(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 686 113**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06F 21/34 (2013.01)
G06F 21/43 (2013.01)
G06Q 20/00 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **14.04.2011 E 11003161 (4)**

(97) Fecha y número de publicación de la concesión europea: **06.06.2018 EP 2512090**

(54) Título: **Procedimiento para la autentificación de un participante**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
16.10.2018

(73) Titular/es:

TELEFÓNICA GERMANY GMBH & CO. OHG (100.0%)
Georg-Brauchle-Ring 23-25
80992 München, DE

(72) Inventor/es:

PIECHA, SEBASTIAN

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Procedimiento para la autentificación de un participante

La invención hace referencia a un procedimiento para la autentificación de un participante en una red de comunicaciones, donde al participante, hacia al menos un dispositivo terminal, se transmite un código de autentificación codificado para una entrada de autentificación.

En la era electrónica se ofrecen numerosos servicios para participantes que necesitan una sólida autentificación de los consumidores finales participantes. Por ejemplo, compras cotidianas, operaciones bancarias, así como otras adjudicaciones de contratos y celebraciones de contratos pueden realizarse vía Internet. Para la protección de eventuales intentos de manipulación a través de agresores externos se utilizan procedimientos de autentificación adecuados a la necesidad.

Para una autentificación sólida de participantes individuales se necesita un criterio seguro. En el caso de por ejemplo de los token únicos debe ponerse a disposición del respectivo usuario un dispositivo adicional. Debido a los costes, por tanto, cada vez más procedimientos de automatización se trasladan al teléfono móvil, como canal adicional.

Para asegurar una transacción, en particular en la banca electrónica mediante Internet, se utilizan procedimientos de autentificación que usan dos vías de transmisión diferentes. Por ejemplo, el participante usa el acceso a Internet de su ordenador para autorizar una transferencia en su banco. De forma inversa, el banco envía a su participante un código por SMS a su teléfono móvil, mediante la red de radio móvil de su proveedor de radio móvil, donde los SMS, en particular el código contenido dentro del mismo, se refieren a los datos de la transferencia antes ingresados. Para la autentificación definitiva de sus datos personales, o bien de los datos de la transacción, el participante ingresa el código recibido en la máscara de entrada en el ordenador, debido a lo cual la transferencia se libera.

Los accesos VPN con tokens de SMS funcionan de forma similar. El empleado de una empresa, con la ayuda de un software de cliente instalado en su ordenador, mediante una red no segura, como por ejempo la red WLAN en un hotel, o en un lugar público, establece una conexión hacia la pasarela de su empresa. La estructura IT correspondiente de la red VPN de la empresa transmite un token único por SMS al dispositivo móvil del empleado de la empresa. Sólo después de una entrada exitosa del token en el software de cliente se establece una conexión segura hacia la red de la empresa.

Los procedimientos de autentificación sólidos descritos ofrecen la ventaja de que no se transmiten contraseñas confidenciales mediante la red no segura, es decir la conexión de Internet o la red WLAN en el hotel, pero en el pasado han sido realizados ataques exitosos en teléfonos móviles que ponen en duda al teléfono como canal adicional seguro. Si un agresor logar instalar un software malicioso en el dispositivo de radio móvil del participante, entonces puede modificar el código recibido por SMS y, por consiguiente, puede imputar al participante una transferencia incorrecta. El problema reside en particular en los ordenadores de tableta que son cada vez más populares, los cuales por una parte permiten navegar en Internet, pero al mismo tiempo están equipados para la recepción de SMS mediante la red de radio móvil.

Por la solicitud EP 1 785 900 A1 se conocen un procedimiento y un sistema para la transferencia de datos desde un primer dispositivo de procesamiento de datos hacia un segundo dispositivo de procesamiento de datos. Para la decodificación se proporciona un filtro óptico para el dispositivo de visualización del primer dispositivo de procesamiento de datos, el cual contiene un patrón de decodificación. En base a ese patrón de decodificación, una máscara de entrada es decodificada por el segundo dispositivo de procesamiento de datos, la cual puede ser decodificada en el primer dispositivo de visualización colocando delante el filtro óptico.

El objeto de la invención consiste en retomar la problemática antes mencionada para, partiendo de la misma, posibilitar con medios sencillos una autentificación segura de participantes individuales. Debe indicarse en particular un método de autentificación que sea independiente del medio de transmisión seleccionado.

Dicho objeto se soluciona a través de un procedimiento con las características de la reivindicación 1. Conforme a éste, para la autentificación de un participante en una red de comunicaciones al participante se le solicita ingresar un código de autentificación correspondiente. El código de autentificación correspondiente se transmite al participante de forma codificada, hacia al menos un aparato terminal.

El código de autentificación comprende preferentemente una cadena de caracteres de cualquier longitud.

De acuerdo con la invención, la decodificación del código de autentificación codificado tiene lugar colocando delante la unidad de visualización del dispositivo terminal una lámina correspondiente, donde dicha unidad representa el código de autentificación codificado recibido. A través de la colocación delante la lámina, el código de autentificación

codificado aparece en forma legible, de modo que la entrada subsiguiente del código de autentificación legible posibilita la autentificación del participante en la red de comunicaciones.

El descifrado del código de autentificación codificado, conforme a ello, no se basa en ningún modelo matemático que puede decodificarse o manipularse con la ayuda de un software informático correspondiente. Conforme a ello, el procedimiento tampoco exige un dispositivo electrónico adicional para la autentificación de un participante. La utilización de una lámina se asocia a costes de producción, de distribución y operativos comparativamente reducidos.

Por participante de la red de comunicaciones se utilizan preferentemente láminas individuales del participante. Gracias a ello se garantiza que exclusivamente el participante involucrado y determinado para la autentificación pueda descifrar el código de autentificación codificado transmitido. Por lo tanto, la lámina utilizada del lado del participante para la decodificación debe considerarse al codificar el código de autentificación.

