



19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA

11 Número de publicación: **2 276 279**

51 Int. Cl.:
G06F 3/023 (2006.01)
G06F 3/033 (2006.01)
G07F 7/10 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Número de solicitud europea: **04712975 .4**
86 Fecha de presentación : **20.02.2004**
87 Número de publicación de la solicitud: **1599786**
87 Fecha de publicación de la solicitud: **30.11.2005**

54 Título: **Teclado virtual.**

30 Prioridad: **25.02.2003 BR 0300474**

45 Fecha de publicación de la mención BOPI:
16.06.2007

45 Fecha de la publicación del folleto de la patente:
16.06.2007

73 Titular/es: **Banco Itaú S.A.**
Praça Alfredo Egydio de Souza Aranha
100 Torre Itausa
04344-902 Jabaquara, Sao Paulo - SP, BR

72 Inventor/es: **Jongh, R. A. de**

74 Agente: **Curell Suñol, Marcelino**

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).

DESCRIPCIÓN

Teclado virtual.

Campo de la invención

La presente invención se refiere a equipos terminales. Más particularmente, la invención se refiere a equipos terminales que utilizan representaciones visuales de teclados y a un procedimiento para la utilización de los mismos.

Antecedentes de la invención

La creciente omnipresencia de los ordenadores en la vida cotidiana ha puesto de manifiesto que, en el futuro cercano, los negocios se realizarán, en gran parte, en la superautopista electrónica o internet. La facilidad de comprar a través de internet y la utilización del comercio electrónico ya ha empezado a penetrar en nuestras vidas. Las transacciones con tarjetas de crédito y los pedidos de productos en internet ya son algo corriente. No obstante, junto con esta facilidad recién descubierta, la seguridad del sistema, la identificación del usuario y la confirmación de la identificación del usuario siguen siendo preocupaciones principales y legítimas de los usuarios de los sistemas actuales.

Los cajeros automáticos (ATM) y la conexión bancaria a través de internet permiten a los clientes de los bancos efectuar transacciones bancarias con instituciones financieras desde ubicaciones remotas en cualquier lugar del mundo. Los clientes de los bancos acceden a sus cuentas a través de diversas tecnologías (inclusive cajeros automáticos y terminales bancarias de internet) para efectuar transacciones y obtener información confidencial sobre sus cuentas. Como medida de seguridad, la entidad financiera emite un número de identificación personal o PIN para cada cliente del banco. El cliente del banco introduce el PIN en un teclado operativamente conectado con un lector de tarjetas u otro dispositivo que lee la información de identificación del usuario codificada magnéticamente en el cheque o en la tarjeta del cajero automático, tarjeta de crédito o similar. A continuación el PIN y la información de usuario son comunicados a la red de la institución financiera, que comprueba la exactitud de la información. Una vez confirmados el PIN y la información de usuario del cliente del banco, el cliente del banco puede efectuar transacciones con la entidad financiera.

En el mercado actual, existen cuatro requisitos de suprema importancia para garantizar el acceso a un usuario autorizado de un recurso protegido: (1) identificación de usuario autorizado, (2) verificación de la identificación de usuario autorizado, (3) denegación del acceso a usuarios no autorizados y (4) un nivel adecuado de seguridad para proteger el recurso de la utilización no autorizada. Por ejemplo, cuando un usuario (autorizado o no autorizado) desea retirar fondos de un cajero automático, se inserta en el cajero automático una tarjeta emitida por el banco y la "tarjeta" es identificada a través de los datos transferidos desde la banda magnética o el chip electrónico de la tarjeta a una base de datos del sistema. Para comprobar que el usuario es el usuario autorizado de la tarjeta emitida por el banco insertada en el cajero automático, el cajero automático pide al usuario que introduzca un Número de Identificación Personal (PIN) que el cedente de la tarjeta bancaria sólo da al usuario autorizado. Si el PIN introducido por el usuario es idéntico al PIN entregado al usuario autorizado y grabado en

la memoria de bases de datos del sistema, se confirma al usuario como usuario autorizado y puede efectuarse la transacción. La seguridad proporcionada en esta transacción implica la posesión de la tarjeta bancaria entregada al usuario autorizado, el conocimiento del código PIN, un límite superior de solicitud de efectivo y la desactivación de la tarjeta si se introducen en el sistema del cajero automático una serie consecutiva de PIN incorrectos. Teóricamente, este sistema de seguridad es adecuado para evitar que un usuario no autorizado pueda acceder a una cuenta, pero lamentablemente, el acceso no autorizado a recursos protegidos se ha convertido en un problema de miles de millones de dólares. La resolución de este problema radica en la comprensión de los puntos débiles de los sistemas actuales y en el modo de eliminarlos de forma efectiva manteniendo, simultáneamente, su simplicidad, seguridad y eficacia.

