(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 386 259**

(51) Int. CI.:
G07F 7/10 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08291060 .5**
(96) Fecha de presentación: **12.11.2008**
(97) Número de publicación de la solicitud: **2187363**
(97) Fecha de publicación de la solicitud: **19.05.2010**

(54) Título: **Dispositivo y método de distribución de un número de identificación personal**

(45) Fecha de publicación de la mención BOPI:
14.08.2012

(45) Fecha de la publicación del folleto de la patente:
14.08.2012

(73) Titular/es:
OBERTHUR TECHNOLOGIES DENMARK A/S
TORRINGVEJ 15
DK-2610 RODOVRE, DK

(72) Inventor/es:
Aage, Peter y
Timm, Carsten

(74) Agente/Representante:
Linage González, Rafael

DESCRIPCIÓN

Dispositivo y método de distribución de un número de identificación personal

La presente invención se refiere a un dispositivo y un método de distribución de un número de identificación personal (PIN).

Cuando un cliente es titular de una cuenta, por ejemplo una cuenta bancaria, esta cuenta está asociada a uno o más instrumentos de transacciones, por ejemplo, tarjetas de débito o crédito. Para usar una tarjeta para hacer un pago, el cliente tiene que conocer el PIN asociado a la tarjeta. El procedimiento estándar para entregar una nueva tarjeta a un cliente es enviar la tarjeta por el correo o al banco donde se mantiene la cuenta del cliente, seguida, tras unos pocos días, por una carta que contiene el PIN asociado a la tarjeta.

Este método de distribuir números PIN tiene varios inconvenientes. En primer lugar, tanto la tarjeta como los números PIN se entregan por correo ordinario con una diferencia de pocos días. Esto brinda las siguientes posibilidades para un ataque por parte del “Hombre en el Medio” (“MITM”):

- el MITM puede recoger la tarjeta y el número PIN, activar la tarjeta y usarla, o

- el MITM puede copiar la tarjeta y copiar el número PIN.

Además, no es posible identificar quién está abriendo efectivamente la carta en la dirección del destinatario. Además, la distribución del número PIN es lenta, cara y limitada al domicilio del titular de la tarjeta. Mientras la carta que contiene el número PIN no esté debidamente destruida, hay un riesgo de que un tercero malintencionado la halle. Debido a que los números PIN no son fáciles de mantener en mente, la gente puede olvidarlo y luego dejar de usar sus tarjetas. Pero si la gente guarda una copia del número PIN cerca de la tarjeta, por ejemplo, en una billetera de un bolso de mano, aumentan los riesgos de falsificación o de uso por un tercero malintencionado. Para el emisor de la tarjeta, el actual método de entrega por correo usado para distribuir el número PIN no proporciona ninguna posibilidad de rastreo. Si el titular de la tarjeta finge que el correo con el PIN no ha sido entregado, el emisor no tiene ninguna información acerca de dónde está el correo con el PIN (por ejemplo, si se ha robado, se ha perdido o nunca ha sido enviado). Debido a que el número PIN y las tarjetas se envían mediante el mismo canal, es decir, el correo ordinario, un tercero, dentro o fuera del hogar, puede acceder fácilmente tanto a la tarjeta como al número PIN:

Se conoce del documento WO 2006 56 826 cómo proporcionar al cliente sus números de PIN mediante Internet, o mediante otros canales de comunicación, tales como un mensaje breve enviado al teléfono móvil del cliente.

Sin embargo, el envío no solicitado del número PIN al titular de la tarjeta tiene numerosos inconvenientes. En primer lugar, el cliente puede dejar el mensaje que contiene el número PIN disponible en su ordenador o su teléfono móvil, porque no solicitó su transmisión. En segundo lugar, debido a que el número PIN se entrega sin ser solicitado por el cliente, podría ser entregado a un teléfono perdido, robado o raramente usado, o podría ser destruido como un mensaje “spam” (mensaje no solicitado). Además, este método no implica un acuse de recibo enviado por el cliente. Además, un cliente que ha pedido más de una tarjeta recibe más de un PIN y puede confundirse al asociar números PIN y tarjetas.

La presente invención se orienta a remediar estos inconvenientes.

La solicitud de patente Nº US 2006 / 168 657 describe una solución para proporcionar a un dispositivo de usuario un conjunto de códigos de acceso. Según esta solución, se envía un código de Identificador al usuario; en un servidor, el código de Identificador es recibido de parte del usuario en un mensaje SMS y es usado a fin de extraer una clave para cifrar el conjunto de códigos de acceso. El conjunto cifrado de códigos de acceso se envía al usuario en un mensaje SMS.

La presente invención se refiere a un método de distribución de un código personal según lo definido en la reivindicación 1 adjunta.