En una realización especialmente ventajosa del procedimiento según la invención, el código de autentificación codificado comprende una trama de puntos aleatoria que, al colocar la lámina delante de la unidad de visualización del dispositivo terminal, se transforma en un código de autentificación adecuado para la entrada consecutiva, para la autentificación del participante.

Un agresor potencial, accediendo a la trama de puntos correspondiente en la vía de transmisión no puede deducir el código de autentificación legible, requerido para la autentificación, ya que el agresor usualmente no tiene acceso a la lámina que se requiere de forma obligatoria. Se excluye una decodificación de la trama de puntos en base a dispositivos electrónicos. Además, deducir las propiedades de la lámina en base a la trama de puntos recibida es prácticamente imposible.

Es posible que la representación del código de autentificación codificado y la entrada del código de autentificación decodificado tengan lugar mediante un dispositivo terminal. Por ejemplo, en la banca electrónica, el acceso al sistema de la banca electrónica puede tener lugar mediante un ordenador convencional conectado mediante Internet. Debido a la realización del procedimiento para la autentificación según la invención, la transmisión hacia el dispositivo y la representación del código de autentificación codificado pueden tener lugar en el mismo aparato. Ya no se necesita un canal de transmisión adicional para la transmisión del código de autentificación, puesto que el ataque no resulta exitoso en el tramo de la transmisión entre el sistema de la banca electrónica y el dispositivo terminal del participante. La decodificación del código de autentificación tiene lugar colocando la lámina delante de la unidad de visualización del dispositivo terminal utilizado.

De manera alternativa es posible una separación en dos dispositivos terminales o canales de transmisión, en donde la representación del código de autentificación codificado tiene lugar mediante un primer dispositivo terminal y la entrada del código de autentificación decodificado tiene lugar mediante un segundo dispositivo terminal. Preferentemente, la transmisión del código de autentificación codificado o bien la transmisión de la instrucción de entrada entre los dispositivos terminales y la red de comunicaciones tiene lugar eventualmente mediante canales de comunicaciones diferentes. De este modo, el procedimiento según la invención puede aplicarse sin dificultad para toda forma de autentificación sólida.

En el caso de aplicación concreto, el participante usa su acceso a Internet en el ordenador para iniciar una transacción bancaria y para confirmar la transacción recibe en su teléfono móvil el código de autentificación codificado desde el banco, por SMS. Colocando la lámina delante de pantalla del teléfono móvil el código de autentificación recibido se transforma en un código de autentificación legible que, al ser ingresado en el ordenador, libera la transferencia correspondiente del participante.

Del modo antes indicado, en principio igualmente es posible que el código de autentificación decodificado se ingrese en el mismo dispositivo al cual fue transmitido el código de autentificación codificado. En el ejemplo antes mencionado, de este modo, el código de autentificación codificado puede transmitirse desde al banco hacia el ordenador, mediante el cual tiene lugar entonces también la entrada del código de autentificación decodificado.

En principio, de este modo, la invención abarca el caso de que sólo se proporcione un tramo de transmisión para la transmisión del código de autentificación codificado y para la entrada o bien la transmisión del código de autentificación decodificado, o de que para las dos transmisiones mencionadas se utilicen tramos o tipos de transmisión diferentes.

Asimismo, cabe señalar que la transmisión antes mencionada del código de autentificación codificado por SMS naturalmente representa sólo un ejemplo. La invención abarca también cualquier otro tipo de transmisión adecuada, como por ejemplo la transmisión del código por MMS.

Además, el procedimiento según la invención para la autentificación de un participante es adecuado para el acceso VPN y/o la identificación en un servidor web y/o de correo electrónico. En principio, el procedimiento según la invención puede usarse para todos los procedimientos de autentificación electrónicos.

Como medida de seguridad, según la invención, se utiliza al menos un símbolo adicional que debe ser definido por el participante, en una posición determinada o variable del código de autentificación. El símbolo individual del participante indica la presencia de una cadena de caracteres válida y transmitida de forma exitosa, y respalda por consiguiente la detección de intentos de manipulación. Por una parte, según esto, se exige una identidad del símbolo entre el símbolo transmitido y una definición del símbolo individual del participante, por otra parte se requiere la integración del símbolo en la posición correcta dentro de la cadena de caracteres transmitida del código de autentificación.

Se considera especialmente ventajoso que el código de autentificación codificado se transmita mediante un canal de radio móvil a un dispositivo terminal móvil. La transmisión del código de autentificación codificado mediante el sistema de radio móvil tiene lugar preferentemente por SMS, MMS, WAP-Push-SMS o un procedimiento de transmisión comparable. Preferentemente, el sistema de radio móvil puede diseñarse según uno de los estándares de radio móvil conocidos o bien posteriores, en particular GSM, GPRS, UMTS, LTE, etc.

Para estar preparado contra ataques estadísticos de un agresor en el procedimiento de autentificación puede tener lugar una desactivación del participante después de una o de varias entradas incorrectas del código de autentificación decodificado, del lado del participante. En ese caso se considera conveniente la desactivación de una cuenta del participante creada para el procedimiento de autentificación.

Junto con el procedimiento según la invención, la invención hace referencia además a la utilización de una lámina para ejecutar el procedimiento según una de las realizaciones ventajosas antes descritas. La lámina está realizada por ejemplo semitransparente y se compone de varias capas con diferente permeabilidad a la luz o alternativamente de un tejido de fibra de vidrio colado. La realización correspondiente de la lámina, al colocarla delante de una trama de puntos recibida, permite transformar la misma en un texto claro legible.