Aunque el sistema de seguridad mediante PIN se ha convertido en el estándar para la verificación de un usuario autorizado en sistemas basados o no en tarjeta, posteriormente los usuarios se han visto obligados a recordar diversos códigos PIN para acceder a recursos y servicios protegidos. Este problema de recordar un número excesivo de códigos PIN se ha resuelto a nivel de usuario consignándolos por escrito y llevando una copia en la cartera o en el bolso para fácil referencia. No obstante, este procedimiento compromete directamente la pretendida seguridad proporcionada por el sistema de PIN y podría dar como resultado el fácil acceso no autorizado a las cuentas correspondientes en caso de robo de la cartera o el bolso. A nivel del cedente el problema se ha resuelto permitiendo la utilización de códigos PIN personalizados, por ejemplo diversos PIN, PIN totalmente dinámicos y otras medidas de seguridad superpuestas. De este modo, un usuario autorizado podría eliminar la necesidad de recordar una multitud de códigos PIN haciendo que sean todos idénticos. En otras palabras, los códigos PIN personalizados permiten a un usuario autorizado utilizar un único código PIN para todos los recursos protegidos y, además, elegido personalmente. No obstante si el PIN personalizado resulta fácil de adivinar, como por ejemplo la fecha de nacimiento o el número de teléfono del usuario autorizado, un usuario no autorizado informado podría acceder a todos los recursos protegidos con un simple procedimiento de adivinación inteligente. Actualmente, el mayor inconveniente de los códigos PIN personalizados es el requisito de longitudes idénticas de los códigos con caracteres constantes e invariables, normalmente numéricos. Si se consigue la utilización no autorizada de un recurso observando la introducción del PIN de un usuario autorizado, dicho usuario no autorizado podría acceder de forma inmediata a todos los recursos protegidos por este PIN personalizado. Por lo tanto, los PIN personalizados reducen la seguridad del usuario autorizado debido a la posible ganancia asociada con la posesión ilegal del bolso o cartera del usuario autorizado y el posterior acceso a los recursos protegidos a través del PIN personalizado. La obtención del acceso a internet y a los entornos de comercio electrónico con un nivel incrementado de seguridad ha supuesto un cambio en los requisitos respecto a la longitud del código y a la mezcla de caracteres alfanuméricos del mismo. Al exigir, actualmente, muchos sitios de internet, códigos de acceso de ocho o más caracteres con un mínimo de dos caracteres numéri-

cos, o en vez de ello la emisión de un código arbitrario de longitud variada, los códigos PIN personalizados sólo resuelven el problema de memorizar un número excesivo de PIN durante un corto período de tiempo.

Existen numerosos procedimientos bien conocidos para garantizar la privacidad del PIN de los clientes de los bancos. Por ejemplo, además de los teclados numéricos fijos, los avances en la tecnología de interfaces gráficas de usuario (GUI) permiten que un cliente de un banco pueda introducir su PIN en un teclado o en una pantalla táctil. El cliente del banco puede resguardarse de un potencial defraudador que pueda apropiarse indebidamente de su PIN. Normalmente, los teclados de terminales, que ya son conocidos en la técnica, se visualizan siempre en los terminales en la misma posición y con la misma disposición de las teclas. El resultado es que un defraudador puede observar los movimientos efectuados por un cliente de un banco mientras teclea el PIN y reconocer los números tecleados, ya que las teclas y los números siempre se representan en la misma ubicación en la pantalla del terminal del cajero automático.

Además, algunos defraudadores utilizan el artificio de limpiar la pantalla táctil del cajero automático antes de que un cliente del banco lo utilice. Esto permite la identificación del PIN del usuario a través de sus huellas digitales, que permanecen impresas en la pantalla táctil después de teclear. Cuando el usuario abandona el cajero automático, el defraudador comprueba las huellas digitales y descubre los números pulsados por el usuario, ya que las teclas y los números se visualizan en la misma posición en el terminal del cajero automático.

El teclado virtual de la presente invención corrige estas y otras limitaciones de la técnica anterior mediante la utilización de un teclado virtual que proporciona una imagen de un teclado compacto en una pantalla de un terminal de cajero automático con el fin de evitar fraudes después de teclear la contraseña de seguridad, como se describe en los párrafos anteriores.

Las referencias disponibles de la técnica anterior no dan a conocer, ni siquiera sugieren, una solución para un teclado a prueba de fraudes como la que presenta la presente invención.

El documento WO 98/27518 A da a conocer un teclado a prueba de fraudes para un terminal bancario automático adecuado para evitar que las teclas pulsadas en el teclado por la persona que utiliza el teclado durante una operación bancaria puedan ser detectadas y utilizadas para rastrear el código de identificación personal u otros datos confidenciales del usuario. El teclado comprende medios que varían de forma automática y aleatoria el número y/o el símbolo asociado con cada tecla, entre dos operaciones bancarias sucesivas.

El documento DE 4129202 A1 da a conocer un circuito de protección para un teclado numérico de números de identificación personal que utiliza un número de teclas para introducir un valor PIN, con valores indicados que varía de forma pseudoaleatoria.

Los teclados de ambos documentos WO 98/27518 A y DE 4129202 A1 muestran que en cada nuevo acceso de usuario al terminal electrónico, la ubicación de cada número respecto a cada tecla podría ser diferente. Tales soluciones no evitan que un observador furtivo identifique los dígitos del código de acceso del usuario observando el teclado desde un punto

suficientemente cercano para ver los caracteres representados en el mismo.

El documento WO 02/101531 A da a conocer un teclado para un dispositivo electrónico de mano que comprende una hilera de teclas en el que cada una de dichas teclas representa por lo menos dos caracteres alfanuméricos y los caracteres de cada tecla están situados respecto a los caracteres en teclas adyacentes para formar una plantilla QWERTY o DVORAK.

En el documento WO 02/101531 A, se asigna más de un valor a cada tecla del teclado. El objetivo de esta clase de asignación consiste en minimizar los costes de producción y facilitar el teclado. Según dicho documento, la configuración y los caracteres asociados con cada tecla permanecen constantes. Por lo tanto, un observador furtivo sólo necesita identificar la secuencia de teclas pulsadas por el usuario para defraudar el acceso del usuario a los servicios electrónicos.

