(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 686 559**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **29.04.2013 PCT/GB2013/051088**

(87) Fecha y número de publicación internacional: **05.12.2013 WO13178982**

(96) Fecha de presentación y número de la solicitud europea: **29.04.2013 E 13722803 (7)**

(97) Fecha y número de publicación de la concesión europea: **06.06.2018 EP 2856380**

(54) Título: **Método y sistema para una identificación de usuario segura**

(30) Prioridad:

28.05.2012 GB 201209404
15.06.2012 US 201261660395 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.10.2018

(73) Titular/es:

SWIVEL SECURE LIMITED (100.0%)
Equinox 1 Audby Lane
Wetherby LS22 7RD, GB

(72) Inventor/es:

RUSSELL, CHRIS

(74) Agente/Representante:

SÁEZ MAESO, Ana

DESCRIPCIÓN

Método y sistema para una identificación de usuario segura

La presente invención se refiere a un método y un sistema para autentificación de un usuario en un sistema informático por medio de un número de identificación personal (NIP) o código de acceso.

Antecedentes

En el mundo actual, las transacciones financieras y otras se realizan a menudo por medio de Internet, con los bancos y otras instituciones que proporcionan un acceso en línea a una cuenta basada en la web para sus clientes. Con el fin de acceder a su cuenta, un cliente típicamente se identifica en una página web introduciendo un identificador de cliente único (que no es secreto), y posteriormente introduciendo un NIP o código de acceso o contraseña (que se debe mantener en secreto y es conocido únicamente por el cliente y el sistema informático al cual el cliente está intentando acceder).

Una debilidad de los sistemas existentes es que el ordenador que está siendo utilizado por el cliente para acceder al sistema informático del banco puede haber sido infectado con un software malicioso, en particular, un registrador de pulsaciones de teclado, que puede grabar las pulsaciones de teclado hechas por el cliente cuando accede a su cuenta. El grabador de pulsaciones de teclado puede entonces transmitir las pulsaciones de teclado grabadas a una tercera parte, que puede acceder a la cuenta de banco del cliente sin dificultad utilizando el identificador de cliente único y la combinación de NIP/código de acceso/contraseña.

Otro problema es el de la observación furtiva, en el que una persona que está de pie cerca de otra persona que utiliza un cajero automático, un cerrojo de puerta con código de entrada o un teclado numérico de PVE (punto electrónico de venta) en una tienda puede fácilmente determinar un NIP que se está introduciendo. Es también conocido para los ladrones manipular los cajeros automáticos instalando clonadores de tarjetas y pequeñas video cámaras para capturar la entrada de NIP, o para comerciantes deshonestos hojear las tarjetas y anotar los códigos NIP de los clientes cuando éstos son introducidos en teclados numéricos de PVE.

Se han realizado esfuerzos para reducir este problema, por ejemplo requiriendo que el cliente no use pulsaciones de teclado para introducir su NIP, sino en su lugar emplear interfaces basadas en pantallas que utilizan un rato, un puntero y menús desplegables, o una interfaz de pantalla táctil. Aunque el uso de un ratón y un puntero, por ejemplo, puede superar las amenazas impuestas por los registradores de pulsaciones de teclado, hay programas de software malicioso más sofisticados que pueden detectar la posición de un puntero en una pantalla, y por tanto pueden deducir los datos que están siendo introducidos si se emplea una interfaz con un teclado numérico virtual fijo.

Ejemplos de interfaces mejorada son conocidos a partir del documento US 6,549,194, donde se proporciona un dispositivo para introducir un NIP con una pantalla táctil, y en donde se muestra un teclado numérico en la pantalla táctil para un usuario para introducir su NIP. Con el fin de obstaculizar a los registradores de pulsaciones de teclado o un software malicioso similar, el monitor de pantalla táctil está configurado para cambiar la configuración del teclado numérico entre usos, de manera que el software malicioso no será capaz de determinar qué número es representado en cualquiera de las transacciones dadas por la porción de la pantalla táctil que es activada.

El documento US 2004/0225601 da a conocer un dispositivo de cajero automático o PV (punto de venta) donde un usuario inserta su tarjeta de banco y después introduce un NIP de la manera usual. El usuario es entonces emplazado a introducir un segundo NIP o código de seguridad, esta vez utilizando teclas del cajero automático o PV que son normalmente utilizadas para introducir números. Se muestran instrucciones de la pantalla para indicar al usuario cual es teclas corresponden a cuales números.

El documento US 7,992,007 presenta un teclado numérico virtual en una pantalla de visualización para qué un usuario introduzca un NIP haciendo clic en las teclas virtuales con un puntero controlado por un ratón. El tamaño, disposición y geometría del teclado numérico y de las teclas que componen el teclado se cambian cada vez para obstaculizar al software malicioso que detecta la posición de un puntero en una pantalla.

Es conocido a partir del documento US 7,392,388 a nombre del presente solicitante (cuyo contenido completo es incorporado por la presente en la presente solicitud a modo de referencia) para proporcionar un sistema de verificación de identidad en el cual un usuario puede identificarse el mismo en un ordenador de un banco o un comerciante o similares aplicando un protocolo relativamente simple a una cadena de desafíos recibida del ordenador del banco o comerciante mediante un mensaje SMS, o un sitio web seguro mediante una conexión con un protocolo seguro de transferencia de hipertexto (HTTPS), o una comunicación por correo electrónico o similares. El usuario está en posesión de un código numérico corto, análogo a un número de identificación personal (NIP) típico utilizado comúnmente como una medida de seguridad junto con una tarjeta de crédito o de débito. Este código numérico, que puede tener una longitud de cuatro dígitos (aunque se pueden utilizar otras longitudes), es conocido únicamente por el usuario y el banco o el emisor de la tarjeta. El usuario aplica el código numérico a una cadena de seguridad pseudo-aleatoria emitida por el banco o el emisor de la tarjeta, seleccionando caracteres de la cadena de seguridad, en una base de posición determinada por cada dígito del código numérico, tomados en orden. Por ejemplo, donde un código del usuario es “2473”, y la cadena de seguridad pseudo-aleatoria es “396&fty7d3GG9”, el usuario devolvería “9&y6”,

con “9” siendo el segundo (2º) carácter en la cadena de seguridad,”&” siendo el cuarto (4º) carácter, “y” siendo el séptimo (7º) carácter y “6” siendo el tercer (3er) carácter.