La producción, distribución y funcionamiento de una lámina de esa clase son comparativamente convenientes en cuanto a los costes y poco complejos. A diferencia de los procedimientos convencionales no se necesita ningún dispositivo adicional, en particular un dispositivo eléctrico, para decodificar el código de autentificación transmitido y codificado. Las láminas de esa clase son mayormente seguras en cuanto a manipulaciones, ya que debido a su particularidad técnica prácticamente se excluye una duplicación o una copia sencilla. El tamaño de la lámina o de la ventana de decodificación semitransparente determina la posibilidad de variación de la trama de puntos. Cuanto más grande es la dimensión de la lámina o de la ventana de decodificación, tanto mayor es la posibilidad de variación para conformar la trama de puntos. Eventualmente es posible un sinfín de variantes diferentes.

La inversión adicional que se necesita para un desciframiento del código de autentificación codificado recibido a través de la colocación anterior de la lámina, se justifica en gran medida con relación al beneficio de seguridad adicional obtenido. Los costes adicionales para la producción y la distribución de la lámina a los participantes correspondientes de una red de comunicaciones son particularmente reducidos en comparación con los riesgos potenciales en los procedimientos convencionales.

De manera ventajosa, la lámina se encuentra integrada en una tarjeta de crédito o en una tarjeta de débito, la cual puede estar realizada por ejemplo como tarjeta EC, o en otra tarjeta de identificación o de legitimación, en un documento de identidad, un permiso de conducir o una tarjeta de acceso a una empresa y, por tanto, puede ser llevada siempre por el participante de forma sencilla. En general es posible integrar la lámina en objetos personalizados adecuados y similares, como por ejemplo en cualquier tarjeta.

Naturalmente, la lámina puede estar realizada también como objeto separado, preferentemente en forma de una tarjeta, y de forma especialmente sencilla y cómoda puede llevarse como llavero.

La presente invención hace referencia además a la utilización de un objeto preferentemente personalizado, en particular una tarjeta de crédito tarjeta de débito, tarjeta de legitimación, tarjeta de identificación, documento de identidad, permiso de conducir, tarjeta de acceso a una empresa, para ejecutar el procedimiento según la invención, donde ese objeto está realizado con al menos una lámina que es adecuada para decodificar un código. Preferentemente la lámina está realizada de modo que es permeable a la luz. La lámina puede estar diseñada según la parte distintiva de una de las reivindicaciones 9 a 11.

Además, la invención apunta a una red de comunicaciones, en particular una red de radio móvil o de telecomunicaciones, donde la red de comunicaciones comprende uno o varios dispositivos terminales del participante, así como medios para ejecutar el procedimiento según una de las ejecuciones ventajosas precedentes.

Las ventajas y propiedades de la red de comunicaciones corresponden evidentemente a aquellas del procedimiento según la invención antes descrito, por lo cual en ese punto se prescinde de una descripción repetida.

En una realización ventajosa de la red de comunicaciones, ésta presenta medios de asociación que permiten una asociación de cada lámina individual, específica de la persona, a uno o a varios participantes individuales de la red de comunicaciones. Preferentemente, el medio de asociación comprende una base de datos que está diseñada para almacenar datos de asociación de esa clase.

Además, se considera conveniente que la red de comunicaciones comprenda un medio generador que codifica uno o varios códigos de autentificación considerando los datos del medio de asociación almacenado y eventualmente los transmite a los participantes correspondientes.

De manera adicional, cabe señalar que el servicio correspondiente que exige una autentificación sólida no es ofrecido obligatoriamente por la red de comunicaciones en sí misma. Por ejemplo, es posible que la red de comunicaciones, en particular en el caso de un proveedor de radio móvil, ofrezca el procedimiento de autentificación correspondiente para un proveedor de servicios externo. El proveedor de radio móvil recibe en ese caso los códigos de autentificación correspondientes en texto claro, los cuales se proporcionan para la transmisión hacia los participantes del servicio correspondientes. En el medio de asociación se determina el tipo de lámina correspondiente para el participante que debe ser autentificado, y se transmite al medio generador. El medio generador codifica el código de autentificación obtenido por el proveedor de servicios externo en base a los datos específicos de la lámina del medio de asociación, y transmite la información codificada a los participantes.

Otras ventajas y particularidades de la invención se explican en detalle a continuación mediante un ejemplo de ejecución. Las figuras muestran:

Figura 1: una posible secuencia de un ataque en un procedimiento convencional para la autentificación de un participante, mediante el ejemplo de un servicio de electrónica,

Figura 2: el procedimiento según la invención para la autentificación de un participante, mediante el ejemplo de un servicio de banca electrónica,

Figura 3: un posible ejemplo de ejecución de la lámina según la invención, y

Figura 4: una tarjeta de crédito o tarjeta de débito con una lámina según la invención integrada.

La figura 1 muestra una posible secuencia de un ataque en un procedimiento de autentificación sólido según el estado del arte, en el ejemplo concreto del TAN (número de transacción) móvil en la banca electrónica. El participante A, mediante la conexión a Internet de su ordenador, se conecta con el servidor bancario 2 de su banco. Usualmente, los bancos conocidos ofrecen como servicio en línea un acceso web para los consumidores finales, para realizar determinadas operaciones bancarias por procedimientos en la banca electrónica.

Para asegurar una transacción del participante A, el servidor bancario 2 usa un así llamado procedimiento de autentificación sólido que para la realización completa de cualquier transacción deseada utiliza siempre dos vías de transmisión diferentes. En el ejemplo mostrado en la figura 1a, la primera vía de transmisión está representada por la conexión del ordenador 1 del participante A mediante Internet 5, hacia el servidor bancario 2. Mediante ese acceso a Internet 5, el participante A en el ordenador 1 inicia una transferencia mediante la interfaz web del servidor bancario 2. De forma inversa, el servidor bancario 2, mediante la red de radio móvil 3 del proveedor de radio móvil del participante A, transmite por SMS un código de autentificación al dispositivo terminal 4 del participante 4.

