(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 809 875**

(51) Int. CI.:

G09C 1/00 (2006.01)
G06F 21/34 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **26.02.2013 E 13156807 (3)**

(97) Fecha y número de publicación de la concesión europea: **20.05.2020 EP 2639732**

(54) Título: **Procedimiento y dispositivos de protección de la introducción de un código alfanumérico, de la producción de un programa de ordenador y medios de almacenamiento correspondiente**

(30) Prioridad:

13.03.2012 FR 1252268

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.03.2021

(73) Titular/es:

INGENICO GROUP (100.0%)
28-32 Boulevard de Grenelle
75015 Paris, FR

(72) Inventor/es:

ROTSAERT, CHRISTOPHER

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento y dispositivos de protección de la introducción de un código alfanumérico, de la producción de un programa de ordenador y medios de almacenamiento correspondiente

1. Campo de la invención

El campo del invento es el de la introducción de un código alfa-numérico de un usuario, por ejemplo, de un código confidencial (código PIN, por “Personal Identity Number”, en inglés), en el marco de una transacción bancaria o para acceder a un servicio protegido y con seguridad.

De una manera más precisa, el invento se refiere a una técnica de protección de tal introducción, siendo los datos del código confidencial datos sensibles.

El invento se aplica especialmente, pero no exclusivamente, en la introducción de tales códigos en dispositivos no protegidos, tales como terminales móviles o en accesorios de pago, llamados incluso “readers”, conectados a los dispositivos no protegidos.

El invento no está limitado a un tipo particular de dispositivos o de utilización de un código alfanumérico.

2. Antecedentes tecnológicos

El fuerte desarrollo actual de los medios de pago con la ayuda de terminales móviles (tales como los teléfonos móviles) necesita desarrollar igualmente unos medios adaptados a la protección de tales transacciones, debido al carácter no protegido de estos terminales, contrariamente a las transacciones “clásicas” protegidas.

En efecto, ofrecer la posibilidad de pagar, por ejemplo, con su teléfono móvil debe verse acompañada por unos medios de protección adaptados a este modo de pago, y especialmente de unos medios de protección de la introducción del código confidencial, clásicamente utilizado para validar el pago.

Actualmente, se conocen técnicas de pago a través de un terminal móvil utilizando un accesorio de pago que se conecta al terminal móvil, ofreciendo un dispositivo que reemplaza a un terminal de transacción clásico bien conocido.

Este accesorio de pago conectado al terminal móvil que sirve de terminal de pago permite especialmente leer los datos de una tarjeta bancaria y transmitir estos datos al terminal móvil (mediante una transmisión hacia un servidor protegido, por ejemplo).

El interés de tal accesorio de pago reside en su pequeño coste y en su facilidad de utilización (se conecta, por ejemplo, a través de una toma de jack a la salida de audio del terminal móvil).

Un ejemplo de tal accesorio de pago está ilustrado en la figura 1, en la que se puede ver un accesorio de pago 10, conectado a un terminal móvil 11, que permite leer una tarjeta bancaria 12.

A continuación, de una manera clásica, después de haber leído los datos de la tarjeta bancaria a través del accesorio de pago, el terminal móvil requiere la introducción de su código confidencial por parte del usuario, en el mismo terminal móvil, que no presenta el nivel de seguridad requerido para los datos bancarios.

Existe actualmente un cierto número de técnicas de protección de la introducción de un código alfanumérico confidencial en un terminal no protegido.

Por ejemplo, existe una técnica llamada “Revo PIN”, descrita especialmente en el documento de la patente WO2010131218_A1, consistente en transmitir al terminal móvil por parte de un servidor protegido, un teclado virtual de uso único, estando las teclas del teclado virtual permutadas con respecto a un teclado “clásico”. Este teclado virtual aparece en el terminal móvil y es en este teclado virtual donde el usuario introduce su código PIN. El código transmitido a continuación al servidor protegido, es, por lo tanto, de hecho, un código permutado, pudiendo volver a encontrar el servidor protegido el código PIN de origen gracias al teclado virtual único que él mismo genera para la transacción.

Esta técnica permite no transmitir el código PIN del usuario al servidor, pero no asegura tampoco el nivel de seguridad suficiente.

En efecto, al estar presentes las informaciones del código permutado y el teclado virtual y, por lo tanto, ser parcialmente accesibles en el terminal móvil, el código PIN puede ser recuperado, por ejemplo, por una aplicación malintencionada que tenga acceso, en el terminal móvil, a estas dos informaciones.