Como una alternativa a la selección de caracteres de una cadena de seguridad en una base de posición mediante un código numérico, el usuario puede hacerlo basándose en la aplicación de una forma o patrones secretos en una matriz de números de seguridad (más bien como una rejilla de Cardano), aunque desde el punto de vista informático el método es similar al descrito anteriormente.

Una ventaja especial del tipo de encriptación divulgado en el documento US 7,392,388 es que es relativamente simple para un usuario aplicar mentalmente, aunque también se puede utilizar una miniaplicación o una aplicación pequeña ejecutándose en un dispositivo móvil propiedad del usuario, siendo aun así todavía razonablemente seguro. En particular, asumiendo una redundancia suficiente en la cadena de seguridad pseudo-aleatoria, no es fácil para una tercera parte deducir el NIP o el código numérico del usuario, incluso si tanto la cadena de seguridad pseudo-aleatoria como la respuesta de vuelta del usuario son pirateadas.

También es conocido, por ejemplo a partir del documento US 2011/0060912, introducir una contraseña mediante un monitor sensible al tacto. Se muestra una matriz de contraseña que tiene una pluralidad de caracteres, los caracteres que están dispuestos en un primer orden. El sistema detecta si se recibe una señal de permutación, y genera una matriz de contraseña que tiene una pluralidad de caracteres en un segundo orden. En otras palabras, el sistema comprende una interfaz de entrada NIP de pantalla táctil donde las teclas del teclado numérico pueden ser desplazadas de forma pseudo-aleatoria tras la recepción de una señal de permutación, que puede ser una entrada de usuario o puede ser enviada automáticamente después de cada entrada de tecla. El documento US 2010/0242104 da a conocer un mapeado creado entre un NIP de usuario estático y un NIP codificado, que corresponde a la ubicación de posición de los dígitos del NIP en una matriz de posición compuesta de celdas individuales, cuyos identificadores de ubicación pueden ser marcados.

Breve resumen de la divulgación

De acuerdo con un primer aspecto, se proporciona un método de verificación de una identidad de un usuario en un sistema informático, el usuario al que se le asigna un código de acceso de usuarios en forma de una cadena invariable de números enteros de 0 a 9, con una longitud no mayor de diez; que comprende:

i) almacenar el código de acceso de usuario en el sistema informático;

ii) el sistema informático que genera una cadena de diez dígitos aleatoria o pseudo-aleatoria sin repetición de números enteros de 0 a 9, la cadena que tiene de una 1ª a una 10ª posiciones cada una con un único número entero y que tiene valores de posición respectivos 1 a 10;

iii) el sistema informático que realiza un algoritmo predeterminado para combinar el código de acceso de usuario y la cadena aleatoria o pseudo-aleatoria, por lo tanto para determinar un código de verificación de un solo uso en forma de una cadena de la misma longitud que el código de acceso del usuario;

iv) el sistema informático que genera celdas 1ª a 10ª, las celdas que tienen unos valores de posición respectivos de 1 a 10;

v) el sistema informático que puebla las celdas con los números enteros de la cadena sin repetición de tal manera que el valor de ubicación de cada celda se corresponde al número entero que contiene combinado con la cadena aleatoria o pseudo-aleatoria que utiliza el mismo algoritmo que el utilizado en la etapa iii);

vi) el sistema informático que muestra las celdas en un monitor;

vii) el usuario que utiliza un dispositivo de entrada del sistema informático para seleccionar, en orden, las celdas en el monitor que contiene los números enteros que constituyen los códigos de acceso de usuario, en donde cada acto de selección devuelve el valor de posición de la celda seleccionada, por lo tanto para generar un código de transacción de un sólo uso que comprende una cadena de números enteros de 0 a 9 que tiene la misma longitud que el código de acceso de usuario;

viii) el sistema informático que compara el código de verificación con el código de transacción de un sólo uso; y

ix) se realiza una verificación de identidad con éxitos y el código de verificación coincide con el código de transacción de un sólo uso.

De acuerdo con un segundo aspecto, se proporciona un sistema para verificar una identidad de un usuario en un sistema informático, el usuario al que es asignado un código de acceso de usuario en forma de una cadena invariable de números enteros de 0 a 9, con una longitud no mayor de diez; el sistema informático que está configurado para:

i) almacenar el código de acceso de usuario en una memoria

ii) generar una cadena de diez dígitos aleatoria o pseudo-aleatoria sin repetición de los números enteros de 0 a 9, la cadena que tiene una 1ª a 10ª posición es cada una con un número entero único y que tiene valores deposición respectivos de 1 a 10;

iii) realizar un algoritmo predeterminado para combinar el código de acceso de usuario y la cadena aleatoria o pseudo-aleatoria, por lo tanto para determinar un código de verificación de un sólo uso en forma de una cadena de la misma longitud que el código de acceso de usuario;