El texto del SMS 10 recibido está reproducido en la caja de texto correspondiente de la figura 1a. El SMS 10 indica al participante A que para la transferencia por el valor de 100,00 euros al número de cuenta 123456789, ordenada mediante el ordenador 1, se encuentra a disposición un código de autentificación A12BCX, a continuación denominado simplemente como TAN móvil. El así llamado TAN móvil, mediante el canal de radio móvil 3 del proveedor de radio móvil, se transmite por SMS 10 en texto claro al dispositivo terminal 4 móvil del participante A. Ingresando el TAN en el ordenador 1 del participante A, la transferencia puede liberarse de forma definitiva.

La figura 1b muestra una posible secuencia de un ataque de un agresor externo a la transacción realizada del participante A. En el ordenador 1 del participante A un troyano 20 fue instalado de forma inadvertida, el cual manipula la orden de transacción realizada mediante la interfaz web del servidor bancario 2, sin conocimiento del participante A, y la transmite modificada al servidor bancario 2. Por ejemplo, el participante A efectúa las entradas para una orden de transferencia por el valor de 100,00 euros al número de cuenta 123456789. El troyano modifica los datos indicados de la orden en un segundo plano y transmite al servidor bancario 2 una orden manipulada que contiene una transferencia de 50.000,00 al número de cuenta del agresor.

Para la autentificación del participante A, el servidor bancario 2 inicia el envío de un SMS 40 con el TAN móvil mediante la red de radio móvil 3, al dispositivo terminal 4, donde el SMS 40, así como los datos TAN móviles, se refieren sin embargo a la orden modificada, por el valor de 50.000,00 euros.

Para que en el participante A no se despierte ninguna sospecha sobre la manipulación de la transacción bancaria, de manera adicional un troyano 30 debe estar instalado en el dispositivo terminal 4 del participante A, el cual suprime el SMS 40 recibido del servidor bancario 2 y en lugar de ello muestra un SMS 50 modificado que corresponde a la orden efectuada originalmente por el participante A.

Los dos troyanos 20, 30 en los respectivos dispositivos terminales 1, 4 cooperan uno con otro de manera que la entrada efectuada del TAN 0123456 modificado en el ordenador 1, que puede ser observado por el participante A en el dispositivo terminal 4, se reemplaza por el TAN A12BCX correcto, pero no conocido para el participante A. Por lo tanto, el participante A supone que fue liberada su transacción por el valor de 100,00 euros al número de cuenta 123456789, mientras que en segundo plano realmente fue legitimada por el participante A una transferencia a la cuenta del agresor, por un valor de 50.000,00 euros.

La realización del procedimiento de ataque explicado se simplifica considerablemente en particular en el caso de la utilización de los así llamados ordenadores de tableta o teléfonos inteligentes, ya que los dispositivos de esa clase están diseñados del mismo modo para el acceso a Internet, así como también para la recepción de SMS. Puesto que ambos dispositivos 1, 4 coinciden en este caso en un único dispositivo, es suficiente con la instalación de un programa troyano en el dispositivo terminal utilizado, donde ese troyano asume entonces las dos funciones de los troyanos 20, 30 representados en la figura 1.

La figura 2a muestra el procedimiento según la invención para la autentificación de un participante A en el caso de la utilización de un servicio de banca electrónica. El procedimiento básico, en el sentido más amplio, corresponde al procedimiento de la figura 1. Conforme a ello, las características u objetos idénticos se indican en las figuras 1, 2 con los mismos símbolos de referencia.

El participante, mediante la conexión de Internet del ordenador 1, autoriza al banco para efectuar una transferencia por el valor de 100 euros al número de cuenta 123456789. El participante efectúa las entradas necesarias para ello mediante la interfaz web del servidor bancario 2.

A diferencia del procedimiento de autentificación conocido de la figura 1, sin embargo, el servidor bancario 2 no transmite el código de autentificación /TAN correspondiente en texto claro con un SMS, al dispositivo terminal 4 del participante A. Más bien, el servidor bancario inicia el envío del SMS mediante la red de radio móvil 3, hacia el dispositivo terminal 4, donde el SMS 70 transmitido contiene una trama de puntos 71 que representa una forma codificada del código de autentificación requerido o bien del TAN móvil. Un agresor podría interceptar el SMS 70 transmitido en cualquier punto del sistema, pero no podría deducir o leer la información necesaria para confirmar una orden de transferencia manipulada.

La transmisión por SMS es sólo un ejemplo. Para la invención es posible en principio cualquier otra forma de transmisión del código de autentificación. Se considera por ejemplo la transmisión por MMS, WAP-Push-SMS, etc.

Para decodificar la trama de puntos 71, el participante A posee la lámina 60 semitransparente que está conformada individualmente para cada participante del procedimiento de autentificación. Colocando o situando la lámina delante de la unidad de visualización del dispositivo terminal 4, la trama de puntos 71 se transforma en el código de autentificación 72 legible, tal como se muestra en la figura 2b.

El TAN proporcionado por el servidor bancario 2 para la respectiva transacción y aún no codificado, junto con los datos distintivos del participante A, por ejemplo el número telefónico del participante A, se envía a un medio de asociación de la red de radio móvil 3. El medio de asociación comprende una base de datos que asocia a los participantes individuales de la red de radio móvil 3 datos correspondientes que se refieren a la particularidad y la ejecución de su lámina individual de participante. Los datos asociados al participante A se ponen a disposición de un medio generador, de manera que en base a los datos obtenidos codifica el TAN y genera la trama de puntos 71 específica del participante. Además, a través del medio generador se inicia y realiza el envío de SMS correspondiente, del SMS 71.