Con esta configuración de teclado no es necesario conocer los números que componen el código de acceso de usuario, sino solamente la secuencia de teclas pulsadas por el usuario para conseguir acceder a los servicios electrónicos del usuario.

El documento EP 0844778 A da a conocer un radioteléfono que comprende una interfaz de usuario y una unidad de control conectada a la interfaz de usuario, comprendiendo la interfaz de usuario una pantalla y un teclado que presenta por lo menos una tecla operativa cuya función se controla mediante la unidad de control y se visualiza en una zona predeterminada de la pantalla. La función de dicha por lo menos una tecla operativa se visualiza en una zona determinada de la pantalla. El radioteléfono puede asumir diversos estados en los cuales dicha por lo menos una tecla operativa puede realizar un grupo de acciones predeterminadas asociadas con el estado correspondiente. La unidad controladora visualiza uno de dichos grupos de acciones como función por defecto en la zona predeterminada de la pantalla.

El documento EP 0844778 A da a conocer una tecla inteligente, cuya funcionalidad varía según el estado del radioteléfono. Correspondientemente, el resultado generado al pulsar la tecla mientras el teléfono se está utilizando en una llamada es diferente de la originada, por ejemplo, al pulsar la tecla cuando el teléfono no se está utilizando.

No obstante, para un estado determinado del teléfono, la funcionalidad asociada con cada tecla permanece invariable. Al haber únicamente una funcionalidad asociada a cada tecla, un observador furtivo que observe el teclado desde un punto suficientemente cercano puede identificar el valor asociado con la tecla pulsada por el usuario.

Sumario de la invención

Según una forma de realización de la invención, se proporciona un procedimiento para proporcionar acceso a servicios electrónicos a través de un código de acceso seguro. El procedimiento comprende las etapas siguientes: disposición de un teclado que comprende un número predeterminado de teclas, las cuales se utilizan para introducir un código de acceso seguro. El procedimiento comprende las etapas siguientes: asociación de por lo menos dos variables con cada tecla individual, pudiendo cambiar el valor de una o más de estas variables de un acceso a otro; visualización de las variables para el usuario; selección, por el usuario, de cada tecla que corresponde a cada variable de este código de acceso; comparación de los

valores asociados con cada tecla seleccionada con un código almacenado en una base de datos; y autorización al usuario del acceso a los servicios electrónicos, si los valores asociados con las teclas, seleccionadas secuencialmente por el usuario, coinciden con el código de acceso almacenado. El teclado de la presente invención puede ser virtual, visualizándose a través de una interfaz de usuario gráfica, o físico.

Según otra forma de realización de la invención, se proporciona un teclado que comprende un número predeterminado de teclas para introducir un código de acceso; caracterizado porque están asociadas a cada tecla por lo menos dos variables, seleccionando el usuario las teclas basándose en las variables correspondientes a alguna parte del código de acceso del usuario, pudiendo cambiar las variables de un acceso a otro. El teclado puede ser virtual, visualizándose a través de una interfaz gráfica de usuario, o físico.

Según otra forma de realización de la invención, se proporciona un terminal de acceso seguro para proporcionar acceso a servicios electrónicos a través de un código de acceso seguro, comprendiendo el terminal una interfaz gráfica de usuario, que permite a un usuario acceder de forma segura a información electrónica, y un teclado, caracterizado porque cada tecla del teclado presenta por lo menos dos variables, asignadas entre un grupo de combinaciones posibles de variables, y las variables se encuentran asociadas con cada una de las teclas de modo que el usuario adquiere el derecho a efectuar determinadas transacciones seleccionando teclas a las cuales han sido asignadas variables que corresponden a un código secreto.

Breve descripción de los dibujos

En los dibujos adjuntos, que forman una parte de la presente memoria y deben considerarse conjuntamente con la misma, se ilustra la presente invención a título de ejemplo no limitativo, utilizando las mismas referencias numéricas para los mismos elementos, en los cuales:

la figura 1 ilustra un ejemplo de un teclado virtual según una forma de realización de la invención;

la figura 2 ilustra otro ejemplo de un teclado virtual, según una forma de realización de la invención;

la figura 3 ilustra otro ejemplo más de un teclado virtual, según una forma de realización de la invención;

la figura 4 es otra ilustración de un teclado virtual, según una forma de realización de la invención;

la figura 5 es otra forma de realización de un teclado virtual, según una forma de realización de la invención;

la figura 6 ilustra un diagrama de flujo de un ejemplo de un procedimiento según una forma de realización de la invención; y

la figura 6(a) es una ilustración de un listado de caracteres según una forma de realización de la invención.

Descripción detallada de la invención

En la siguiente descripción detallada, se establecen numerosos detalles específicos para proporcionar una comprensión profunda de la invención. No obstante, resultará evidente para los expertos en la materia que estos detalles específicos no son necesarios para la práctica de la invención. En otros ejemplos, estructuras, interfaces y procesos bien conocidos no se muestran para no ocultar innecesariamente la invención.

El procedimiento de la presente invención, que

puede implementarse mediante software, consiste en la generación de un teclado virtual, preferiblemente como el ilustrado en las figuras 1 a 6, en un monitor de un terminal de cajero automático o cualquier otro terminal de ordenador, por ejemplo, un ordenador personal o un ordenador portátil.