iv) generar celdas 1ª a 10ª, las celdas que tienen valores de posición 1 a 10 respectivos;

v) poblar las celdas con los números enteros de la cadena sin repetición de tal manera que el valor de exposición de cada celda se corresponda al número entero que contiene combinado con la cadena aleatoria o pseudo-aleatoria que utiliza el mismo algoritmo que el utilizado en la etapa iii);

vi) mostrar las celdas en un monitor;

vii) recibir una entrada del usuario, el usuario que utiliza un dispositivo de entrada del sistema informático para seleccionar, en orden, las celdas en el monitor que contiene los números enteros que constituyen el código de acceso de usuario, en donde cada acto de selección devuelve el valor de ubicación de la celda seleccionada, por lo tanto para generar un código de transacción de un sólo uso que comprende una cadena de números enteros de 0 a 9 que tiene la misma longitud del código de acceso de usuario;

viii) comparar el código de verificación con el código de transacción de un sólo uso; y

ix) hacer una verificación de identidad con éxito si el código de verificación coincide con el código de transacción de un sólo uso.

En una implementación básica, por ejemplo, modos de realización de la invención podrían permitir al usuario acceder a un edificio o abrir una puerta cerrada escribiendo un código de acceso de usuario en la etapa vii). El hecho de que el usuario escriba el código de acceso correcto se considera suficiente para identificar al usuario como un usuario autorizado. Usuarios múltiples podrían todos utilizar el mismo código de acceso. Esto es análogo a un cerrojo de combinación tradicional, que se puede abrir por cualquiera que esté en posesión del código de combinación. La ventaja del presente método es que el usuario podría activar diferentes claves cada vez que es introducido el código de acceso de usuario, y esto ayuda a reducir el riesgo de observación furtiva.

En implementaciones más sofisticadas, a cada usuario se le asigna con una identidad usuario. Esto podría ser, por ejemplo, un número de cuenta de banco u otro número de ID que pueda ser almacenado en una tarjeta (por ejemplo en una banda magnética o en un circuito o chip integrado), o en una identificación de ID o almacenado en un dispositivo electrónico portátil tal como un teléfono móvil. Esto permite a cada usuario tener su propio código de acceso de usuario, y requiere a un usuario identificarse a sí mismo proporcionando su identidad de usuario junto con el código de acceso de usuario asociado, dado que esta combinación será única para cada usuario. El sistema informático podrá tener almacenado en su memoria tanto la identidad de usuario (de forma más probable junto con la información de otro usuario, tal como el nombre, dirección y otros detalles) y el código de acceso de usuario, y el usuario necesita proporcionar tanto su identificación de usuario como su código de acceso de usuario para acceder al sistema. El método de entrada de código de acceso de usuario particular de los modos de realización de la invención busca proporcionar una manera más segura para el usuario de introducir su código de acceso de usuario que el método de entrada directo tradicional.

El usuario necesita tener conocimiento del algoritmo predeterminado que es utilizado para generar el código de verificación y para poblar las celdas con los números enteros de la cadena aleatoria o pseudo-aleatoria. De hecho, modos de realización preferidos buscan proporcionar un método seguro de generación de un código de transacción de un sólo uso y un código de verificación correspondiente en una manera que es casi transparente al usuario, por tanto facilitando el uso del sistema y el método.

En un modo de realización, el algoritmo puede funcionar como sigue. El sistema informático determina un código de verificación de una manera similar a la divulgada en el documento US 7,392,388, de forma específica tomando el primer dígito de un código de acceso de usuario, seleccionando el número entero en la posición correspondiente en la cadena aleatoria o pseudo-aleatoria, y devolviendo este número entero como el primer dígito del código de verificación. Este mismo proceso es repetido para el segundo, tercer, etcétera dígitos del código de acceso de usuario, por tanto generando un código de verificación que tiene la misma longitud que el código de acceso de usuario, pero con diferentes números enteros que constituyen el código.

Con el fin de poblar las celdas con los números enteros de la cadena aleatoria o pseudo-aleatoria, el sistema informático determina la posición del número entero “1” en la cadena, y coloca el valor de posición de la posición del número entero “1” en la 1ª celda; determina la posición del número entero “2” en la cadena, y coloca el valor de posición de la posición del número entero “2” en la 2ª celda; determina la posición del número entero “3” en la cadena, y coloca el valor de posición de la posición del número entero “3” en la 3ª celda; y así sucesivamente para determinar la posición del número entero “0” en la cadena, y colocar el valor de posición de la posición del número de “0” en la 10ª celda.

Cuando el usuario mira al monitor, los números enteros 1, 2, 3, 4, 5, 6, 7, 8, 9 y 0 son mostrados, por ejemplo en una matriz correspondiente a un teclado numérico tradicional, pero no estarán en el orden tradicional (a menos que, por casualidad, la cadena aleatoria o pseudo-aleatoria sea “1234567890” para un teclado del estilo de un teléfono, tomando la parte izquierda superior una posición 1 y la parte inferior como una posición 10). Sin embargo, cuando el usuario selecciona los números enteros que constituyen su código de acceso de usuario de la matriz de teclado numérico mostrada, el código de transacción de un sólo uso que es realmente introducido en el sistema informático comprende los valores de posición correspondientes de los dígitos del código de acceso de usuarios los cuales, debido al algoritmo utilizado para poblar las celdas, corresponderán con el código de verificación (asumiendo una entrada de código correcta). Se ha de apreciar que esto proporciona una diferencia significativa con respecto a los sistemas tales como el descrito en el documento US 2011/0060912, que no puebla de forma cuidadosa las celdas en una permutación únicamente (para cada cadena aleatoria o pseudo-aleatoria) de acuerdo con un algoritmo predeterminado de manera que cuando el usuario introduce su código de acceso de usuario, el código de transacción de un sólo uso que es realmente introducido al sistema informático se basa en los valores de ubicación de las celdas, no en los contenidos de las celdas. Esto tiene la sutil, pero importante consecuencia de que el código de transacción de un sólo uso es automáticamente idéntico al código de verificación.