Por otra parte, en el caso de un código PIN con redundancia de cifras, este tipo de solución genera una pérdida de entropía puesto que es posible deducir del código permutado la presencia y la posición relativa de las cifras del código de partida.

Los documentos US 2010/242104 A1, DE 10 2007 043843 A1 y WO 2009/069872 A1 describen unos procedimientos de protección de las transacciones que impliquen el cifrado de un código de un usuario por unos códigos de uso único que se han obtenido por un dispositivo distinto que el utilizado para la introducir el código.

Existe, por lo tanto, una necesidad real de proteger estas técnicas anteriores de introducción de un código alfanumérico confidencial en un terminal no protegido.

3. Objetivos de la invención

El invento, en al menos un modo de realización, tiene como objetivo especialmente paliar estos diferentes inconvenientes del estado de la técnica.

De una manera más precisa, en al menos un modo de realización del invento, un objetivo es el de proporcionar una técnica de protección de la introducción de un código alfanumérico confidencial que permita reducir muy fuertemente, e incluso evitar, los riesgos de espionaje de tal introducción, en un entorno no protegido completamente.

Al menos un modo de realización del invento tiene como objetivo igualmente proporcionar una técnica tal sin necesitar otro dispositivo que los que están a disposición en el comercio, por ejemplo, su terminal móvil y un accesorio de pago conectado.

Un objetivo más del invento, según un modo de realización, es el de proporcionar una técnica de protección que permita no tener acceso a los datos sensibles (por ejemplo, a un código confidencial) nada más que en el dispositivo protegido, por ejemplo, en un servidor protegido.

Otro objetivo de al menos un modo de realización del invento es el de proporcionar una técnica tal que sea sencilla de utilizar y poco costosa.

4. Exposición de la invención

En un modo particular del invento, se ha propuesto un procedimiento de protección de la introducción de un código alfanumérico por parte de un usuario, que utiliza las siguientes etapas:

• obtención, por parte de un primer dispositivo, de unos medios de conversión de al menos una porción del código alfanumérico en al menos una porción de código convertido, siendo la tabla de conversión de uso único;

• introducción, en un segundo dispositivo distinto del primer dispositivo, de al menos la porción del código convertido con la ayuda de unos medios de conversión.

De esta manera, el procedimiento según un modo de realización del invento permite proteger la introducción de un código alfanumérico, por una parte, utilizando un código convertido y no el código alfanumérico confidencial del usuario, y, por otra parte, separando, en dos dispositivos distintos, la introducción misma de la conversión del código confidencial.

Para ello, el procedimiento según un modo de realización del invento prevé obtener, en un primer dispositivo, unos medios de conversión del código confidencial del usuario, en un código convertido que será introducido de una manera efectiva en un segundo dispositivo. De esta manera, cada uno de los dos dispositivos no tiene acceso nada más que a una o a otra de las dos informaciones que son el código confidencial y los medios de conversión, pero no a las dos informaciones, asegurando de esta manera la protección de la introducción del código confidencial.

Además, estos medios de conversión, por ejemplo, bajo la forma de una tabla de conversión, son de uso único. Esto permite reforzar la protección, no pudiendo ser “deducidos” los medios de conversión por una observación malintencionada de varias introducciones sucesivas de los códigos convertidos.

Por otra parte, está previsto utilizar unos medios de conversión para un código alfanumérico completo, o para una porción solamente de un código alfa-numérico.

De esta manera, por ejemplo, según una primera variante, los primeros medios de conversión se obtienen para convertir todos los caracteres de un código confidencial alfanumérico, y se obtienen unos nuevos medios de conversión para la introducción ulterior de otro código confidencial.

Según otra variante, los primeros medios de conversión se obtienen para convertir un solo carácter de un código confidencial alfanumérico. Es necesario, por lo tanto, en este caso, tantos medios de conversión distintos como caracteres del código alfanumérico para la introducción completa del código.

Según una característica particular, el procedimiento de protección utiliza una etapa de transmisión de al menos una porción del código convertido hacia un servidor protegido.

De esta manera, el código convertido, o una porción del código convertido, es transmitido, por lo tanto, hacia un servidor protegido, de tal manera que es tratado de una forma protegida.