Gracias a estas características, el emisor y el usuario se benefician de algunas ventajas significativas, en comparación con el PIN existente entregado por correo.

Por ejemplo, enviar un código personal a través de un canal electrónico (por ejemplo, una red de telefonía móvil) crea grandes ahorros para el emisor, dado que desaparece un buen número de costes, tales como la carta postal, la impresión, la administración de existencias, el trabajo, las impresoras, el mantenimiento y los sellos.

Además, debido a que casi todo usuario de instrumentos financieros tiene un teléfono móvil, el usuario tiene la oportunidad de extraer su código personal en cualquier parte y en cualquier momento.

Un tercero que conociera el código de solicitud no podría solicitar de manera válida y recibir luego el código

personal.

El método según la presente invención también proporciona al emisor características de rastreo, porque el usuario tiene que solicitar el número de identificación personal. El emisor tiene la oportunidad de saber si el código personal ha sido solicitado y recibido por el titular de la tarjeta.

Además, debido a que el código personal y el instrumento financiero asociado, preferiblemente, no se envían a través del mismo canal, se mejora la seguridad. En efecto, es mucho más difícil para un tercero acceder tanto al instrumento financiero como al código personal. Además, el método de la presente invención puede autenticar a quien recibe el código personal, porque el usuario puede ser identificado al solicitar el código personal.

En realizaciones específicas, durante la etapa de enviar el código de solicitud, se envía un instrumento financiero a un usuario mediante el primer canal, junto con el código de solicitud asociado a dicho instrumento financiero. Gracias a estas características, el usuario puede obtener el código personal en cuanto recibe el instrumento financiero. De esta manera, el usuario no necesita esperar unos pocos días antes de poder usar este instrumento financiero. En el caso de que el instrumento financiero sea una tarjeta y el código de solicitud se proporcione junto con la tarjeta, el código personal, es decir, el PIN, está potencialmente disponible para el titular de la tarjeta en cuanto se recibe la tarjeta, y puede ser extraído en cualquier momento.

Según estas características específicas, el método según la presente invención, tal como se ha estipulado sucintamente en lo anterior, incluye adicionalmente una etapa de descifrado del código personal usando el código de solicitud como una clave de descifrado. Gracias a estas características, cada código personal registrado está protegido por una clave específica que solamente conoce el usuario.

Según características específicas, ambos canales segundo y tercero son canales asegurados. Gracias a estas características, se protege la transmisión del código personal.

Según características específicas, el primer canal es un canal de entrega por correo. La entrega del código personal es rápida, fácil y puede ser iniciada en cualquier sitio, siempre que pueda accederse a una señal de red de telefonía móvil.

Gracias al hecho de que ambos canales segundo y tercero son una red para transmitir mensajes breves, la entrega del código personal es rápida, fácil y puede iniciarse desde cualquier sitio, siempre que pueda accederse a una señal de red de telefonía móvil. Además, el mensaje breve que contiene el código personal puede almacenarse en una memoria de teléfono.

Según otro aspecto, la presente invención se refiere a un medio de almacenamiento de información que puede ser leído por un ordenador o un microprocesador que almacene instrucciones de un programa de ordenador, que permita la implementación del método de la presente invención, según se ha estipulado brevemente en lo anterior.

Según otro aspecto más, la presente invención concierne a un programa de ordenador cargable en un sistema de ordenador, conteniendo dicho programa instrucciones que permiten la implementación del método de la presente invención, según se ha estipulado brevemente en lo anterior, cuando ese programa es cargado y ejecutado por un sistema de ordenador.

Dado que las ventajas, objetivos y características específicas de este medio de almacenamiento de información, y de este programa de ordenador, son similares a los del método de distribución del PIN, según se ha estipulado brevemente en lo anterior, no se repiten aquí.

Otras ventajas, fines y características de la presente invención surgirán de la siguiente descripción, presentada, con propósito explicativo que no es limitador en modo alguno, con respecto a los dibujos adjuntos, en los cuales:

- la figura 1 representa, en forma de un diagrama en bloques, una realización específica del dispositivo según la presente invención,

- la figura 2 muestra los campos del mensaje de solicitud del PIN y de un registro en una base de datos, y

- la figura 3 representa las etapas efectuadas para implementar una realización específica del método según la presente invención.

Incluso aunque, en la siguiente descripción, el único instrumento financiero descrito sea una tarjeta, la presente invención no está limitada a tal clase de instrumento financiero. Por el contrario, la presente invención abarca cualquier clase de instrumentos financieros, por ejemplo, códigos de transferencia por cable. De manera similar, la descripción solamente se refiere a un código secreto personal específico, llamado “PIN”, que es usualmente una secuencia de números. Sin embargo, la presente invención no se limita a tal clase de código personal secreto o contraseña, sino que se extiende a cualquier clase de código personal, incluso una secuencia de símbolos y, en

particular, de símbolos alfanuméricos.