El algoritmo en su lugar puede ser aplicado al revés. El código de verificación puede ser determinado tomando el valor de posición en la cadena aleatoria o pseudo-aleatoria del primer dígito del código de acceso del usuario. Después tomando la posición en la cadena aleatoria o pseudo-aleatoria del segundo dígito del código de acceso de usuario útil, y así sucesivamente para generar el código de verificación de la misma longitud del código de acceso de usuario. Las celdas son entonces pobladas poniendo el primer dígito de la cadena en la 1ª celda, el segundo dígito en la 2ª celda y así sucesivamente. Por consiguiente, cuando el usuario selecciona los dígitos de su código de acceso de usuario de las celdas mostradas, devolverá los valores de ubicación de las celdas seleccionadas, que formarán un código de transacción de un sólo uso que corresponde al código de verificación.

Se pueden utilizar otros algoritmos, por ejemplo, un algoritmo “añadir n” donde el valor de ubicación de cada dígito en la cadena aleatoria o pseudo-aleatoria corresponde al valor del dígito más n (módulo 10). Para una mejor seguridad, el valor de n puede ser aleatorio o pseudo aleatorio y cambia de una transacción a la siguiente.

Se entenderá que se puede utilizar cualquier número de algoritmos, siempre que generen una correspondencia uno a uno permitiendo que se genere un código de verificación a partir de la cadena aleatoria o pseudo-aleatoria combinada con el código de acceso de usuario, y para permitir que se genere un código de transacción de un sólo uso idéntico mediante un usuario seleccionando dígitos de celdas que han sido pobladas basándose en el mismo algoritmo y operandos.

El dispositivo de entrada puede ser una pantalla táctil, puede ser un puntero controlado por un ratón, un ratón de bola, un panel táctil, unas teclas de cursor u otro dispositivo de control. Lo que es importante es que el dispositivo de entrada permita a los contenidos de las celdas ser mostrados de una manera que cambiarán entre transacciones cambiando la permutación no repetitiva de los dígitos de 0 a 9. De forma preferible, el dispositivo de entrada es tal que evita que los registradores de pulsaciones sean capaces de determinar los datos que están siendo introducidos por el usuario, y también obstaculizar a un observador furtivo o una cámara oculta para determinar las teclas que están siendo presionadas basándose en los movimientos de la mano o los dedos.

El contenido de las celdas puede ser mostrado como una matriz regular de dimensiones predeterminadas. Por ejemplo, la matriz puede ser representada como un teclado numérico convencional con los dígitos 0 a 9 cada uno representado una vez. La matriz puede ser de 2x5 o 5x2 o 3x3+1 o de nido de abeja u otra disposición, por ejemplo tal y como se muestra en el documento US 6,549,194. Sin embargo, a diferencia de un teclado numérico convencional, los números mostrados pueden cambiar cada vez que se muestra el teclado numérico. Esto significa que es difícil sino imposible para un software malicioso determinar qué números son seleccionados incluso si se puede determinar la posición del puntero.

De forma alternativa, la matriz de caracteres se puede presentar como cualquier matriz irregular, siempre que cada posición en la matriz tenga un único identificador de posición. La disposición de la matriz irregular se puede cambiar entre verificaciones de identidad sucesivas, por ejemplo tal y como se muestra en el documento US 7,992,007. De forma relativa o adicionalmente, las posiciones de los elementos de la matriz en el monitor se pueden disponer de forma diferente en aplicaciones sucesivas del método.

El monitor y el dispositivo de entrada pueden estar asociados con un terminal informático en comunicación con un ordenador principal al cual el usuario desea acceder. El terminal informático puede ser un ordenador de la casa del usuario, o un ordenador público en un locutorio de Internet o en un hotel, un cajero automático, una máquina EPV, un auricular móvil o una tableta o cualquier otro dispositivo apropiado.

El ordenador principal puede definir la disposición y contenido de la matriz de caracteres mostrada en el monitor del terminal informático.

El método y el sistema se pueden utilizar para identificar un usuario en un sistema informático mediante una página web o mediante un cajero automático o un dispositivo EPV, o cualquier otra interfaz donde se pueda mostrar una

matriz de caracteres en un monitor y donde el usuario pueda seleccionar dígitos apropiados en secuencia, la selección siendo introducida en el sistema informático. El método y el sistema no están limitados a identificar un usuario para una institución financiera tal como un banco, sino en cualquier situación en la que un usuario tiene un código de identidad de usuario y un código de acceso del usuario asociado (por ejemplo un NIP o contraseña) que debe mantener en secreto y que es conocido solo por el usuario y el sistema informático de la organización emisora.

Una ventaja particular es que el código de acceso del usuario secreto del usuario nunca es introducido en sí mismo en el sistema informático, sino que en su lugar es traducido en identificadores deposición automáticamente por el proceso de selección. Esto proporciona una capa adicional de seguridad con respecto al mecanismo de entrada de puntero o basado en pantalla táctil anterior.