De esta manera, el código confidencial del usuario no es transmitido, solo es transmitido el código convertido, no siendo, por lo tanto, deducible el código confidencial de origen por una aplicación o por un dispositivo, que no conozca la tabla de conversión. La seguridad de la introducción del código confidencial se ve, por lo tanto, reforzada.

Según una característica particular, la etapa de obtención obtiene igualmente una información de identificación de los medios de conversión y la etapa de transmisión transmite igualmente la información de identificación de los medios de conversión.

De esta manera, a cada obtención de los medios de conversión está asociado un identificador, que permite ulteriormente conocer qué medios de conversión se han utilizado para la conversión del código.

De esta manera, la transmisión, hacia un servidor protegido, de este y tener conocimiento de todas las informaciones necesarias para la reconstrucción del código confidencial de origen, cuando recibe un código convertido.

Según una característica particular, la etapa e obtención incluye una sub-etapa de visualización de los medios de conversión obtenidos.

De esta manera, el usuario puede convertir su código confidencial y obtener un código convertido visualizando los medios de conversión visualizados en el primer dispositivo e introducir a continuación el código convertido obtenido en el segundo dispositivo.

Según una característica particular, la etapa de obtención obtiene los medios de conversión y/o la información de identificación de la tabla de conversión por parte del servidor protegido.

De esta manera, se protege en mecanismo de introducción del código confidencial en la medida en la que el tratamiento del código convertido se efectúa en el seno de un servidor protegido que solo tiene conocimiento a la vez del código convertido introducido (transmitido) y de los medios de conversión a utilizar (proporcionados por el servidor protegido mismo).

Según una característica particular, los medios de conversión convierten una cifra en una letra.

De esta manera, se mejora más la protección suprimiendo el riesgo de que el usuario meta de una manera inadvertida su código confidencial numérico y no el código convertido.

Según un uso particular, el procedimiento de protección incluye, antes de la etapa de transmisión, una etapa de cifrado de al menos la porción de código convertido.

En esta utilización particular, la protección del mecanismo de introducción del código confidencial se ve reforzada incluso por el cifrado (según un método conocido y no detallado aquí) del código convertido, antes de su transmisión hacia el servidor protegido. De esta manera, no solamente no se transmite el código confidencial del usuario, sino que se transmite el código convertido cifrado, disminuyendo todavía más los riesgos de obtención del código de origen por el espionaje de la introducción y de la transmisión del código convertido.

Según una característica particular, la etapa de cifrado utiliza igualmente el cifrado de la información de identificación de los medios de conversión.

De esta manera, se mejora todavía más la protección al no transmitir claramente el identificador de los medios de conversión utilizados asociados al código convertido transmitido. Por lo tanto, no se transmite de una manera clara ninguna información, ni el código convertido ni el identificador de los medios de conversión utilizados.

Según un modo de realización particular, el primero y el segundo dispositivos son respectivamente un dispositivo de un comercial implicado en una transacción que necesita la introducción del código alfanumérico y un accesorio de pago conectado al dispositivo del comercial.

En este modo de realización particular, el terminal del comercial recibe, por parte del servidor protegido, unos medios de conversión de un código alfa-numérico en un código convertido y los visualiza, de manera que el usuario pueda servirse de ello para convertir su código confidencial, íntegramente o por porciones sucesivas, en un código (o en unas porciones de código) convertido.

Una vez obtenido su código convertido, o una porción del código convertido, el usuario lo (la) introduce en un accesorio de pago conectado al terminal del comercial, accesorio que ha servido previamente para la lectura de los datos de la tarjeta bancaria del usuario, por ejemplo.

De esta manera, según este modo de realización particular, el terminal del comercial no tiene conocimiento del código convertido, que se introduce en el accesorio de pago, y el accesorio de pago no tiene conocimiento de los medios de conversión, que son conocidos y visualizados únicamente por el terminal del comercial.

Según una característica particular de este modo de realización particular, los medios de conversión son transmitidos al primer dispositivo por el segundo dispositivo.

Por ejemplo, es el accesorio de pago el que genera una tabla de conversión y la transmite al terminal del comercial. El accesorio de pago puede, a continuación, por ejemplo, cifrar el código convertido, incluyendo al identificador de la tabla de conversión utilizada, y transmitir al servidor las informaciones cifradas que le permitan encontrar el código confidencial, sin que se haya transmitido ninguna información de forma clara. En este caso, es preferible entonces que el accesorio de pago sea protegido.