Como se muestra en la figura 1, un servidor 180 de distribución de PIN contiene una tabla de registros 181. Como se muestra sobre la línea inferior de la figura 2, cada registro 200 en esta tabla se refiere a una y solamente una tarjeta, y contiene al menos la siguiente información: un número 205 de teléfono móvil del cliente, el PIN 210 para esa tarjeta, un código 215 de solicitud de PIN, un MAC (Código de Autenticación de Mensaje) 225 y un indicador 220 de entrega. El campo del código 215 de solicitud de PIN es el "campo de clave" de la tabla. El código 215 de solicitud de PIN tiene un valor que nunca aparece más de una vez dentro de la tabla. De esta manera, un código 215 dado de solicitud de PIN identifica a un y solamente un registro. El número 205 de abonado de teléfono móvil es el número de teléfono desde el cual el servidor 180 de distribución de PIN espera recibir el código 215 de solicitud de PIN asociado, y al cual enviará el PIN 210. El emisor 195 de la tarjeta habrá obtenido este número 205 de teléfono móvil de todos aquellos clientes que escogen tener sus PIN distribuidos por el SMS (acrónimo de "sistema de mensajes breves").

El indicador 220 de entrega se fija inicialmente en el valor "no entregado", y se fija en el valor "entregado" cuando se confirma la entrega del PIN al cliente.

El código 215 de solicitud de PIN es proporcionado por un proveedor 190 de datos. En otras variantes, el código de solicitud de PIN es generado por el Servidor 180 de Distribución de PIN o es suministrado por el emisor 195.

El PIN 210 es cifrado por el proveedor 190 de datos según la siguiente función de cifrado:

PIN cifrado = cifrado(cifrado(PIN, clave_de_zona), código-de-solicitud-de-PIN)

donde "cifrado(x,y)" es una función de cifrado, por ejemplo una función de cifrado DES (acrónimo de "Estándar de Cifrado de Datos"), con dos argumentos. El primer argumento son los datos a cifrar, es decir, el PIN, y el segundo argumento es la clave a usar para el cifrado. Como puede verse, este es un doble cifrado, en el cual el código de solicitud de PIN es la clave para la segunda ocurrencia de cifrado. La función de descifrado permite al servidor 150 de contenido de SMS o a un módulo 160 de seguridad de hardware recuperar el texto llano según la siguiente función de descifrado:

PIN descifrado = descifrado(descifrado(PIN cifrado, código-de-solicitud-de-PIN), clave_de_zona)

donde "descifrado(x,y)" es la función de descifrado recíproca de cifrado (x,y).

Como puede entenderse, tanto el dispositivo como el método según la presente invención añaden una dosis extra de seguridad en comparación con el cifrado simple. A fin de descifrar el PIN, un estafador necesita dos elementos, el código de solicitud de PIN y la clave de zona, en lugar de solamente la clave de zona.

El registro de entrega de PIN está adicionalmente protegido por el cifrado de al menos el campo de PIN y el cálculo de un Código de Autenticación de Mensaje ("MAC") 225 para todo el registro. El MAC 225 se mantiene en la tabla con el correspondiente registro 200 y es un medio bien conocido de asegurar la integridad de los datos en el registro referido.

Una tarjeta nueva, o de reemplazo, a enviar a un cliente se adosa a lo que se conoce como un "portador", es decir, un trozo de cartón o papel diseñado para ser manipulado automáticamente y sobre el cual se imprime la dirección de destino de la tarjeta, más cualquier otra información que el emisor de la tarjeta pueda desear comunicar al cliente. En particular, según realizaciones específicas de la presente invención, el código de solicitud de PIN se imprime sobre este portador. El portador, con la tarjeta adosada, se coloca en un sobre y se envía por el correo al cliente.

A fin de obtener el PIN que es necesario para usar el instrumento financiero, es decir, la tarjeta, el cliente compone un mensaje 250 de SMS (véase la línea superior de la figura 2) que contiene una cabecera 255 y, en el cuerpo del SMS, el código 260 de solicitud de PIN que el cliente recibió con la tarjeta.

El cliente envía este mensaje 250 de SMS a un número de teléfono que bien está indicado en el portador o bien se proporciona de alguna otra manera, por ejemplo, mediante Internet. El mensaje 250 de SMS es encaminado desde su teléfono móvil, también llamado "Estación Móvil" ("MS") 110, a un centro de servicios de SMS ("SMSC") 140, mediante una estación base 120 y un centro 130 de conmutación de una red 170 de telefonía móvil. La integridad y seguridad del mensaje a través de la red 170 de telefonía móvil están proporcionadas por el sistema 111 de seguridad del operador móvil. El SMSC 140 descifra el mensaje usando el sistema 111 de seguridad del operador móvil y lo vuelve a cifrar usando un medio 141 de seguridad acordado de antemano con el operador del servidor 150 de contenido de SMS. El SMSC 140 remite luego el código 215 de solicitud de PIN recientemente cifrado, junto con el número 205 de teléfono móvil desde el cual llegó el SMS, al servidor 150 de contenido de SMS.