El presente ejemplo de ejecución se refiere a una transacción con un banco. En este punto cabe señalar que la presente invención naturalmente no está limitada sólo a transacciones bancarias, sino que también puede aplicarse a otros servicios, como por ejemplo procesos de venta. De este modo, con la presente invención también es posible efectuar una compra por Internet, donde en este caso un banco no participa de la transacción, sino cualquier empresa que ofrece productos o servicios en Internet.

Es posible que la lámina o su soporte, como por ejemplo una tarjeta o similares, estén realizados de modo que diferentes servicios, como por ejemplo transacciones bancarias, procesos de compras, etc., puedan realizarse con una lámina.

Para aumentar aún más la seguridad del procedimiento según la invención y detectar intentos de manipulación potenciales de modo fiable, siempre un símbolo que puede definirse del modo deseado se integra en la cadena de caracteres del TAN/código de autentificación. En el ejemplo representado en la figura 2, detrás del segundo caracter del TAN 72 se encuentra integrado un símbolo de flor 73 que previamente fue determinado por el participante A. Además, para el participante A es conocida la posición previamente determinada del símbolo 71 dentro de la cadena de caracteres 72. Por ejemplo, el tipo de símbolo y la posición del símbolo podrían variar para cualquier transacción posterior o podrían determinarse nuevamente.

Además, a través de la entrada incorrecta reiterada del TAN en el ordenador 1, el procedimiento de autentificación puede bloquearse para el participante A, para excluir posibles ataques estadísticos.

La figura 3 muestra la estructura de la lámina según la invención, mediante una representación de la sección transversal. La función de decodificación de la lámina 60 se determina a través de una pluralidad n de capas 1...n que se sitúan unas sobre otras, con una permeabilidad a la luz diferente. Las superficies blancas y negras de las capas n individuales indican la permeabilidad a la luz puntual de cada capa, donde una superficie blanca señala una permeabilidad a la luz comparativamente elevada, y una superficie negra señala un área casi no permeable a la luz. Por ejemplo, un punto de imagen 74 de la trama de puntos 71 está marcado en el lado inferior de la lámina. Los haces de luz emitidos desde el punto de imagen 74 se desvían a través de la disposición de capas 1...n de la lámina 60 y desplazan por tanto la percepción de la imagen del punto 74 al punto 75. La trama de puntos 71 de la figura 2a, por consiguiente, puede transformarse en la cadena de caracteres 72 legible a través de la colocación de la lámina 70 sobre la representación de la trama 71.

La cantidad n de las capas por lámina 60, así como su conformación individual, define las propiedades individuales del participante de cada lámina 60. Además, el dimensionamiento espacial de las capas, así como de la lámina 60 como totalidad, es determinante para la cantidad de posibilidades de variación de la trama de puntos 71.

La figura 4 muestra un posible ejemplo de ejecución de la lámina 60. En la representación mostrada, la lámina 60 se encuentra integrada en una tarjeta de débito conocida que está realizada como tarjeta EC 80. La totalidad de la lámina 60 comprende una ventana de decodificación 61 que comprende la estructura explicada de la figura 3. La integración de la lámina 60 en una tarjeta de débito o tarjeta EC permite que llevar diariamente la lámina sea especialmente cómodo para el participante A. Para la decodificación, la tarjeta de débito 80 se posiciona sobre la pantalla del teléfono móvil 4, donde la ventana de decodificación 61 cubre de forma precisa un área de visualización del dispositivo marcada de forma separada, para posibilitar una transformación sin errores de la trama de puntos 71 en el texto claro 72.

[0058] Otra posibilidad de aplicación ventajosa de la lámina según la invención consiste en proporcionar una lámina a una tarjeta de crédito, tarjeta de débito u otra tarjeta, como por ejemplo una tarjeta de legitimación o tarjeta de identificación. Gracias a ello es posible verificar la respectiva tarjeta en cuanto a su validez o autenticidad. Por ejemplo, es posible que la tarjeta presente al menos un primer código con el cual pueda identificarse la tarjeta o su usuario. Como ejemplo se considera una banda magnética o un chip. A través de la lámina puede entonces verificarse la corrección de ese código, por ejemplo de manera que se determine que la información decodificada a través de la lámina confirma la corrección del código mencionado o corresponde a dicho código.

En un ejemplo de ejecución concreto es posible que el usuario introduzca una tarjeta de débito en un cajero automático, la cual puede estar realizada por ejemplo como tarjeta EC, para extraer dinero. En ese caso, por una parte, es leída información almacenada en la banda magnética o en otro medio, como por ejemplo un chip. Además, el cajero automático está diseñado de modo que el mismo conduce una señal determinada, por ejemplo óptica, a través de la lámina, y verifica cómo la lámina ha decodificado esa señal. Si la información decodificada es compatible con las otras características de identificación de la tarjeta, preferentemente personalizadas, la tarjeta se considera como auténtica, o de lo contrario como no válida.

Naturalmente, este ejemplo no está limitado a una tarjeta para realizar una transacción bancaria, sino que aplica también para tarjetas para realizar otros procesos, como por ejemplo movimientos de pedidos o similares.

REIVINDICACIONES

1. Procedimiento para la autentificación de un participante (A) en una red de comunicaciones (3), donde al participante (A), hacia al menos un dispositivo terminal (4), se transmite un código de autentificación (72) codificado para una entrada de autentificación, donde el código de autentificación (72) codificado representado en la unidad de visualización del dispositivo terminal (4) se decodifica colocando delante una lámina (60) y el código de autentificación (72) decodificado se ingresa para la autentificación del participante (A) en la red de comunicaciones (3), caracterizado porque un símbolo (73) adicional que debe ser definido por el participante (A) se utiliza respectivamente en una posición determinada o variable del código de autentificación (72).