Según otro modo de realización particular, el primero y el segundo dispositivos son respectivamente un accesorio de pago conectado a un dispositivo de un comercial implicado en una transacción que necesita la introducción del código alfanumérico y el dispositivo del comercial.

De esta manera, según este modo de realización particular, es el accesorio de pago el que genera y visualiza los medios de conversión, y es en el terminal del comercial donde el usuario introduce un código convertido.

Según otro modo de realización particular más, el primer y el segundo dispositivos son respectivamente un terminal móvil del usuario implicado en una transacción que necesita la introducción de un código alfanumérico y un accesorio de pago conectado a un dispositivo de pago de un comercial implicado en la transacción.

En este caso, el terminal móvil del usuario sirve para obtener y visualizar los medios de conversión, y el accesorio de pago sirve para introducir el código convertido. En nivel de seguridad aumenta de esta manera, al no utilizarse el terminal del comercial (que puede estar comprometido) para la introducción del código.

Según una característica particular, la etapa de transmisión se pone en marcha por parte del primer dispositivo o por parte del segundo dispositivo.

De esta manera, el código convertido introducido por el usuario puede ser transmitido directamente por el accesorio de pago, si posee los medios de transmisión, hacia el servidor protegido, o bien el accesorio de pago transmite el código convertido al terminal del comercial, que los hace seguir al servidor protegido.

Si el accesorio de pago no transmite directamente al servidor protegido el código convertido, es preferible que el accesorio de pago cifre este código antes de transmitirlo al terminal del comercial.

El invento se refiere igualmente a un producto de un programa de ordenador que incluye unas instrucciones del código del programa para la puesta en marcha del procedimiento descrito anteriormente (en uno cualquiera de sus diferentes modos de realización), cuando el citado programa se ejecuta en un ordenador o en un procesador.

El invento se refiere igualmente a un medio de almacenamiento legible por parte de un ordenador y no transitorio, almacenando un programa de ordenador que incluye un juego de instrucciones ejecutables por un ordenador o un procesador para poner en marcha el procedimiento citado anteriormente (en uno cualquiera de sus diferentes modos de realización).

En otro modo de realización del invento, se ha propuesto un dispositivo de protección para la introducción de un código alfanumérico de un usuario poniendo en marcha el procedimiento de protección citado anteriormente (en uno cualquiera de sus diferentes modos de realización).

De una manera ventajosa, el dispositivo de protección incluye unos medios de puesta en marcha de las etapas que efectúa en un procedimiento tal como el descrito precedentemente, en uno cualquiera de sus modos de realización.

El invento se refiere igualmente a un accesorio de pago que utiliza el procedimiento de protección citado anteriormente (en uno cualquiera de sus modos de realización).

De una manera ventajosa, el accesorio de pago incluye unos medios de puesta en marcha de las etapas que efectúa en el procedimiento descrito precedentemente, en uno cualquiera de sus diferentes modos de realización.

5. Lista de figuras

Otras características y ventajas del invento aparecerán con la lectura de la siguiente descripción, dada a título de ejemplo indicativo y no limitativo, y de los dibujos anexos, en los cuales:

-la figura 1, ya descrita en relación con la técnica anterior, presenta un ejemplo de un accesorio de pago conectado a un terminal móvil;

- la figura 2 ilustra las principales etapas del procedimiento de protección según un modo de realización particular del invento;

- la figura 3 presenta un ejemplo de sistema en el cual se pone en marcha el procedimiento según un modo de realización del invento; y

- la figura 4 presenta la estructura de un dispositivo de protección, según un modo de realización particular del invento.

6. Descripción detallada

6.1 Principio general

El principio general del invento se basa en la separación, en dos dispositivos distintos, de unos medios de conversión de un código alfanumérico en un código convertido, y de unos medios de introducción del código convertido, permitiendo de esta manera reforzar la seguridad de la introducción de un código alfanumérico confidencial, por ejemplo.

En un esfuerzo de simplificación, se utiliza a partir de ahora en la descripción el ejemplo de unos medios de conversión bajo la forma de una tabla de conversión.

Está claro que la técnica presentada a continuación, según diferentes modos de realización del invento, no está limitada a este ejemplo de medios de conversión.

6.2 Descripción de un primer modo de realización del invento.

Se presenta ahora, en relación con las figuras 2 y 3, las principales etapas del procedimiento de protección de la introducción de un código alfanumérico, así como un ejemplo de sistema en el cual el invento puede ser utilizado, según un modo de realización del invento.