El servidor 150 de contenido de SMS descifra el código 215 de solicitud de PIN usando el medio 151 de seguridad acordado. El servidor 150 de contenido de SMS mantiene una copia de la tabla 181. El servidor 150 de contenido de

SMS busca en la tabla 181 un registro que coincida con el código 215 de solicitud de PIN.

Cuando se halla un registro coincidente, el servidor 150 de contenido de SMS comprueba el número de teléfono del solicitante con respecto al número de teléfono en el registro coincidente. En el caso de no hallarse ninguna coincidencia para el código de solicitud de PIN, o en el caso de que el número del solicitante no corresponda al número de teléfono en el registro coincidente, en realizaciones específicas, se compone un mensaje de error y se devuelve al solicitante.

El servidor 150 de contenido de SMS usa un módulo 160 de seguridad de hardware para verificar el Código 225 de Autenticación de Mensaje. Si la verificación del Código de Autenticación de Mensaje tiene éxito, el servidor 150 de contenido de SMS usa sucesivamente el código de solicitud de PIN y el módulo 160 de seguridad de hardware para descifrar el PIN en el registro coincidente. El servidor 150 de contenido de SMS genera luego un mensaje de SMS cuyo contenido es el PIN, y cuya dirección de destino es el número 205 de móvil hallado en el registro. El servidor 150 de contenido de SMS cifra el mensaje de SMS usando el medio 151 de seguridad y lo envía de vuelta al SMSC 140. El SMSC 140 descifra el PIN usando el medio 141 de seguridad acordado y envía el mensaje de SMS con el PIN a la Estación Móvil 110 del cliente. La integridad y seguridad del mensaje están proporcionadas por el sistema 111 de seguridad del operador móvil.

El sistema de informes de entrega del SMS permite al SMSC 140 rastrear precisamente cuáles PIN han sido solicitados y cuáles han sido entregados.

Una vez que el cliente ha memorizado el PIN en su propia memoria, supuestamente borra el mensaje del PIN de la memoria de su teléfono móvil. De esta manera, la extensión del tiempo en que el PIN permanece accesible en la memoria del teléfono móvil se mantiene en mínimos.

Para el emisor de la tarjeta, la recepción del código de solicitud de PIN significa que el cliente acusa recibo de la tarjeta.

Un cliente que ha pedido más de una tarjeta puede estar esperando más de un PIN 210; el código 251 de solicitud de PIN identifica sin ambigüedad qué código corresponde a qué tarjeta.

Con un código 215 de solicitud de PIN impredecible, un tercero malintencionado necesita hallar el teléfono correcto y el código 215 de solicitud de PIN. Cuando un usuario consciente de la seguridad recibe la tarjeta y el código 215 de solicitud de PIN, memoriza el código 215 de solicitud de PIN y luego destruye su rastro impreso. Esto aumenta la seguridad al reducir la extensión del tiempo en que el rastro impreso del código 215 de solicitud de PIN permanece accesible a un tercero.

Como se ha manifestado anteriormente, el método de la presente invención permite a un emisor de instrumento financiero distribuir el PIN 210 asociado al teléfono móvil de los clientes mediante la red 170 telefónica móvil, usando el sistema de mensajes breves (“SMS”).

El envío de un PIN 210 a través del canal de SMS genera grandes ahorros para el emisor, dado que ya no existe un buen número de costes, tales como: la carta postal, la impresión, la administración de existencias, el trabajo, las impresoras, el mantenimiento y los sellos.

El uso de la presente invención también proporciona un mejor servicio y comodidad para el usuario. Debido a que todos tienen un teléfono móvil y lo usan profusamente como una nueva interfaz para charlar, hacer operaciones bancarias, adquirir servicios y contenidos, hacer que el PIN 210 sea enviado directamente al teléfono móvil que lleva siempre el titular de la tarjeta es una clara ventaja para el usuario. El titular de la tarjeta tiene la oportunidad de extraer su PIN en cualquier sitio, siempre que pueda accederse a la red telefónica. Además, el PIN 210 está disponible para el titular de la tarjeta en cuanto recibe la tarjeta. En realizaciones específicas, el PIN se mantiene en la tabla 181 y el usuario puede extraer el PIN muchas veces. En otras realizaciones, los datos del PIN se borran o bien se prohíbe el acceso al PIN una vez que el usuario lo ha recibido por primera vez.