La figura 1 ilustra un teclado virtual 100, según una forma de realización de la invención. El teclado virtual 100 presenta cinco teclas 105-125, aunque los expertos en la materia podrán apreciar fácilmente que la figura no significa una limitación del ámbito de la invención y que puede utilizarse cualquier número de teclas. A cada tecla 105-125 del teclado virtual 100 se encuentran asociados diversos caracteres alfanuméricos, que se visualizan relativamente cerca de la tecla 105-125. Estos caracteres son preferiblemente números, como ilustra la figura, pero los expertos en la materia podrán apreciar que también pueden ser combinaciones de letras, números o símbolos. Además, los expertos en la materia podrán apreciar que aunque la figura ilustre dos caracteres asociados con cada tecla, esto no significa una limitación de la invención, sino que el objetivo es meramente ilustrativo.

Como muestra la figura 1, los caracteres alfanuméricos 7 y 4 se asignan a la primera tecla 105, los caracteres alfanuméricos 2 y 9 se asignan a la segunda tecla 110, los caracteres alfanuméricos 1 y 3 se asignan a la tercera tecla 115, los caracteres alfanuméricos 6 y 5 se asignan a la cuarta tecla 120 y los caracteres alfanuméricos 8 y 0 se asignan a la quinta tecla 125. Correspondientemente, para introducir una contraseña (por ejemplo 723604), el usuario pulsa de la primera tecla 105 a la quinta tecla 125 y vuelve a pulsar la primera tecla 105. Los expertos en la técnica podrán apreciar que pueden existir diversos cambios de valores basados en las teclas pulsadas.

Como ilustra la figura, hay más de un número asignado a cada tecla. Por lo tanto, cuando un usuario pulsa teclas asociadas con elementos de la contraseña, se efectúa un proceso para determinar cuál de los valores posibles introducidos es la contraseña correcta. Por ejemplo, si el usuario pulsa teclas para introducir 723604, surgen diversas combinaciones de contraseñas posibles (por ejemplo 491587). El sistema determina la contraseña posible utilizando una contraseña almacenada o una contraseña cifrada. Por ejemplo, supongamos que una contraseña de usuario secreta es 723604, y el teclado numérico está configurado como muestra la figura 1. Si la contraseña está almacenada en un ordenador central, se compara la contraseña almacenada y los valores introducidos por el usuario. El sistema sabe que el usuario ha pulsado la primera tecla indicando que el primer valor de la contraseña es 7 ó 4. El valor 7 y, a continuación, el valor 4 se comparan con la contraseña almacenada y se retiene el valor que corresponde a la misma. Se toma una decisión por cada dígito de la contraseña, resolviendo la distinción entre diferentes contraseñas posibles. Si no existe coincidencia, significa que se ha introducido una contraseña incorrecta y se notifica al usuario. Otra técnica implica la posibilidad de que el ordenador central no tenga acceso a la contraseña. Cuando el usuario abre una cuenta con una entidad financiera, elige una contraseña, que se cifra, y la entidad financiera almacena el valor cifrado de la contraseña. Cuando el usuario pulsa las teclas asociadas con la contraseña, el sistema analiza todas las combinaciones posibles de caracteres utilizan-

do el mismo procedimiento de cifrado, (por ejemplo triple DES) y compara los resultados del valor cifrado almacenado con las combinaciones de los valores cifrados.

Estos caracteres alfanuméricos pueden reproducirse alrededor de cada tecla para ayudar a su visualización, no obstante, los expertos en la materia podrán seleccionar otras posiciones de las teclas, por ejemplo representarlos dentro de cada una de las teclas virtuales 105-125.

Según la invención, el sistema comprende múltiples teclas y diversos caracteres asignados a las teclas. Estas características permiten a un usuario diversas capas de protección contra observadores furtivos u otros tipos de fraude. Por ejemplo, con diversos caracteres asignados a cada tecla, la cantidad de combinaciones que debe deducir un eventual observador furtivo resulta considerable. Si un usuario teclea cada una de las teclas durante el proceso de introducción de su número PIN, el observador furtivo debe determinar tanto el número que el usuario pretende introducir como la secuencia adecuada de los botones, ya que la combinación de números por tecla cambiará cuando el defraudador acceda al terminal. Por lo tanto, la invención proporciona una doble capa protectora contra actividades fraudulentas.

Cuando un usuario utiliza el terminal electrónico, se visualiza el teclado virtual 100 en una pantalla táctil (no mostrada). Los expertos en la materia reconocerán que existen numerosos procedimientos de visualización de información para un usuario y que el tipo de visualización no significa ninguna limitación de la invención.

El usuario identifica los caracteres generados, que se asignan a cada una de las cinco teclas, y se pulsan las teclas que corresponden a los valores del PIN para disponer de acceso a las transacciones electrónicas.

Las teclas 105-125 junto con los caracteres asociados se consideran como una "pantalla". La pantalla puede cambiar de usuario a usuario o después de un período de tiempo predeterminado. Una pantalla puede asignarse a un usuario durante un cierto período de tiempo. Los expertos en la materia podrán apreciar los diversos tipos de posibilidades que pueden ofrecerse. La única variable de cada pantalla son los valores de los caracteres asignados a cada tecla. Como puede apreciarse en las figuras 1 y 2, la única diferencia entre las figuras son los valores asignados a cada tecla. Para cada pantalla se disponen un total de diez caracteres asignados a las teclas. El ordenador central de la entidad financiera almacenaría todas las combinaciones posibles de los diez caracteres que no presentan caracteres repetidos (por ejemplo, no dos números 3, porque ello generaría excesiva confusión entre usuarios y al descifrar la contraseña). La figura 6(a) ilustra un ejemplo de las combinaciones de valores. Una vez autenticada la tarjeta de usuario emitida por el banco, se asigna una pantalla a este usuario para un período de tiempo predeterminado.