Breve descripción de los dibujos

Modos de realización de la invención son descritos adicionalmente de aquí en adelante con referencia a los dibujos que acompañan, en los cuales:

La figura 1 muestra una representación de un teclado numérico estándar que comprende una matriz de celdas;

La figura 2 muestra una representación del teclado numérico de la figura 1, pero con las celdas pobladas por dígitos de una cadena aleatoria o pseudo-aleatoria sin repetición; y

La figura 3 muestra una arquitectura básica de un modo de realización de la invención.

Descripción detallada

La figura 1 muestra una representación de un teclado 1 numérico típico que comprende una matriz de celdas: las celdas 2 son pobladas de forma no repetitiva con los dígitos de 0 a 9. La configuración mostrada es similar a la de un teclado numérico de teléfono. Otras configuraciones estándar podrían ser como las que se encuentran en un teclado numérico de una calculadora o de un ordenador, con el 9 en la parte izquierda superior y el 3 en la parte derecha inferior. En el modo de realización mostrada, cada celda 2 tiene un valor de posición, con el dígito “1” que está en la celda con el valor de posición 1, el dígito “2” que está en la celda con el valor de posición 2, y así sucesivamente hasta el dígito “0” que está en la celda con el valor de posición 10.

Suponiendo que el usuario tiene un código de acceso de usuario “2468”. El sistema informático está configurado para generar una cadena de diez dígitos aleatoria o pseudo-aleatoria sin repetición de los números enteros 0 a 9, por ejemplo “5094382716”. La cadena será diferente para cada transacción. Con el fin de generar un código de verificación, el ordenador combina el código de acceso del usuario “2468” con la cadena sin repetición “5094382716” tomando el 2º, 4º, 6º y 8º dígitos de la cadena sin repetición. Esto genera un código de verificación “0487” (la longitud del código de verificación es la misma que la del código de acceso de usuario).

El sistema informático también determina cuáles dígitos necesitan ser colocados en cual celda 2 del teclado 1 para el proceso de autentificación. En el presente ejemplo, debido a que el dígito “1” es el 9º dígito en la cadena “5094382716”, el dígito “9” será colocado en la celda con el valor de posición 1. El dígito “2” es el 7º dígito en la cadena, y por tanto el dígito “7” será colocado en la celda con el valor de posición 2. El dígito “3” es el 5º dígito en la cadena, y por tanto el dígito “5” será colocado en la celda con el valor de posición 3. Esto continúa hasta el dígito “0” que es el 2º dígito en la cadena, con el dígito 2 que es colocado en la celda con el valor de ubicación 10.

La figura 2 muestra las celdas 2 del teclado 1 pobladas con los dígitos de la cadena aleatoria o pseudo-aleatoria sin repetición “5094382716” tal y como se describió en el párrafo anterior. Cuando el usuario es presentado con este teclado 1, introducirá el código de acceso de usuarios seleccionando los dígitos “2,”, “4”, “6” y “8” mostrados en orden. Esto devolverá un código de transacción de un sólo uso en forma de una cadena que comprende los valores de ubicación de las celdas 2 que contienen estos dígitos, en particular “0487” (se entenderá que el valor de ubicación “10” en las celdas y el valor “10” de posición en la cadena aleatoria o pseudo-aleatoria se corresponde a un valor 0 en el código de acceso de usuario y en el código de verificación en el modo de realización ilustrado).

Por tanto, si y sólo si un usuario introduce de forma exitosa el código de acceso de usuario correcto, se devuelve un código de transacción de un sólo uso “0487” que coincide automáticamente con el código de verificación “0487”.

La figura 3 muestra un sistema de arquitectura típico para un modo de realización de la invención, en el que un servidor 100 de autentificación se comunica con un monitor 200 de un dispositivo informático (no mostrado). El monitor 200 puede ser un monitor de pantalla táctil, puede ser un monitor en el que las celdas 2 pueden ser seleccionadas con un dispositivo de entrada tal como un ratón y un puntero. Un usuario (no mostrado) se identifica a sí mismo a través de una forma de un formulario de entrada introduciendo su identidad de usuario única (aquí “prueba”). La identidad de usuario es transmitida al servidor 100 de autentificación, en donde la identidad de usuario es utilizada para consultar un código de acceso de usuario asociado. Se genera una permutación aleatoria o pseudo-aleatoria sin repetición de los dígitos 0 a 9, y esta se combina con el código de un usuario para generar un código de verificación. Adicionalmente, las celdas 2 del monitor 200 son pobladas de forma no repetitiva con los dígitos 0 a 9 basándose en el código de acceso de usuario y la permutación aleatoria o pseudo-aleatoria tal y como se expuso anteriormente.

El usuario puede entonces seleccionar los dígitos de su código de acceso de usuario en el monitor 200 de manera que devuelve los valores de ubicación de las celdas 2 que contienen los dígitos relevantes, por lo tanto generando un código de transacción de un sólo uso que es devuelto al servidor 100 de autentificación por medio de una caja 300 de diálogo. El servidor 100 de autentificación compara el código de transacción de un sólo uso con el código de verificación, y si éstos son iguales, concede acceso al usuario.