En este modo de realización particular, los medios de conversión se obtienen para convertir un código alfanumérico completo, una variante, descrita en el párrafo siguiente, permitiendo la conversión de porciones de un código alfanumérico.

En este modo de realización, se utiliza una etapa 20 de obtención de los medios de conversión (por ejemplo, una tabla de conversión), de tal manera que permite al usuario convertir su código alfanumérico confidencial en un código convertido.

Esta etapa 20 de obtención se utiliza en un primer dispositivo, por ejemplo, y como está ilustrado en la figura 3, el terminal móvil 30 del comerciante, sobre el cual se hace la transacción. Es en efecto cada vez más frecuente para un comercial utilizar su terminal móvil para hacer las transacciones, en lugar de disponer de un terminal de transacción específico.

En este ejemplo, la tabla de conversión se transmite al terminal móvil 30 del comercial por parte del servidor protegido 32, a cargo de la validación de la transacción.

Según una segunda variante, no ilustrada, el primer dispositivo puede ser el accesorio de pago 31, o bien incluso un terminal móvil del usuario.

Una vez obtenida la tabla de conversión durante la etapa 20, por parte del primer dispositivo, éste la visualiza, sobre una pantalla 300, por ejemplo, de tal manera que el usuario tenga acceso a ella. Éste convierte entonces su código confidencial alfanumérico en un código convertido e introduce este código convertido, durante una etapa 21, en un segundo dispositivo.

Por ejemplo, y como está ilustrado en la figura 3, el segundo dispositivo corresponde al accesorio de pago 31, conectado al terminal móvil del comercial 30.

El segundo dispositivo incluye unos medios 310 de introducción del código convertido, por ejemplo, bajo la forma de un teclado, o de un panel resistivo imprimido, permitiendo esta alternativa especialmente reducir el coste de la implementación y utilizar esta misma superficie para introducir el código convertido y para introducir una firma del usuario (funcionalidad habitual para un accesorio de pago).

De esta manera, según este modo de realización, el terminal móvil del comercial no tiene conocimiento nada más que de la tabla de conversión y el accesorio de pago no tiene conocimiento nada más que del código convertido, de tal manera que la introducción del código por parte del usuario está fuertemente protegida.

En efecto, un mismo dispositivo implicado en el procedimiento según este modo de realización del invento, ya sea el terminal móvil del comercial, o el accesorio de pago, no tiene conocimiento de las dos informaciones (la tabla de conversión y el código convertido obtenido) necesarias para la reconstrucción del código de partida. Una aplicación

“espía” en uno o en otro de estos dos dispositivos no podría, por lo tanto, encontrar el código de partida, contrariamente a las técnicas anteriores.

Una tabla de conversión consiste, por ejemplo, en asociar una cifra a un carácter, como está ilustrado en la figura 3. Un interés de esta utilización particular reside en la conversión de un código alfanumérico en un código compuesto por letras, suprimiendo de esta manera el riesgo de que el usuario introduzca de una manera inadvertida su verdadero código confidencial numérico. En este caso, el teclado 310 del accesorio de pago presenta, por lo tanto, por ejemplo, únicamente letras, y no cifras.

Una vez introducido el código convertido por parte del usuario en el segundo dispositivo, éste lo transmite al servidor protegido 32.

Esta transmisión puede ser utilizada, según una primera variante, directamente por el accesorio de pago, si éste dispone de tales medios de transmisión. Esta variante permite en particular no introducir intermediarios en la transmisión, y, por lo tanto, conservar un nivel de seguridad óptimo.

Según una segunda variante, especialmente cuando el accesorio de pago no dispone de los medios de transmisión hacia el servidor protegido, el código convertido se transmite en primer lugar por parte del accesorio de pago 31 al terminal móvil del comercial 30, y éste, a continuación, transmite el código convertido hacia el servidor protegido.

Según otro aspecto particular de este primer modo de realización, el código convertido introducido por el usuario en el accesorio de pago 31 es cifrado (según un método conocido ya y no detallado aquí) por este último, antes de ser transmitido al servidor protegido 32. En efecto, el accesorio de pago es capaz de cifrar los datos, como los datos leídos de la tarjeta bancaria, y es juicioso utilizar esta capacidad para reforzar todavía más la seguridad de la introducción del código. De esta manera, no solamente la introducción del código convertido está separada de la tabla de conversión, en dos dispositivos distintos, sino que, además, el código convertido no es transmitido tal cual al servidor protegido, sino bajo una forma cifrada, únicamente descifrable por parte del servidor protegido (y del accesorio de pago).