En comparación con los sistemas de la técnica anterior, es un rasgo de seguridad añadido enviar el nuevo PIN 210 mediante un canal por separado. En efecto, es más difícil para un tercero malintencionado acceder tanto a la tarjeta como al PIN 210, ya que no siguen los mismos canales. Además, el destinatario del PIN 210 está identificado y / o autenticado por su número 250 de teléfono móvil.

Como puede verse en la figura 3, en una realización específica, el método de la presente invención comienza en una etapa 305 de registro del número de teléfono móvil del cliente cuando el cliente pide una nueva tarjeta.

Optativamente, el emisor de la tarjeta envía un mensaje breve que requiere una respuesta al número de teléfono móvil registrado, para comprobar que es correcto, durante la etapa 310.

Durante la etapa 315, la tarjeta y el PIN asociado se generan usando métodos convencionales.

Durante la etapa 320, una única palabra clave del SMS, llamada el “código de solicitud de PIN”, es generada por cada instancia de PIN / tarjeta. Esta es la palabra clave que será enviada por el titular de la tarjeta que desea recibir el PIN. La palabra clave es única porque un titular de tarjeta puede pedir varias tarjetas a la vez. La palabra clave también se envía con la tarjeta, impresa sobre el portador (carta de entrega que acompaña a la tarjeta).

Durante la etapa 325, los datos de PIN (Número de móvil, PIN cifrado, referencia de entrega, indicador de entrega) se almacenan en un servidor 180 de distribución de PIN que rastrea la entrega. Los datos se asocian a un MAC para garantizar la integridad.

Durante la etapa 330, los datos de PIN (Número móvil, PIN cifrado, código de solicitud de PIN) se distribuyen a un servidor de contenido de SMS. Los datos se asocian a un MAC para evitar cambios en los datos (principalmente, el número de móvil).

Durante la etapa 335, el titular de la tarjeta solicita el PIN enviando un SMS que incluye el código de solicitud de PIN a un número de teléfono especificado por el emisor.

Durante la etapa 340, el código de solicitud de PIN del SMS recibido y el número de teléfono asociado al SMS recibido se buscan en la tabla de registros, para determinar si hay un PIN asociado a ellos en un registro de la tabla almacenada en el servidor de contenido. Si no es así, durante la etapa 370, se envía un mensaje de error de vuelta al número de teléfono móvil y, optativamente, un informe que notifica el intento fallido se envía al emisor. Si hay un PIN asociado al código de solicitud de PIN y al número de teléfono, durante la etapa 345, se descifra el PIN y se envía al número de Móvil.

Durante la etapa 350, se determina si se ha recibido un informe de entrega desde el operador de la red de telefonía móvil. Si no es así, el proceso vuelve a la etapa 335.

Si se ha recibido un informe de entrega, durante la etapa 355, el PIN se marca como “entregado” en el registro almacenado en el servidor de contenido. Optativamente, durante la etapa 360, los datos de PIN se borran del servidor de contenido después de que se confirma la entrega. En otras palabras, optativamente, el PIN no puede ser entregado dos veces por el servidor de contenido.

Durante la etapa 365, el servidor de contenido proporciona un informe de entrega que incluye una referencia de entrega, la hora y la fecha de la entrega al servidor 180 de Distribución de PIN, el cual informa a su vez al emisor 195 de que el PIN ha sido entregado al cliente. Este informe de entrega es proporcionado por el operador de la red telefónica sin ninguna acción por parte del titular de la tarjeta.

Hay básicamente dos maneras de capturar el número de teléfono móvil desde el cual se envía el primer SMS:

- El método directo, usando un SMS de validación: el cliente da el número de teléfono móvil durante el proceso de registro o pedido, con presencia física o usando un sistema en línea. Cuando el número es proporcionado / ingresado por el cliente, se envía un mensaje de prueba al número de teléfono móvil. El cliente debe luego proporcionar el contenido de este mensaje de prueba (una palabra o un número) a fin de confirmar la validez del número. Este proceso es conocido por parte de los operadores de redes de telefonía móvil.

- El método de coincidencia por referencia: creando una referencia de coincidencia, habitualmente un número, que se da al cliente que supuestamente envía el número en un SMS a un número de teléfono especificado por el emisor. El mismo número debe ser incluido en el pedido de distribución de PIN proveniente del emisor. Cuando el SMS y el pedido son recibidos por el servidor de PIN, se compara el número de referencia y se registra el número de GSM del SMS recibido en el pedido de distribución.

Cualquier número de perfiles de distribución (conocidos como “portadores electrónicos”) puede definirse en el Servidor de Distribución de PIN. Cada portador puede contener distintas configuraciones y textos a enviar al receptor.