Normalmente, cuando un nuevo usuario utiliza el terminal, se visualiza una nueva pantalla con una nueva combinación de caracteres y las teclas virtuales permanecen siempre en la misma posición. La figura 2 ilustra un nuevo teclado virtual 200 con una nueva combinación de caracteres, según una forma de realización de la invención. El teclado virtual 200 dispone cinco teclas 205-225; no obstante, los expertos en la materia podrán apreciar fácilmente que la figura no

significa una limitación del ámbito de la invención y que puede utilizarse cualquier número de teclas.

Como podrá apreciarse en las figuras 3 y 4, la disposición de las teclas del teclado virtual 200 puede personalizarse según las preferencias de la mayoría de usuarios. Como se ilustra, la única diferencia entre la figura 1 y la figura 2 es la combinación de caracteres asignados a cada una de las cinco teclas. Por ejemplo, en la figura 1, las teclas virtuales 105-125 que muestran la figura de una mano junto al texto "clicar aquí" se visualizan en la misma posición, pero los números representados alrededor de cada una de las teclas virtuales varían de un usuario a otro, como puede apreciarse en la figura 2, donde la disposición de las teclas es la misma, pero la combinación de números es diferente. Por lo tanto, las figuras 1 y 2 muestran ejemplos de teclados virtuales que se visualizarían para dos usuarios distintos.

La figura 3 ilustra un teclado virtual 300 según una forma de realización de la invención. El teclado virtual 300 presenta cinco teclas 305-325; no obstante, los expertos en la materia podrán apreciar fácilmente que la figura no significa una limitación del ámbito de la invención y que puede utilizarse cualquier número de teclas. Parejas de caracteres asociados con las teclas 305-325 del teclado 300 se encuentran dispuestas alrededor de cada tecla 305-325 o dentro de la misma. Estos caracteres son preferiblemente números, como ilustra la figura, pero los expertos en la materia podrán apreciar que también pueden ser combinaciones de letras o de letras y números. Como muestra la figura, las teclas 305-325 se visualizan en una configuración horizontal a lo largo de la pantalla.

La figura 4 también ilustra una configuración horizontal del teclado 400. No obstante, la figura 4 ilustra un teclado 400 en el cual los caracteres asignados a cada tecla 405-425 han sido reconfigurados para visualizarlos para un nuevo usuario.

La figura 5 ilustra una forma de realización alternativa de la invención. La figura ilustra un teclado 500 que presenta las teclas en el exterior de la pantalla. La pantalla muestra diversos caracteres que representan elementos de un número de identificación personal (PIN) y una casilla que muestra los caracteres seleccionados. Las teclas se encuentran alineadas de forma que se asocian con diversos caracteres. Por ejemplo, la primera tecla (en la parte superior izquierda) está asociada con los caracteres A, C y D. Los caracteres A, C y D se muestran en la pantalla. La pantalla ilustra los caracteres y una casilla que indica el número de caracteres que han sido pulsados. El usuario selecciona el botón correspondiente al elemento del PIN y en la casilla aparece un número o un carácter.

La figura 6 ilustra un diagrama de flujo de un procedimiento 600 para acceder a un terminal seguro, según una forma de realización de la invención. En la etapa 605, un usuario se acerca al terminal, decide efectuar por lo menos una transacción bancaria a través del terminal e inserta una tarjeta emitida por un banco en el terminal.

En la etapa 610, el terminal lee la información de la tarjeta emitida por el banco y la transmite al ordenador del banco (no mostrado). Normalmente, la información se cifra conforme a un procedimiento de cifrado bien conocido. El ordenador del banco determina y registra que el usuario asociado con la tarjeta bancaria está utilizando el terminal.

En la etapa 615, el sistema determina el teclado que debe visualizarse para el usuario. Al seleccionar el usuario una tecla a la cual corresponden por lo menos dos caracteres, hay un cierto número de caracteres que pueden ser asociados con cada tecla. Por ejemplo, existen dos caracteres asociados con cada tecla (como muestra la figura 1). El ordenador almacena listas predeterminadas de caracteres de modo que no se asigne un mismo número dos veces a la misma tecla. Cada "pantalla" contiene dos columnas de números entre 0 y 9. Hay 945 combinaciones posibles de pantallas existentes.

En la etapa 620, el ordenador del banco seleccio-

na una pantalla aleatoriamente y visualiza la pantalla para el usuario, de forma similar a las figuras 1 y 2.

En la etapa 625, el usuario introduce la contraseña secreta. El usuario pulsa las teclas asociadas con los números de la contraseña secreta.

En la etapa 630, el terminal cifra los datos asociados con la contraseña secreta y los transmite al ordenador del banco. Los datos se cifran de forma conocida por los expertos en la materia.

En la etapa 635, el ordenador del banco comprueba la información de la contraseña de usuario secreta y permite al usuario efectuar transacciones bancarias predeterminadas con el banco.

15

20

25

30

35

40

45

50

55

60

65

REIVINDICACIONES

1. Procedimiento para proporcionar acceso a servicios electrónicos a través de un código de acceso seguro, que comprende las etapas siguientes:

- (i) disponer un teclado (100, 200, 300, 400, 500) que comprende un número predeterminado de teclas, las cuales se utilizan para introducir un código de acceso seguro,

caracterizado porque comprende además las etapas siguientes:

- (ii) asociar por lo menos dos variables con cada tecla individual, en el que el valor de una o más de estas variables puede cambiar de un acceso a otro;
- (iii) visualizar las variables para el usuario;
- (iv) seleccionar, por parte del usuario, cada tecla que corresponde a cada variable de este código de acceso;
- (v) comparar los valores asociados con cada tecla seleccionada con un código almacenado en una base de datos; y
- (vi) autorizar al usuario al acceso a los servicios electrónicos, si los valores asociados con las teclas, seleccionadas secuencialmente por el usuario, coinciden con el código de acceso almacenado.