Por otra parte, para que el servidor protegido pueda encontrar el código alfanumérico de partida, debe igualmente tender conocimiento de la tabla de conversión utilizada para obtener el código convertido que ha recibido.

De esta manera, la transmisión del código convertido debe ser acompañada por la transmisión de una información que permita encontrar esta tabla de conversión, por ejemplo, una información de identificación de la tabla de conversión.

En este modo de realización del invento, al ser transmitida la tabla de conversión al terminal móvil del comercial 30 por parte del servidor protegido 32, este último transmite igualmente una información de identificación de la tabla de conversión. Esta información es retransmitida a continuación al servidor con el código convertido asociado.

En la variante descrita anteriormente, en la cual el código convertido es cifrado por el accesorio de pago, el terminal móvil del comercial puede transmitir al accesorio de pago el identificador de la tabla de conversión, sin transmitir la tabla misma, de tal manera que el accesorio de pago cifre igualmente esta información de identificación de la tabla de conversión. En este caso, solamente las informaciones cifradas son transmitidas al servidor 32, el código convertido cifrado y el identificador de la tabla de conversión cifrado. Estas dos informaciones pueden eventualmente ser combinadas en un solo dato cifrado.

Por otra parte, como ya se ha indicado anteriormente, este modo de realización prevé que una tabla de conversión se obtenga para convertir un código alfanumérico completo, y que otra tabla de conversión se genere ulteriormente para convertir otro código alfanumérico.

Por ejemplo, (como está ilustrado en la figura 3), un código numérico compuesto por cuatro cifras “1234”es convertido en un código convertido de cuatro caracteres “CAEB”.

Una tabla de conversión es, por lo tanto, de un uso único, reforzando, de esta manera, la seguridad del procedimiento según el invento. En efecto, un observador malintencionado no puede deducir el código de partida observando varias introducciones sucesivas de un código convertido, al ser diferente la tabla de conversión para cada introducción.

6.3 Descripción de un segundo modo de realización del invento.

Según este segundo modo de realización, no ilustrado, una tabla de conversión se obtiene para convertir una porción de un código alfanumérico, y no un código alfanumérico completo.

En este caso, so obtienen varias tablas de conversión sucesivamente para convertir un código completo.

Este modo de realización permite evitar la pérdida de entropía relacionada con un código alfanumérico compuesto por varios caracteres idénticos, que sería convertido en un código convertido compuesto por varios caracteres idénticos, si se utilizase una sola tabla para convertir todos los caracteres del código.

De esta manera, si se considera una tabla de conversión de una cifra en una letra, cuyo ejemplo está ilustrado en la figura 3, y un código numérico compuesto por cuatro cifras, se obtienen sucesivamente cuatro tablas de conversión para convertir el código numérico completo.

Por ejemplo, se considera un código numérico compuesto por cuatro cifras “1234”, a convertir con la ayuda de las siguientes cuatro tablas de conversión sucesivas:

1C 2A 3E 4B 5F 6D 7H 8G 9J 0I: permite convertir el “1” en “C”,

1J 2B 3G 4I 5A 6H 7C 8D 9E 0F: permite convertir el “2” en “B”,

1A 2J 3B 4E 5C 6F 7D 8H 9I 0G: permite convertir el “3” en “B”,

1I 2J 3G 4H 5D 6F 7B 8E 9A 0C: permite convertir el “4” en “H”.

El código “1234” se convierte, por lo tanto, en “CBBH”.

Según una primera variante de este modo de realización, cada letra del código convertido puede ser transmitida al servidor protegido, progresivamente, acompañada por una información de identificación de la tabla de conversión utilizada.

Según una segunda variante, el código convertido completo es transmitido al servidor protegido, una vez convertidas las cuatro cifras del código de partida, así como los identificadores de las cuatro tablas de conversión utilizadas.

6.4 Ejemplo de la estructura del dispositivo de protección según un modo de realización del invento.

La figura 4 presenta la estructura de un dispositivo 30 de protección para la introducción de un código alfanumérico, según un modo de realización particular del invento. Este dispositivo utiliza la técnica presentada anteriormente (en uno cualquiera de los modos de realización, presentados en relación con las figuras 2 y 3).