Al enviar un pedido de distribución (de un PIN), debe proporcionarse el número de portador.

En otras variantes, se introduce un retardo de la entrega para garantizar que la tarjeta esté entregada antes de que pueda entregarse un PIN.

El periodo en donde el PIN está disponible para la solicitud y la entrega también puede limitarse.

Para cada portador es posible definir un Texto de Notificación de Datos Listos. Este mensaje está concebido para informar al cliente de que el PIN puede ser extraído ahora del Servidor de PIN.

Usando una característica específica del SMS, es posible reescribir el SMS que contiene el PIN anteriormente

entregado al titular de la tarjeta. Obsérvese que la característica de reescritura del SMS está proporcionada por el estándar del SMS. Por ejemplo, esa característica se usa cuando un operador de red telefónica envía un SMS para notificar un mensaje de correo de voz en espera, a fin de evitar llenar la bandeja de entrada del SMS con notificaciones de correo de voz. Este mensaje de reescritura se envía después de un periodo especificado, con un texto reescrito especificado. Gracias a esta característica, incluso si el usuario ha mantenido su PIN en la memoria del teléfono, es posible borrarlo reescribiendo el texto. Se mejora de esta manera la seguridad del PIN.

Para evitar ataques por fuerza bruta o la adivinación de palabras clave, es posible incluir números de GSM en una lista negra durante un periodo, si se reciben demasiadas solicitudes erróneas. Puede enviarse un mensaje cuando el número es vedado.

Otra política de sistema es el periodo de tiempo durante el cual se almacena información de entrega en el sistema. Como se ha observado anteriormente, el PIN y la palabra clave también pueden borrarse cuando se entregan.

El sistema da soporte a un cierto número de configuraciones de PIN a fin de dar soporte a distintos métodos de cifrado y versiones de claves.

Muchos operadores de GSM-SMS (pasarela) ofrecen recoger los SMS mediante los denominados “números breves”. Un número breve tiene habitualmente entre tres y cinco dígitos. Es cómodo para el titular de la tarjeta solicitar el PIN mediante un número breve, porque es más fácil ingresar el número.

El servidor de PIN siempre envía mediante una conexión de SMSC, a fin de evitar todo husmeo antes de la transmisión.

Todos los mensajes tienen un registro de entrega, lo que significa que se registra si el mensaje es entregado. El mecanismo usado para esto son los informes de entrega del SMS, que es una característica de las redes de telefonía móvil. Si se solicita, el teléfono responde con un informe de entrega cuando se recibe un SMS.

Cuando el sistema ha generado el código de solicitud de PIN, sólo se almacena un troceo (por ejemplo, MD5 o SHA) en los sistemas.

Los datos de PIN están doblemente cifrados, usando una clave de cliente y la palabra clave. Esto garantiza que los datos solamente puedan ser descifrados y enviados cuando la palabra clave correcta es proporcionada por el titular de la tarjeta.

Todos los datos almacenados en el Servidor de PIN están asegurados con un MAC (“Código de Autenticación de Mensaje”). El MAC se comprueba antes de transmitir el PIN. Esto garantiza que nadie ha alterado los datos y, en particular, el número de teléfono móvil.

REIVINDICACIONES

1. Un método de distribución de un código personal a un usuario de un instrumento financiero asociado a dicho código personal, que comprende, después de una etapa de envío al usuario, mediante un primer canal, de un código de solicitud asociado a dicho código personal:

- una etapa (335) de recepción de dicho código (260) de solicitud mediante un segundo canal;

caracterizado por:

- una etapa de extracción del código personal (210) asociado a dicho código (260) de solicitud, y

- una etapa de envío al usuario del código (210) personal extraído mediante un tercer canal;

en el que el segundo canal y el tercer canal son una red (170) de telefonía móvil, en el que el segundo canal es una red para transmitir mensajes breves y en el que la etapa de extracción del código personal incluye una etapa de comprobación del número (205) de teléfono móvil del usuario en el segundo canal.

2. Un método según la reivindicación 1, en el que, durante la etapa del envío del código de solicitud, se envía un instrumento financiero a un usuario mediante el primer canal, junto con el código de solicitud asociado a dicho instrumento financiero.

3. Un método según cualquiera de las reivindicaciones 1 a 2, que incluye una etapa de descifrado del código personal (210) usando el código (260) de solicitud como una clave de descifrado.

4. Un método según cualquiera de las reivindicaciones 1 a 3, en el que ambos canales segundo y tercero son canales asegurados.

5. Un método según cualquiera de las reivindicaciones 1 a 4, en el que el primer canal es un canal de entrega por correo.

6. Un medio de almacenamiento de información que puede ser leído por un ordenador o un microprocesador que almacena instrucciones de un programa de ordenador, que permite la implementación de un método según una cualquiera de las reivindicaciones 1 a 5.