El formulario de acceso es fácil de implementar dentro de tecnologías web estándar, notablemente en html y JavaScript. Por ejemplo, el teclado numérico puede ser implementado como una tabla, con cada celda que tiene un evento de pulsación de clic que añade su posición al campo de credenciales del formulario, aunque se apreciará que las teclas o botones se pueden colocar en cualquier posición en la página.

```
function addOtc(digit){
                    var otc;
                    otc = document.getElementById("otc");
                    otc.value = otc.value + digit;
}
.
.
.
<table>
<tr>
<td onclick=addOtc("1")>
<img id="1"></img>
</td>
.
.
.
<tr>
<td>OTC</td><td><input type = "password" disabled="disabled"
id="otc"></input></td>
</tr>
```

Para mostrar la rejilla, el formulario pide las imágenes al servidor 100 de autentificación. El formulario suministra un nombre de usuario y una clave de sesión. Se crea una cadena de seguridad diferente para cada clave de sesión.

```
function getButtons() {
             var name,n,sessionKey;
             sessionKey = + Math.ceil(10000*Math.random());
             name = document.getElementById("username").value;
             for(n = 1; n<=10; n++){
                    img = document.getElementById("" + n);
                    img.src = serverurl + name + "&padno=" +
                    sessionKey + ":" + n ;
       }
}
```

A lo largo de toda la descripción y las reivindicaciones de esta memoria descriptiva, las palabras “comprende” y “contiene” y variaciones de las mismas significa “que incluye pero no limitado a”, y no están destinadas (y no) incluyen otras fracciones, aditivos, componentes, enteros o etapas. A lo largo de toda descripción y reivindicaciones de esta manera descriptiva, el singular engloba el plural a menos que el contexto requiera lo contrario. En particular, cuando se utiliza el artículo indefinido, la memoria descriptiva se ha de entender como que contempla la pluralidad así como la singularidad, a menos que el contexto requiera lo contrario.

Funciones, enteros, características, compuestos, fracciones químicas o grupos descritos en conjunción con un aspecto particular, modo de realización o ejemplo de la invención se han de entender para ser aplicables a cualquier otro aspecto, modo de realización o ejemplo descritos en el presente documento a menos que sea incompatible con el mismo. Todas las características divulgadas en esta memoria descriptiva (incluyendo cualquier reivindicación, resumen y dibujos que acompañan) y/o todas las etapas de cualquier método o proceso por tanto divulgado, pueden ser combinados en cualquier combinación, excepto combinaciones en las que al menos algunas de dichas características y/o etapas son mutuamente exclusivas. La invención no está restringida a los detalles de cualquiera de los modos de realización anteriores. La invención se extiende a cualquier característica novedosa o cualquier combinación de características novedosas divulgadas en esta memoria descriptiva (incluyendo cualquier reivindicación, resumen y dibujos que acompañan) o cualquier etapa novedosa o cualquier combinación de etapas novedosas de cualquier método o proceso por tanto divulgado.

La atención del lector se dirige a todos los papeles o documentos que son presentados de forma concurrente con o previos a esta memoria descriptiva en conexión con esta solicitud y que están abiertos a la inspección pública con

esta memoria descriptiva, y los contenidos de todos dichos papeles y documentos están incorporados en el presente documento por referencia.

REIVINDICACIONES

1. Un método de verificación de una identidad de un usuario en un sistema informático, el usuario al que se asigna un código de acceso de usuario en forma de una cadena invariable de números enteros de 0 a 9 con una longitud mayor de diez; que comprende:

i) almacenar el código de acceso de usuario en el sistema informático;

ii) el sistema informático que genera una cadena de diez dígitos aleatoria o pseudo-aleatoria sin repetición de los números enteros de 0 a 9, la cadena que tiene de una 1ª a una 10ª posiciones cada una con un único número entero y que tiene valores de posición respectivos 1 a 10;

iii) el sistema informático que selecciona números enteros de la cadena aleatoria o pseudo-aleatoria sin repetición en una base posicional determinada por los valores de número entero de los números enteros del código de acceso de usuario, tomados en un orden de posición, por lo tanto para determinar un código de verificación de un sólo uso en forma de una cadena de la misma longitud que el código de acceso de usuario, con el valor de número entero 1 correspondiente al valor de posición 1, el valor de número entero 2 correspondiente al valor de posición 2 y así sucesivamente, con el valor de número entero 0 correspondiente al valor de posición 10;

iv) el sistema informático que genera celdas 1ª a 10ª, las celdas que tienen unos valores de ubicación respectivos de 1 a 10;

v) el sistema informático que puebla las celdas con los números enteros de la cadena sin repetición de tal manera que el valor de posición de cada celda se corresponde con el valor de posición en la cadena aleatoria o pseudo-aleatoria del número entero que representa el valor de ubicación de la celda, con el valor de número entero 1 correspondiente al valor de posición 1, el valor de número entero 2 correspondiente al valor de posición 2 y así sucesivamente, con el valor de número entero 0 correspondiente al valor de posición 10;

vi) el sistema informático que muestra las celdas en un monitor;

vii) el usuario que utiliza un dispositivo de entrada del sistema informático para seleccionar, en orden, las celdas en el monitor que contiene los números enteros que consultan los códigos de acceso de usuario, en donde cada acto de selección devuelve el valor de posición de la celda seleccionada, por lo tanto para generar un código de transacción de un sólo uso que comprende una cadena de números enteros de 0 a 9 que tiene la misma longitud que el código de acceso de usuario;

viii) el sistema informático que compara el código de verificación con el código de transacción de un sólo uso; y

ix) se realiza una verificación de identidad con éxitos y el código de verificación coincide con el código de transacción de un sólo uso.

2. Un método de acuerdo con la reivindicación 1, en donde a cada usuario se le asigna una identidad de usuario única.

3. Un método de acuerdo con la reivindicación 2, en donde el sistema informático almacena cada identidad de usuario en asociación con el código de acceso de usuarios del usuario.

4. Un método de acuerdo con cualquiera de las reivindicaciones anteriores, en donde el dispositivo de entrada es una pantalla táctil, o en donde el dispositivo de entrada es un puntero controlado por un ratón, un ratón de bola, un panel táctil, teclas de cursor u otro dispositivo de control.