En este ejemplo, el dispositivo incluye una memoria RAM 40 (por “Ramdom Access Memory”, en inglés), una unidad de tratamiento 41 (o CPU, por “Central Processing Unit”, en inglés), equipada, por ejemplo, con un procesador y pilotada por un programa almacenado en una memoria ROM 42 (por “Ready Only Memory”, en inglés). Al principio, las instrucciones del código del programa están cargadas, por ejemplo, en la memoria RAM 40 antes de ser ejecutadas por la unidad de tratamiento 41. La unidad de tratamiento 41 obtiene unos medios de conversión de al menos una porción de un código alfanumérico en al menos una porción del código convertido, según las instrucciones del programa 42, con el fin de utilizar la técnica presentada anteriormente (en uno cualquiera de los modos de realización).

Esta figura 4 ilustra únicamente una manera particular, entre varias posibles, de realizar la técnica presentada anteriormente.

REIVINDICACIONES

1. Procedimiento de protección para la introducción de un código alfanumérico por parte de un usuario durante una transacción, caracterizado por que utiliza las siguientes etapas:

-obtención, por parte de un primer dispositivo (30);

- de unos medios de conversión de al menos una porción del citado código alfanumérico en al menos una porción de un código convertido, siendo los citados medios de conversión de uso único e impidiendo la deducción del código de partida por la observación de varias introducciones sucesivas de un código convertido;

- de una información de identificación asociada a los citados medios de conversión, y permitiendo conocer cuáles son los medios de conversión que han sido utilizados para la conversión del código;

- introducción, en un segundo dispositivo (31) distinto del citado primer dispositivo (30), de al menos la citada porción del código convertido por parte del usuario con la ayuda de los citados medios de conversión obtenidos por parte del primer dispositivo (30);

- transmisión, hacia un servidor protegido (32) a cargo de la validación de la transacción, de al menos la citada porción del código convertido y de la citada información de identificación de los citados medios de conversión, permitiendo, de esta manera, al citado servidor (32) identificar los medios de conversión utilizados previamente para la conversión de la citada porción del código convertido con el fin de reconstruir el citado código alfanumérico de origen,

y por que los citados primer y segundo dispositivos (30, 31) son respectivamente un dispositivo de un comercial implicado en una transacción que necesita la introducción del citado código alfanumérico y un accesorio de pago conectado al citado dispositivo del citado comercial, y siendo transmitidos los medios de conversión al citado primer dispositivo (30) por parte del segundo dispositivo (31).

2. Procedimiento según la reivindicación 1, caracterizada por que la citada etapa de obtención incluye una sub-etapa de visualización de los citados medios de conversión obtenidos.

3. Procedimiento según la reivindicación 1, caracterizado por que incluye, antes de la citada etapa de transmisión, una etapa de cifrado de al menos la citada porción del código convertido.

4. Procedimiento según la reivindicación 1 y la reivindicación 3 caracterizado por que la citada etapa de cifrado utiliza igualmente el cifrado de la citada información de identificación de los citados medios de conversión.

5. Procedimiento según la reivindicación 1, caracterizado por que la citada etapa de transmisión se utiliza por parte del citado primer dispositivo o por parte del citado segundo dispositivo.

6. Producto de un programa de ordenador, que incluye unas instrucciones de código del programa para la utilización del procedimiento según al menos una de las reivindicaciones 1 a 5, cuando el citado programa se ejecuta en un ordenador o en un procesador.

7. Medio de almacenamiento legible por parte del ordenador y no transitorio, que almacena un programa de ordenador que incluye un juego de instrucciones ejecutables por parte de un ordenador o de un procesador para utilizar el procedimiento según al menos una de las reivindicaciones 1 a 5.

8. Dispositivo (30) de protección para la obtención de un código alfanumérico por parte de un usuario según el procedimiento de una de las reivindicaciones 1 a 5, caracterizado por que incluye unos medios de obtención de unos medios de conversión de al menos una porción de un código alfanumérico en al menos una porción de un código convertido.

9. Accesorio de pago (31), caracterizado por que incluye unos medios de introducción de al menos una porción de un código convertido según el procedimiento de protección para la introducción de un código alfanumérico por pate de un usuario de la reivindicación 1.

10. Dispositivo según la reivindicación 8 o la reivindicación 9, caracterizado por que incluye unos medios de transmisión de al menos una porción de un código convertido hacia un servidor protegido.