7. Un programa de ordenador cargable en un sistema de ordenador, conteniendo dicho programa instrucciones que permiten la implementación del método según una cualquiera de las reivindicaciones 1 a 5, cuando ese programa es cargado y ejecutado por un sistema de ordenador.

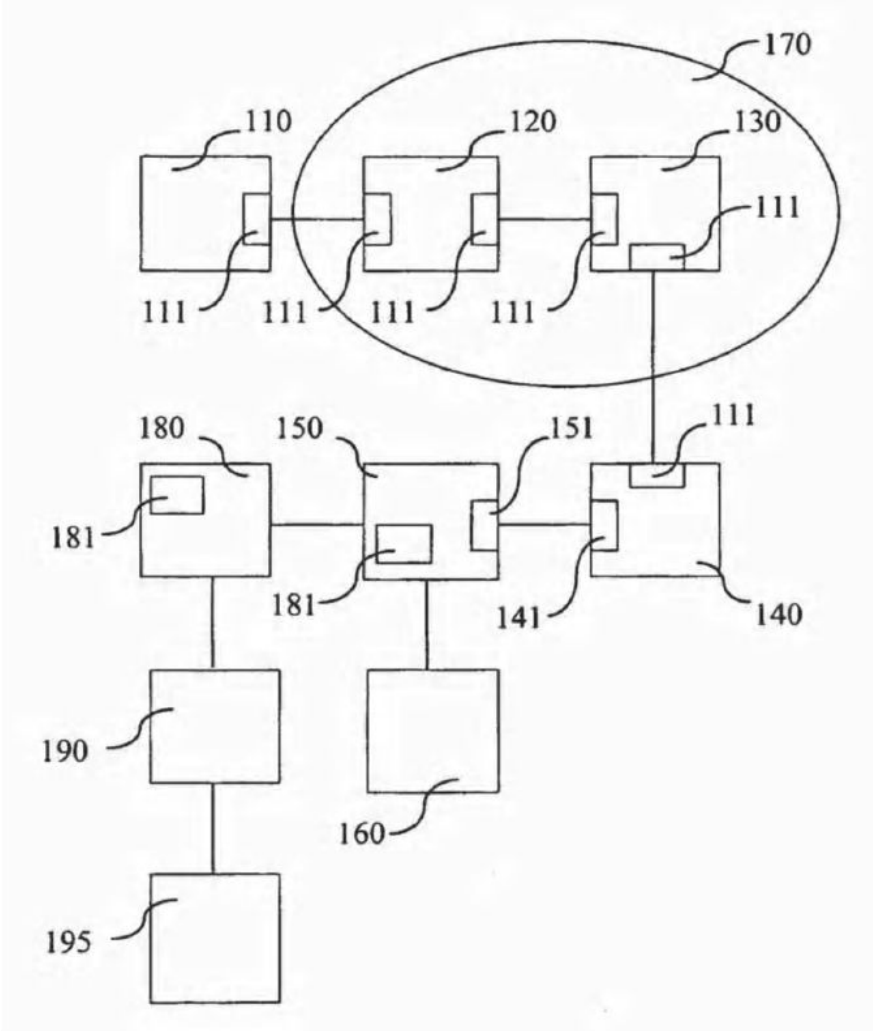
170
110
120
130
111
111
111
111
111
180
150
151
111
181
181
141
140
190
160
195

Figura 1

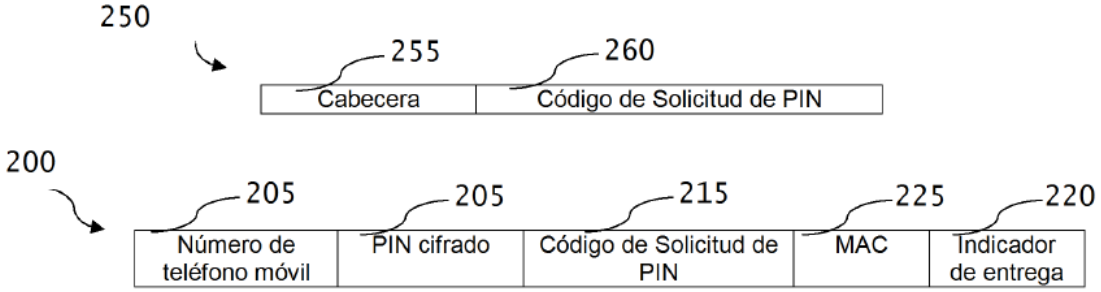
250
255
260
Cabecera
Código de Solicitud de PIN
200
205
205
215
225
220
Número de teléfono móvil
PIN cifrado
Código de Solicitud de PIN
MAC
Indicador de entrega