5. Un método de acuerdo con cualquiera de las reivindicaciones anteriores, en donde las celdas son mostradas como una matriz regular de dimensiones predeterminadas, o en donde las celdas son mostradas como una matriz irregular.

6. Un método de acuerdo con cualquiera de las reivindicaciones anteriores, en donde las posiciones de las celdas en el monitor están dispuestas de forma diferente en aplicaciones sucesivas del método.

7. Un método de acuerdo con cualquiera de las reivindicaciones anteriores, en donde el monitor y el dispositivo de entrada están asociados con un terminal informático en comunicación con un ordenador principal al cual el usuario desea acceder.

8. Un método de acuerdo con la reivindicación 7, en donde el ordenador principal define una disposición y un contenido de las celdas mostradas en el monitor del terminal informático.

9. Un sistema para verificación de una identidad de un usuario en un sistema informático, el usuario al que es asignado un código de acceso de usuario en forma de una cadena invariable de números enteros de 0 a 9, con una longitud no mayor de diez; el sistema informático que está configurado para:

i) almacenar el código de acceso de usuario en una memoria

ii) generar una cadena de diez dígitos aleatoria o pseudo-aleatoria sin repetición de los números enteros de 0 a 9, la cadena que tiene una 1ª a 10ª posición es cada una con un número entero único y que tiene valores deposición respectivos de 1 a 10;

iii) seleccionar números enteros de la cadena aleatoria o pseudo-aleatoria sin repetición en una base posicional determinada por los valores de número entero de los números enteros del código de acceso de usuario, tomados en un orden de posición, por lo tanto para determinar un código de verificación de un sólo uso en forma de una cadena de la misma longitud que el código de acceso de usuario, con el valor de número entero 1 correspondiente al valor de posición 1, el valor de número entero 2 correspondiente al valor de posición 2 y así sucesivamente, con el valor de número entero 0 correspondiente al valor de posición 10;

iv) generar celdas 1ª a 10ª, las celdas que tienen unos valores de posición respectivos de 1 a 10;

v) poblar las celdas con los números enteros de la cadena sin repetición de tal manera que el valor de posición de cada celda se corresponde con el valor de posición en la cadena aleatoria o pseudo-aleatoria del número entero que representa el valor de ubicación de la celda, con el valor de número entero 1 correspondiente al valor de posición 1, el valor de número entero 2 correspondiente al valor de posición 2 y así sucesivamente, con el valor de número entero 0 correspondiente al valor de posición 10;

vi) mostrar las celdas en un monitor;

vii) recibir una entrada del usuario, el usuario que utiliza un dispositivo de entrada del sistema informático para seleccionar, en orden, las celdas en el monitor que contienen los números enteros que consultan los códigos de acceso de usuario, en donde cada acto de selección devuelve el valor de posición de la celda seleccionada, por lo tanto para generar un código de transacción de un sólo uso que comprende una cadena de números enteros de 0 a 9 que tiene la misma longitud que el código de acceso de usuario;

viii) comparar el código de verificación con el código de transacción de un sólo uso; y

ix) realizar una verificación de identidad con éxitos y el código de verificación coincide con el código de transacción de un sólo uso.

10. Un sistema como el reivindicado en la reivindicación 9, en donde a cada usuario es asignado una identidad de usuario única y en donde el sistema informático está configurado para almacenar cada identidad de usuario en asociación con el código de acceso de usuario del usuario.

11. Un sistema como el reivindicado en cualquiera de las reivindicaciones 9 a 10, en donde el dispositivo de entrada es una pantalla táctil, o en donde el dispositivo de entrada es un puntero controlado por un ratón, un ratón de bola, un panel táctil, teclas de cursor u otro dispositivo de control.

12. Un sistema como el reivindicado en cualquiera de las reivindicaciones 9 a 11, en donde las celdas son mostradas como una matriz regular de dimensiones predeterminadas, o en donde las celdas son mostradas como una matriz irregular.

13. Un sistema como el reivindicado en cualquiera de las reivindicaciones 9 a 12, en donde las posiciones de las celdas en el monitor están dispuestas de forma diferente en aplicaciones sucesivas del método.

14. Un sistema como el reivindicado en cualquiera de las reivindicaciones 9 a 13, en donde el monitor y el dispositivo de entrada están asociados con un terminal informático en comunicación con un ordenador principal al cual el usuario desea acceder.

15. Un sistema como el reivindicado en la reivindicación 14, en donde el ordenador principal está configurado para definir la disposición y el contenido de la matriz de caracteres mostrados en el monitor del terminal informático.