2. Procedimiento según la reivindicación 1, **caracterizado** porque en la etapa (v) se retiene cada valor asociado con cada tecla seleccionada que coincide con la parte correspondiente del código de acceso del usuario; y porque en la etapa (vi), si los valores retenidos por las teclas, seleccionadas secuencialmente por el usuario, coinciden con el código de acceso almacenado, se autoriza el acceso del usuario a los servicios electrónicos.

3. Procedimiento según cualquiera de las reivindicaciones 1 ó 2, **caracterizado** porque las variables de la etapa (ii) cambian después de un período de tiempo predeterminado.

4. Procedimiento según cualquiera de las reivindicaciones 1 a 3, **caracterizado** porque el teclado es un teclado físico (500).

5. Procedimiento según cualquiera de las reivindicaciones 1 a 3, **caracterizado** porque el teclado es un teclado virtual (100, 200, 300, 400).

6. Procedimiento según la reivindicación 5, **caracterizado** porque el teclado virtual se visualiza a través de una interfaz gráfica de usuario.

7. Procedimiento según cualquiera de las reivindicaciones 5 ó 6, **caracterizado** porque el teclado virtual comprende cinco teclas (105, 110, 115, 120, 125; 205, 210, 215, 220, 225; 305, 310, 315, 320, 325; 405, 410, 415, 420, 425).

8. Procedimiento según cualquiera de las reivindicaciones 1 a 7, **caracterizado** porque cuando las teclas seleccionadas y el código almacenado no coinciden se notifica al usuario.

9. Procedimiento según cualquiera de las reivindicaciones 1 a 8, **caracterizado** porque los servicios electrónicos son funciones bancarias.

10. Procedimiento según cualquiera de las reivindicaciones 1 a 9, **caracterizado** porque las variables son caracteres alfanuméricos.

11. Procedimiento según cualquiera de las reivindicaciones 1 a 9, **caracterizado** porque las variables son números.

12. Procedimiento según cualquiera de las reivindicaciones 1 a 9, **caracterizado** porque las variables son letras.

13. Procedimiento según cualquiera de las reivindicaciones 1 a 9, **caracterizado** porque las variables son una combinación de letras y números.

14. Procedimiento según cualquiera de las reivindicaciones 1 a 9, **caracterizado** porque las variables son símbolos.

15. Procedimiento según cualquiera de las reivindicaciones 1 a 14, **caracterizado** porque se selecciona y visualiza un grupo de variables para cada usuario.

16. Procedimiento según la reivindicación 15, **caracterizado** porque el grupo de variables se genera con una secuencia predeterminada.

17. Procedimiento según la reivindicación 15, **caracterizado** porque el grupo de variables se asocia con las teclas conforme a una secuencia aleatoria de combinación de valores.

18. Procedimiento según cualquiera de las reivindicaciones 1 a 17, **caracterizado** porque el procedimiento se implementa en un terminal de acceso seguro.

19. Procedimiento según cualquiera de las reivindicaciones 1 a 18, **caracterizado** porque se visualiza un teclado predeterminado para un usuario.

20. Procedimiento según cualquiera de las reivindicaciones 1 a 19, **caracterizado** porque comprende además la etapa de inserción, en un terminal, de una tarjeta emitida por un banco, para ejecutar una transacción (605).

21. Procedimiento según cualquiera de las reivindicaciones 1 a 20, **caracterizado** porque comprende además la etapa de solicitud del código de acceso del usuario (620).

22. Procedimiento según la reivindicación 20, **caracterizado** porque comprende además las etapas siguientes:

transmitir la información de la tarjeta a un servidor (610);

comprobar la autenticidad de la tarjeta emitida por el banco; y

determinar el teclado que debe visualizarse para el usuario (615).

23. Procedimiento según cualquiera de las reivindicaciones 1 a 22, **caracterizado** porque comprende además las etapas siguientes:

iv.a) encriptar los datos del código de acceso del usuario; y

iv.b) transmitir los datos a un servidor (630).

24. Teclado (100, 200, 300, 400, 500) para proporcionar acceso a servicios electrónicos a través de un código de acceso seguro, que comprende:

un número predeterminado de teclas para introducir un código de acceso (105, 110, 115, 120, 125; 205, 210, 215, 220, 225; 305, 310, 315, 320, 325; 405, 410, 415, 420, 425; 500);

estando el teclado **caracterizado** porque están asociadas a cada tecla por lo menos dos variables, las cuales se visualizan para el usuario, en el que el usuario selecciona secuencialmente las teclas que corresponden a todas las variables de este código de acceso, pudiendo cambiar las variables de un acceso a otro, en

el que los valores asociados con cada tecla seleccionada se comparan con un código almacenado en una base de datos y se permite el acceso a los servicios electrónicos al usuario, si los valores asociados con las teclas, seleccionadas secuencialmente por el usuario, coinciden con el código de acceso almacenado.

25. Teclado según la reivindicación 24, **caracterizado** porque las variables pueden cambiar después de un período de tiempo predeterminado.

26. Teclado según cualquiera de las reivindicaciones 24 a 25, **caracterizado** porque el teclado es un teclado virtual.

27. Teclado según la reivindicación 26, **caracterizado** porque el teclado virtual se visualiza a través de una interfaz gráfica de usuario.