Figura 2

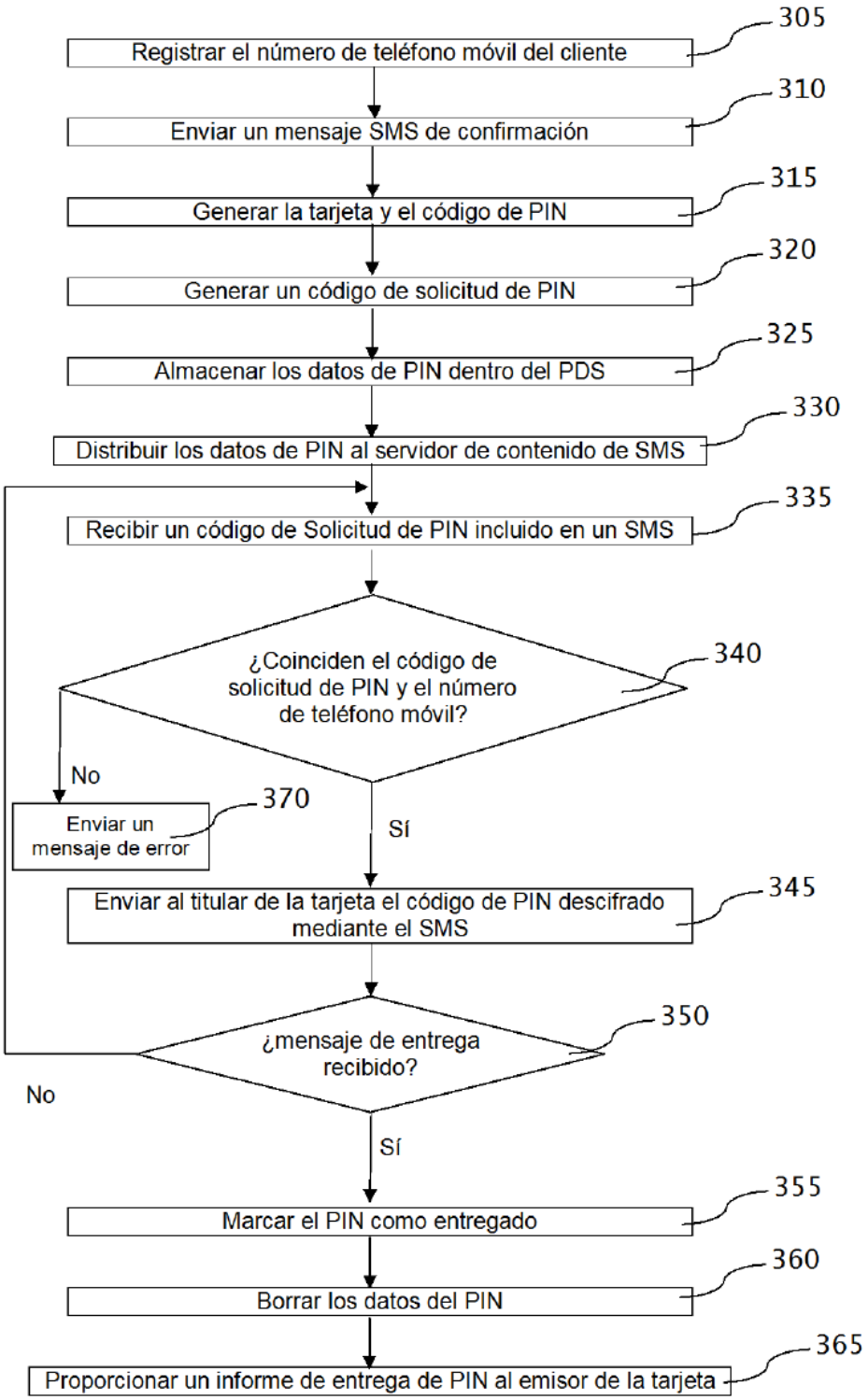
305
Registrar el número de teléfono móvil del cliente
310
Enviar un mensaje SMS de confirmación
315
Generar la tarjeta y el código de PIN
320
Generar un código de solicitud de PIN
325
Almacenar los datos de PIN dentro del PDS
330
Distribuir los datos de PIN al servidor de contenido de SMS
335
Recibir un código de Solicitud de PIN incluido en un SMS
340
¿Coinciden el código de solicitud de PIN y el número de teléfono móvil?
No
370
Enviar un mensaje de error
Sí
345
Enviar al titular de la tarjeta el código de PIN descifrado mediante el SMS
350
¿mensaje de entrega recibido?
No
Sí
355
Marcar el PIN como entregado
360
Borrar los datos del PIN
365
Proporcionar un informe de entrega de PIN al emisor de la tarjeta

Figura 3