2. Procedimiento según la reivindicación 1, caracterizado porque el código de autentificación (72) codificado transmitido comprende una trama de puntos aleatoria (71), donde colocando delante la lámina (60) se vuelve visible un código de autentificación (72) legible.

3. Procedimiento según la reivindicación 1 ó 2, caracterizado porque una codificación del código de autentificación (72) tiene lugar antes de la transmisión, considerando la lámina (60) utilizada, individual del participante, del participante (A) receptor.

4. Procedimiento según una de las reivindicaciones precedentes, caracterizado porque la representación del código de autentificación (72) codificado y la entrada del código de autentificación (72) decodificado tienen lugar mediante un dispositivo terminal.

5. Procedimiento según una de las reivindicaciones precedentes, caracterizado porque la representación del código de autentificación (72) codificado y la entrada del código de autentificación (72) decodificado tiene lugar mediante diferentes dispositivos terminales (4), donde la transmisión del código de autentificación (72) codificado, o bien la transmisión de la instrucción de entrada entre los dispositivos terminales (4) y la red de comunicaciones (3) tiene lugar eventualmente mediante canales de comunicaciones diferentes.

6. Procedimiento según una de las reivindicaciones precedentes, caracterizado porque el procedimiento para la autentificación de un participante (A) se utiliza para un servicio de banca electrónica y/o un acceso VPN y/o la entrada en servidores web o servidores de correo electrónico (2).

7. Procedimiento según una de las reivindicaciones precedentes, caracterizado porque el código de autentificación (72) codificado se transmite a un dispositivo terminal (4) móvil mediante un canal de radio, en particular por SMS, MMS, WAPPush-SMS o similares.

8. Procedimiento según una de las reivindicaciones precedentes, caracterizado porque después de una o de varias entradas incorrectas del código de autentificación (72) decodificado tiene lugar un bloqueo del participante.

9. Utilización de una lámina (60) para ejecutar el procedimiento según una de las reivindicaciones 1 a 8, caracterizada porque la lámina (60) se compone de varias capas (1 ... n) con una permeabilidad a la luz diferente.

10. Utilización de una lámina (60) para ejecutar el procedimiento según una de las reivindicaciones 1 a 8, caracterizada porque la lámina (60) se compone de un tejido de fibra de vidrio colado.

11. Utilización de la lámina (60) según una de las reivindicaciones 9 ó 10, caracterizada porque la lámina (60) puede ser llevada en un llavero.

12. Utilización de un objeto personalizado, en particular tarjeta de crédito (80), tarjeta de débito, tarjeta de legitimación, tarjeta de identificación, documento de identidad, permiso de conducir, tarjeta de acceso a una empresa, para ejecutar el procedimiento según una de las reivindicaciones 1 a 8, caracterizada porque el objeto (80) está realizado con al menos una lámina (60) que es adecuada para decodificar un código (72), donde la lámina (60) preferentemente está diseñada según la parte distintiva de una de las reivindicaciones 9 a 11.

13. Red de comunicaciones (3), en particular red de telecomunicaciones o red de radio, con uno o con varios dispositivos terminales del participante (3) y con medios para ejecutar el procedimiento según una de las reivindicaciones 1 a 8.

14. Red de comunicaciones (3) según la reivindicación 13, donde la red de comunicaciones (3) presenta un medio de asociación que permite una asociación de cada lámina (60) individual específica de la persona a uno o a varios participantes individuales de la red, y comprende un medio generador que codifica uno o varios códigos de autentificación (72) considerando los datos del medio de asociación y eventualmente los transmite a los participantes (A) correspondientes.

Fig. 1a) (Estado del arte)

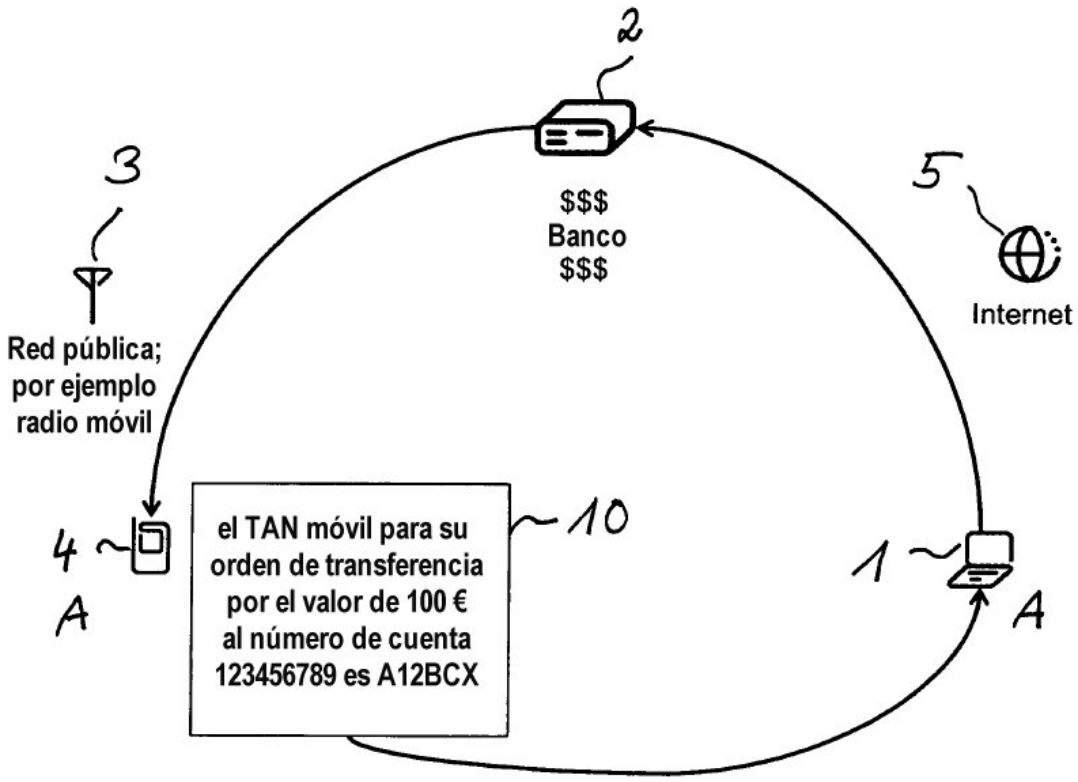

Fig. 1b) (Estado del arte)