28. Teclado según cualquiera de las reivindicaciones 24 a 25, **caracterizado** porque las teclas son físicas.

29. Teclado según la reivindicación 28, **caracterizado** porque las teclas están situadas fuera de la pantalla.

30. Teclado según la reivindicación 29, **caracterizado** porque las variables se visualizan en la pantalla.

31. Teclado según cualquiera de las reivindicaciones 24 a 30, **caracterizado** porque comprende cinco teclas.

32. Teclado según cualquiera de las reivindicaciones 24 a 31, **caracterizado** porque las variables son caracteres alfanuméricos.

33. Teclado según cualquiera de las reivindicaciones 24 a 31, **caracterizado** porque las variables son números.

34. Teclado según cualquiera de las reivindicaciones 24 a 31, **caracterizado** porque las variables son letras.

35. Teclado según cualquiera de las reivindicaciones 24 a 31, **caracterizado** porque las variables son una combinación de letras y números.

36. Teclado según cualquiera de las reivindicaciones 24 a 31, **caracterizado** porque las variables son símbolos.

37. Teclado según cualquiera de las reivindicaciones 24 a 36, **caracterizado** porque se selecciona y visualiza un grupo de variables para cada usuario.

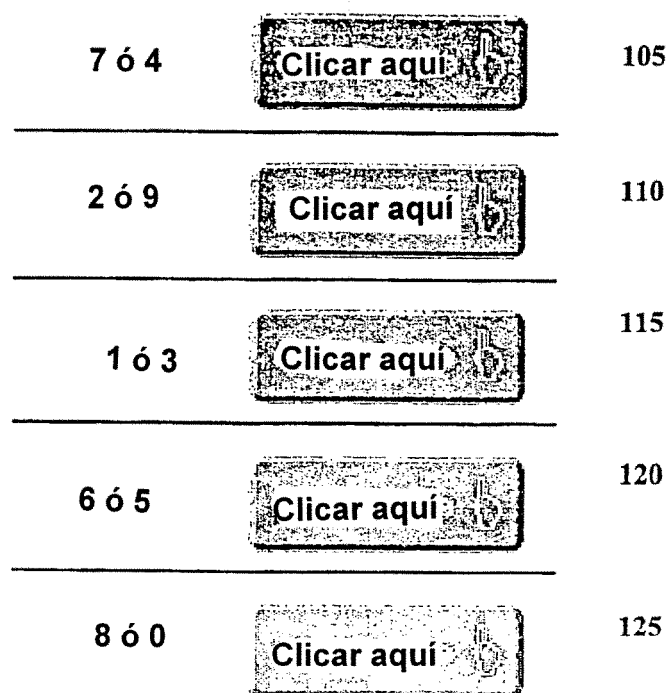
38. Teclado según la reivindicación 37, **caracterizado** porque el grupo de variables se genera con una secuencia predeterminada.

39. Teclado según la reivindicación 37, **caracterizado** porque el grupo de variables se asocia con las teclas conforme a una secuencia aleatoria de combinación de valores.

40. Teclado según cualquiera de las reivindicaciones 24 a 39, **caracterizado** porque se visualiza un teclado predeterminado para un usuario.

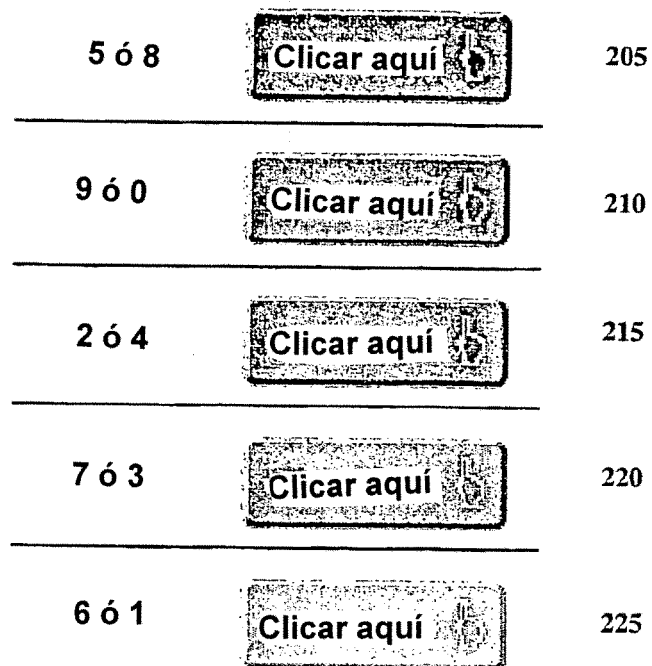
41. Teclado según cualquiera de las reivindicaciones 24 a 40, **caracterizado** porque el procedimiento se implementa en un terminal de acceso seguro.

42. Terminal de acceso seguro para proporcionar acceso a servicios electrónicos a través de un código de acceso seguro, comprendiendo el terminal una interfaz gráfica de usuario, que permite a un usuario acceder de forma segura a información electrónica, y un teclado como el que se define en cualquiera de las reivindicaciones 24 a 41.