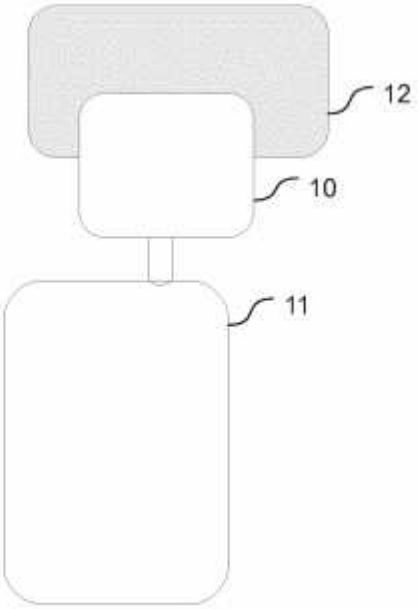

Figura 1

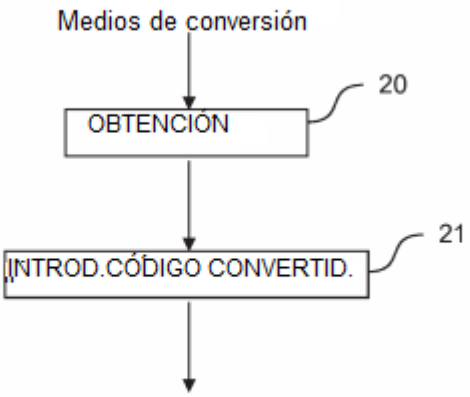

Figura 2

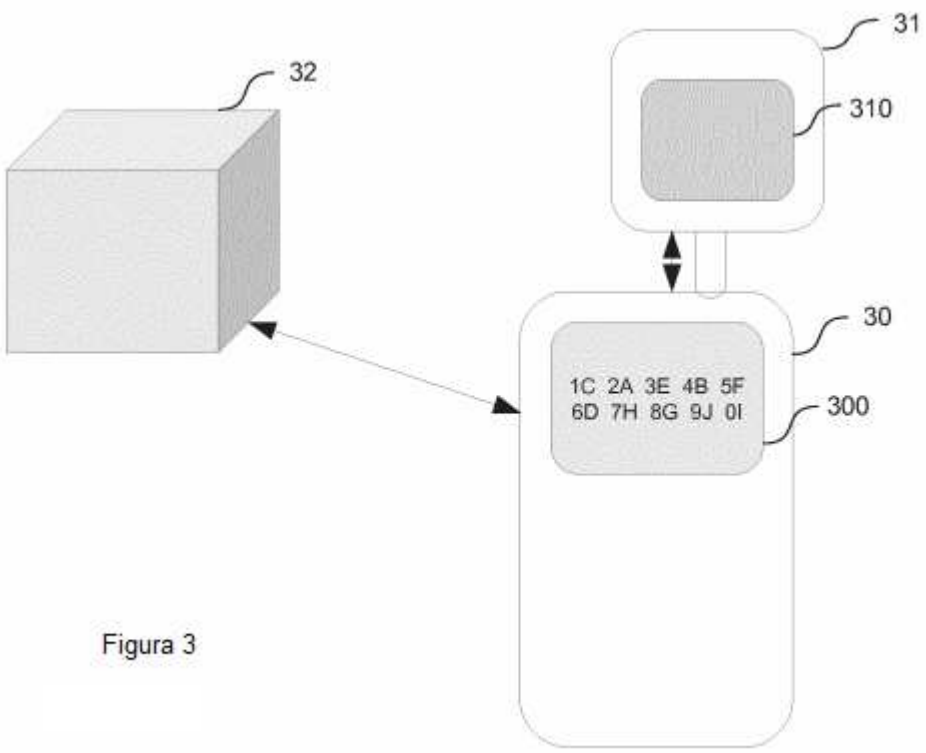

Figura 3

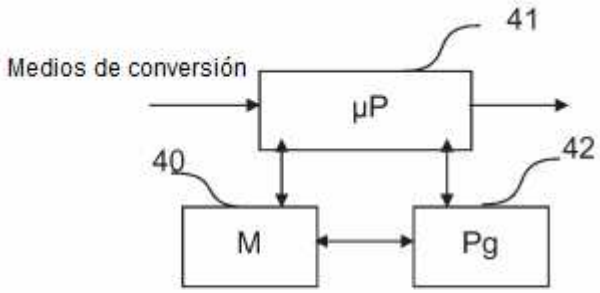

Figura 4