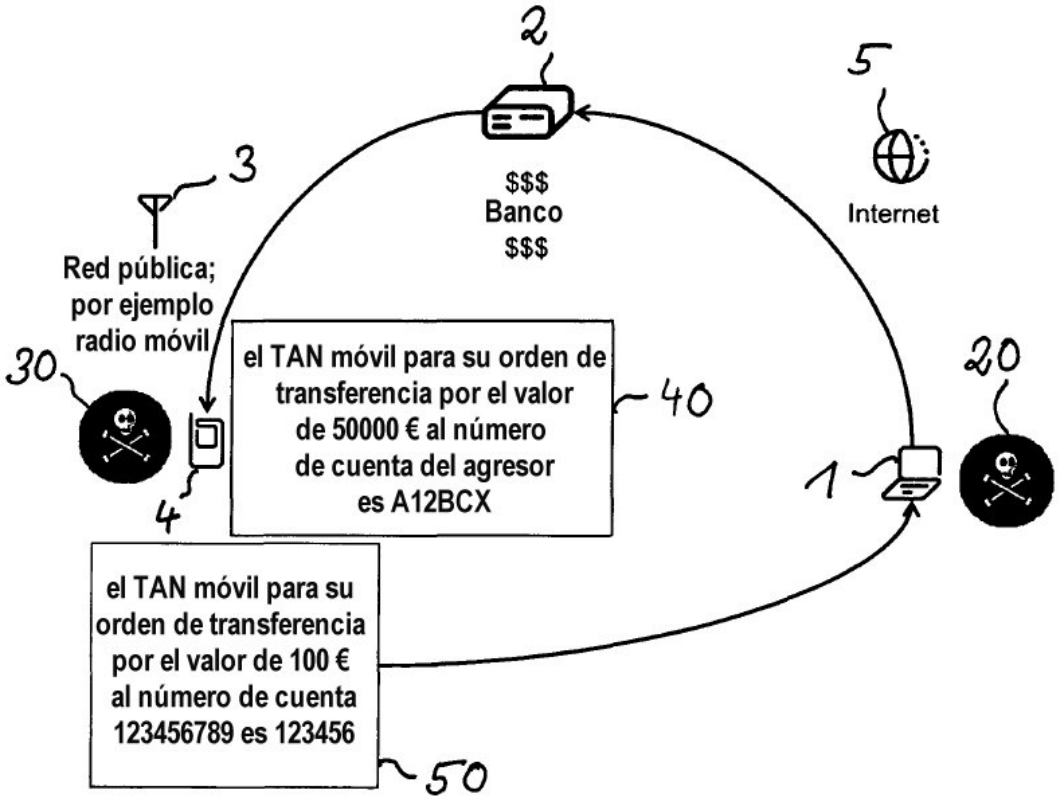

Fig. 2a)

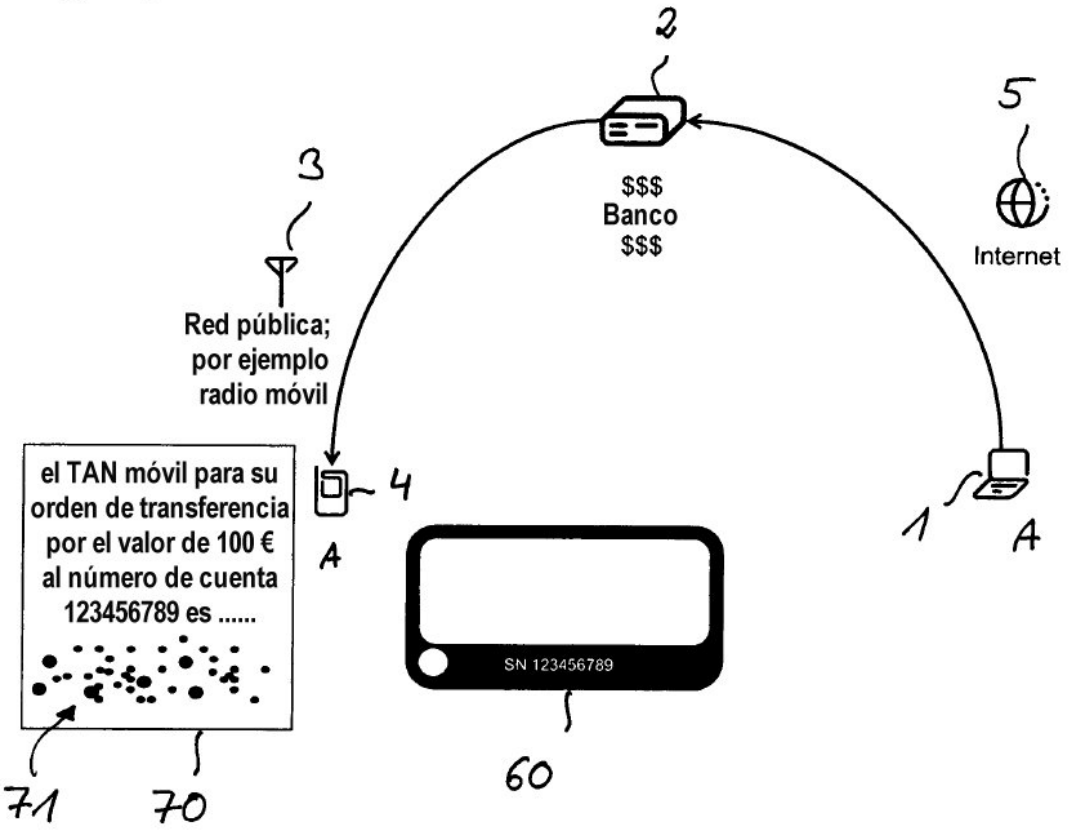
2
5
3
$$$
Banco
$$$
Internet
Red pública;
por ejemplo
radio móvil
el TAN móvil para su
orden de transferencia
por el valor de 100 €
al número de cuenta
123456789 es .....
4
A
1
A
SN 123456789
60
71
70

