+1Nn+1)
Kn+1a=f(Kna Nna+1)
1
2
3
6
12
15
19
20
21
23
24
25
26
27
28
29
30
31
35
36
37
38
39
23a
24a
25a
26a
27a
28a
29a
30a
31a
38a
39a