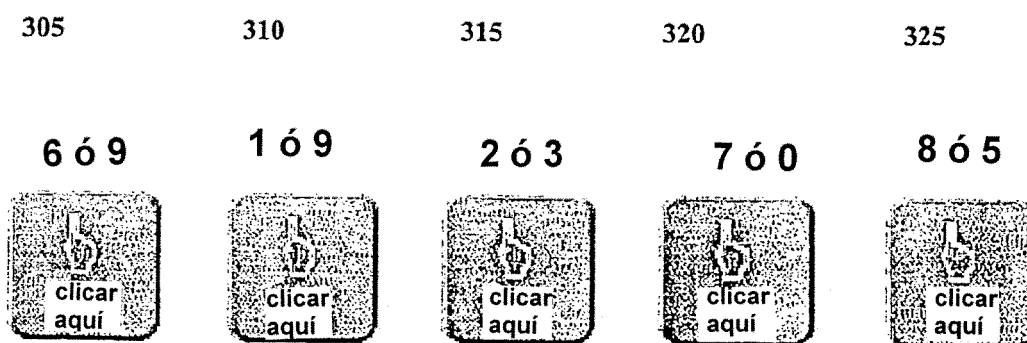
100

FIG. 1



200

FIG. 2



300

FIG. 3

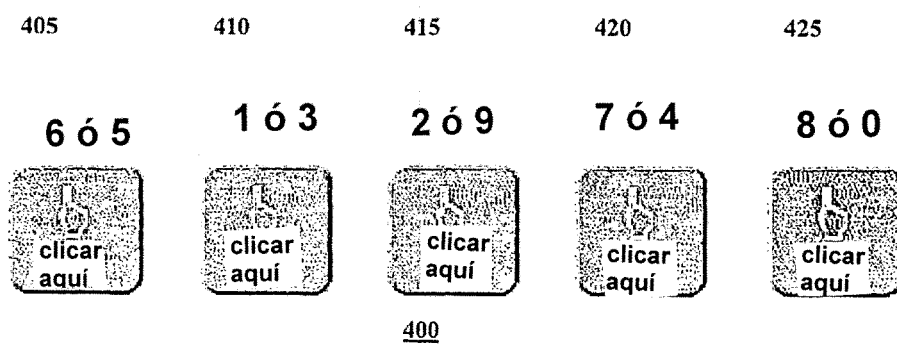


FIG. 4

Introducir contraseña de 3 letras:

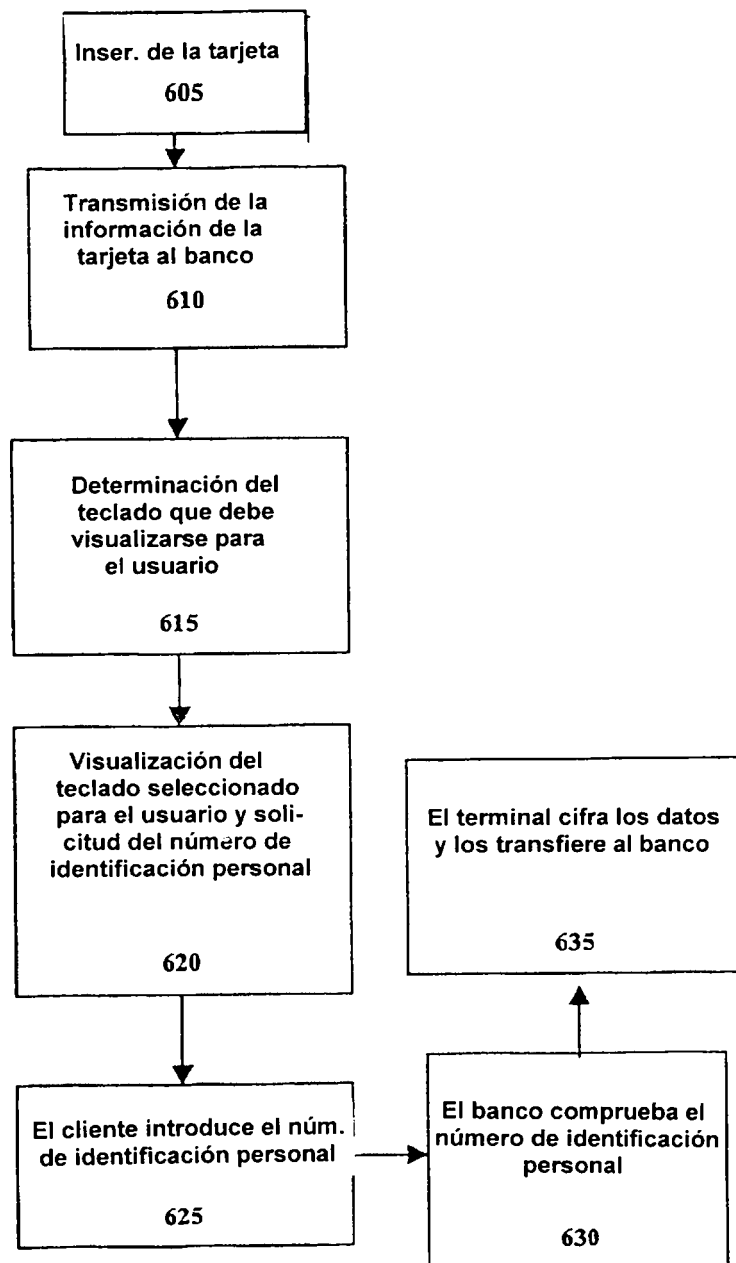
	A,D,C,	R, Q	
	W,J, Z, K, B	P,G,S	
	E,I, V	T,N, X,U	
	F, L	O, M	

500

FIG. 5

FIG. 6

600



0 5		0 6		0 7		0 8		0 9
1 6		1 7		1 8		1 9		1 5
2 7		2 8		2 9		2 5		2 6
3 8		3 9		3 5		3 6		3 7
4 9		5 5		4 6		5 7		5 8

FIG. 6(a)