Fig. 2b)

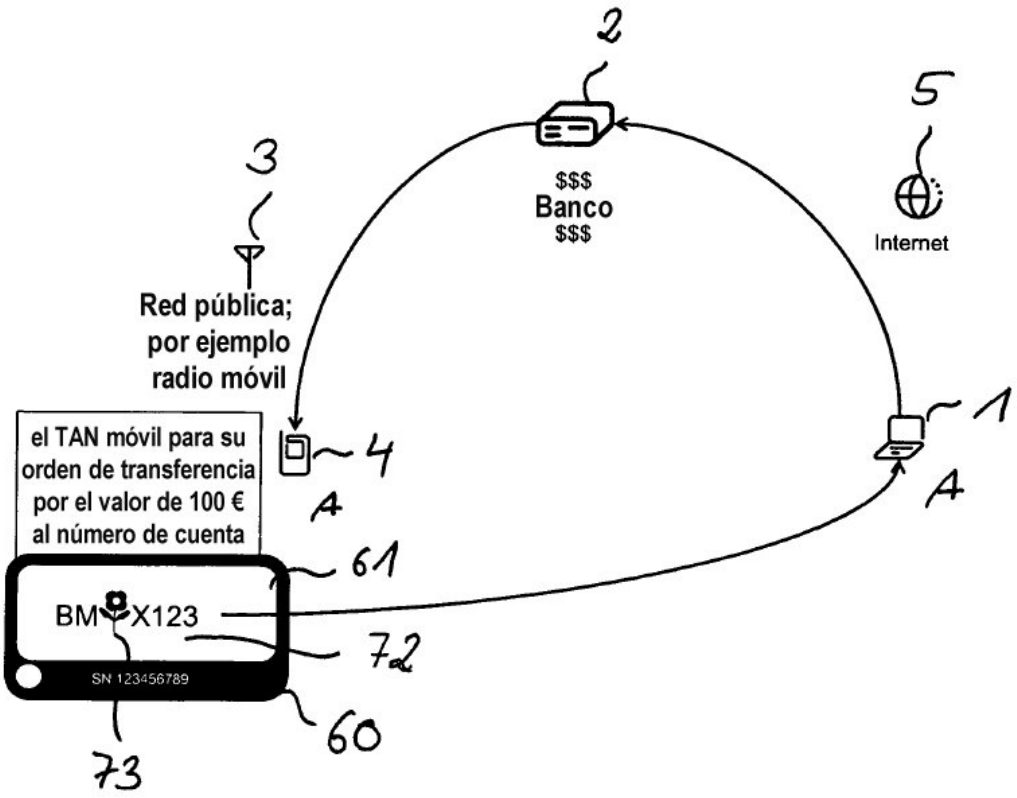
2
5
3
$$$
Banco
$$$
Internet
Red pública;
por ejemplo
radio móvil
el TAN móvil para su
orden de transferencia
por el valor de 100 €
al número de cuenta
4
A
1
A
61
BM X123
72
SN 123456789
60
73

Fig. 3

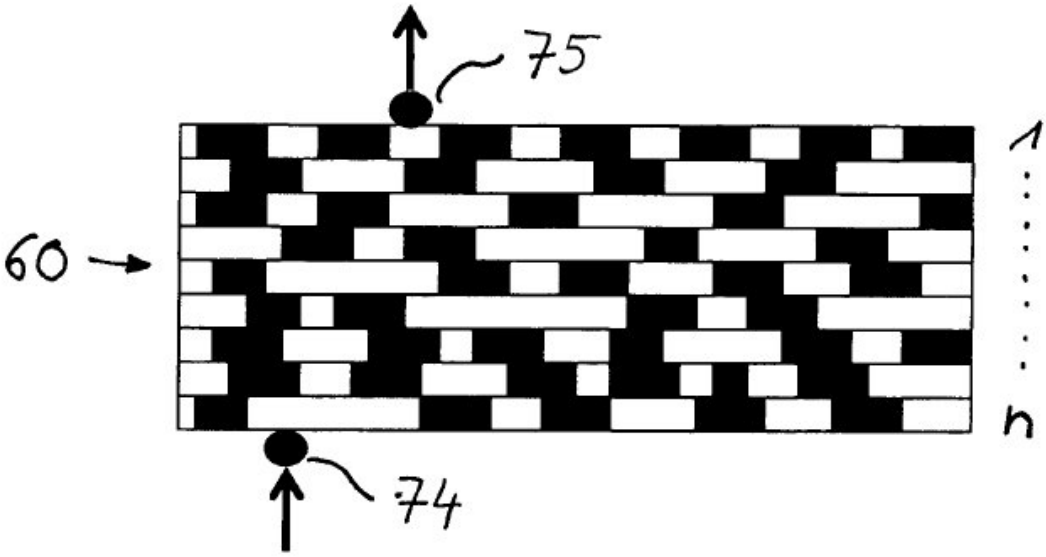

Fig. 4