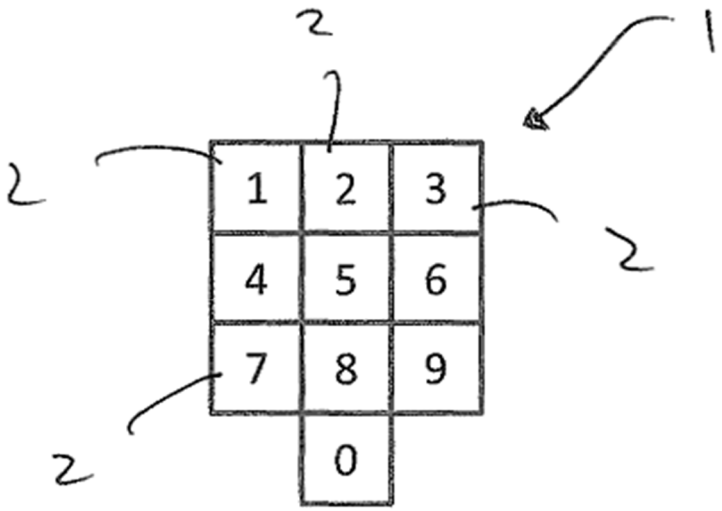

Figura 1

Cadena aleatoria/eudo-aleatoria: 5094382716

Código de acceso de usario: 2468

Código de verificación: 0487

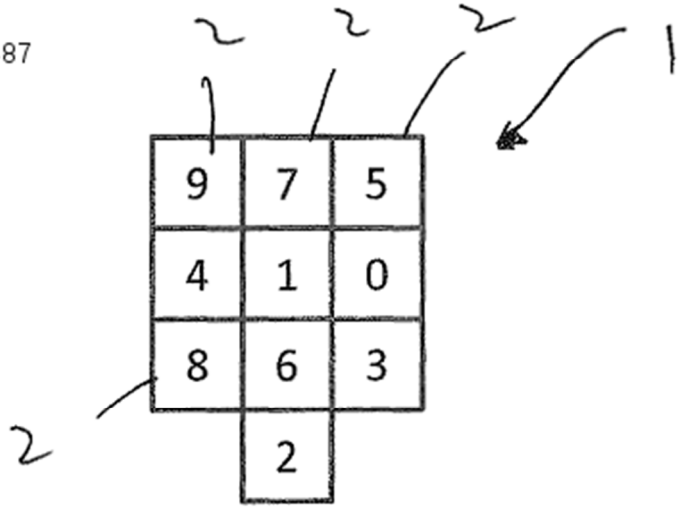

Figura 2

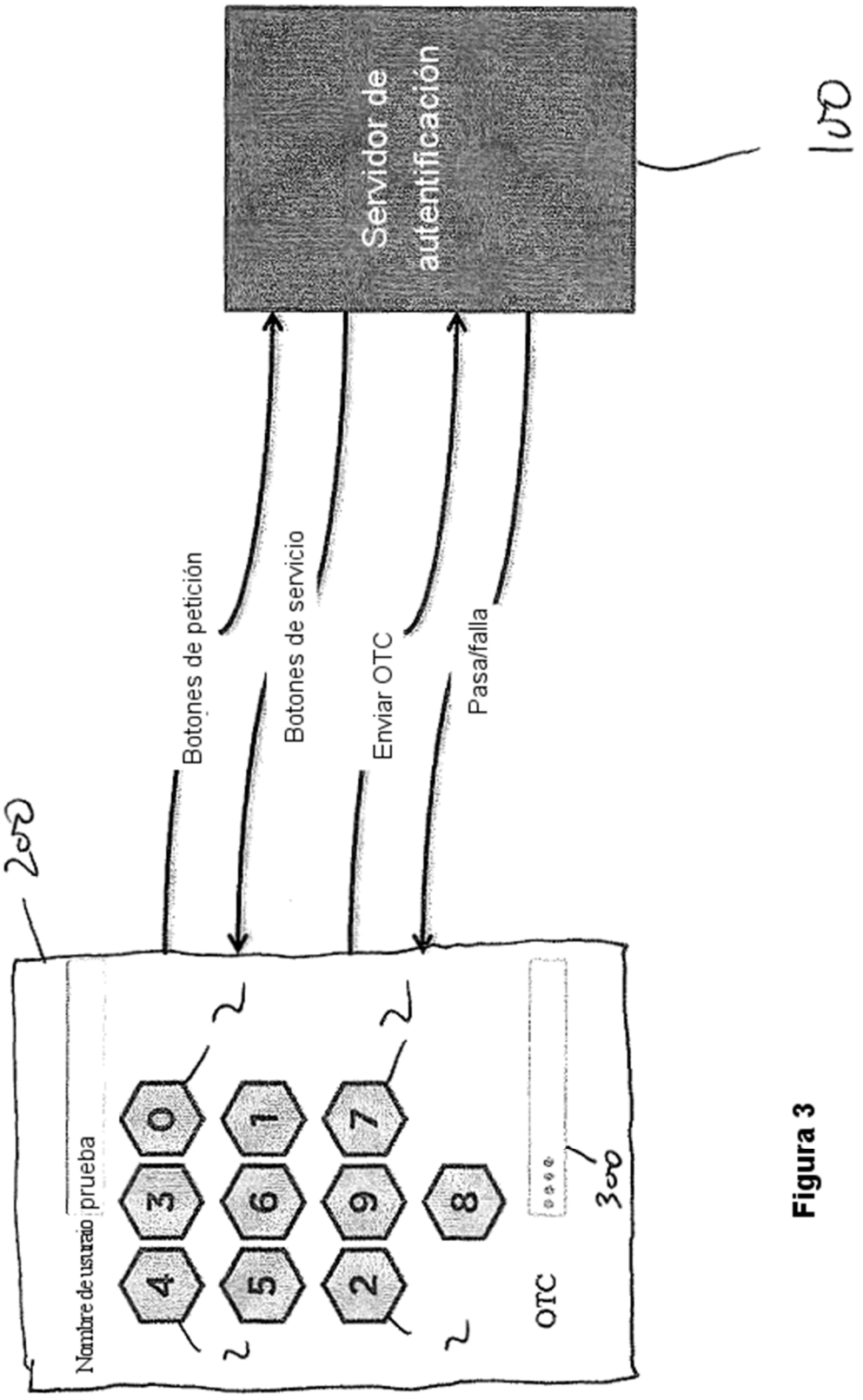
Servidor de autentificación
100
Botones de petición
Botones de servicio
Enviar OTC
Pasa/falla
200
Nombre de usuario
prueba
4
3
0
5
6
1
2
9
7
8
OTC
300

Figura 3