(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 603 157**

(51) Int. CI.:

G07F 7/10 (2006.01)
G06F 21/36 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **26.09.2012 E 12186008 (4)**

(97) Fecha y número de publicación de la concesión europea: **24.08.2016 EP 2713345**

(54) Título: **Procedimiento y sistema para la introducción segura de datos de identificación para la autenticación de una transacción realizada mediante un terminal de autoservicio**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.02.2017

(73) Titular/es:

WINCOR NIXDORF INTERNATIONAL GMBH (100.0%)
Heinz-Nixdorf-Ring 1
33106 Paderborn, DE

(72) Inventor/es:

URBAN, PATRICK

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Procedimiento y sistema para la introducción segura de datos de identificación para la autenticación de una transacción realizada mediante un terminal de autoservicio

La invención se refiere a un procedimiento para la introducción segura de datos de identificación para la autenticación de una transacción según el preámbulo de la reivindicación 1 así como a un sistema apropiado para realizar el procedimiento según el preámbulo de la reivindicación de dispositivo principal asociada.

En el campo de las operaciones de pago asistidas automáticamente son ampliamente conocidos procedimientos y terminales de autoservicio (denominadas también abreviadamente terminales AS, de "AutoServicio") del tipo citado al principio. Como ejemplos típicos para tales terminales de autoservicio pueden citarse cajeros automáticos, que están instalados en bancos, centros comerciales, etc. y que permiten a un usuario, empleando su tarjeta bancaria, retirar en cualquier momento dinero de su cuenta y recibir el pago en efectivo. Son conocidos también terminales AS que permiten por ejemplo la transferencia de sumas de dinero y/o el ingreso de efectivo. Para asegurar una transacción frente a abusos, se realiza habitualmente una autenticación mediante datos de identificación, en particular mediante un denominado PIN (del inglés "Personal Identification Number", número de identificación personal), que está asociado a la tarjeta bancaria y que el usuario debe introducir correctamente en el cajero automático. Para ello, los cajeros automáticos habituales y otros terminales AS disponen de un campo de teclas, el denominado EPP (teclado encriptador de PIN, del inglés "Encrypting PIN Pad"), que transmite de forma encriptada el PIN introducido a la(s) unidad(es), en particular a un servidor central, que realiza la autenticación.

En el pasado, en el diseño de cajeros automáticos se ponía a menudo énfasis en componentes de alto valor y equipamiento abundante, lo que iba asociado sin embargo a costes de fabricación más altos. Hoy en día se perfila una tendencia a soluciones más económicas, en particular para el empleo en países emergentes y mercados en crecimiento, tales como los denominados estados "BRIC" (Brasil, Rusia, India, China). Ahí se demandan predominantemente sistemas de bajo coste, es decir terminales AS, que estén fabricadas de la forma más barata posible, pero que deben ofrecer los requisitos necesarios relativos a la seguridad y similares. Para el fabricante, la producción (empleo de componentes más económicos, adquisiciones a suministradores más baratos, optimización del proceso de fabricación, etc.) genera a menudo sólo un beneficio muy pequeño. Además, existe el riesgo de que se vean afectadas la calidad del producto, la facilidad de manejo y la seguridad. Por ello, son deseables soluciones alternativas, que hagan posibles ciertamente costes de producción bajos, pero sin tener que asumir pérdidas en calidad, facilidad de manejo y seguridad. Aquí forma parte de la seguridad el hecho de que pueda seguir realizándose también un procedimiento para la introducción segura de datos de identificación para la autenticación de una transacción.

En el documento US 2012/0047564 A1 se describe un sistema de seguridad y un procedimiento para la introducción segura de datos de identificación en forma de un PIN (número de identificación personal) asociado al usuario o respectivamente cliente, para realizar transacciones a través de Internet, que están relacionadas con el pago en línea de pedidos de mercancías y la utilización de servicios de pago (véase ahí [0002]). Para la introducción del PIN, en vez del teclado habitual con disposición de teclas normal, es generado un así denominado "teclado desordenado" (*"scrambled keypad"*) con una disposición de teclas desordenada o respectivamente entremezclada y es enviado a través de una comunicación de SMS (del inglés "Short Message Service", servicio de mensajes cortos) por móvil a un dispositivo terminal móvil de usuario (véanse ahí [0060], [0062-63] y [0065] así como la figura 5). Se solicita entonces al usuario, a través de la aplicación de pago por Internet, que introduzca en su PC (del inglés "Personal Computer", ordenador personal) o en su dispositivo terminal móvil su PIN correspondientemente a la disposición de teclas entremezclada, presentándose al usuario el teclado habitual (figura 6) o un teclado en blanco (figura 7) (véanse [0067-68]). A través de ello se evita que el verdadero PIN pueda ser espiado por extraños al accionar el teclado (figura 6 o figura 7). Debe asegurarse sin embargo que el entremezclado de las teclas afecte también en lo posible a todas aquellas teclas que deben ser utilizadas para el respectivo PIN, es decir las teclas relevantes para la introducción del PIN. En otro caso podría ocurrir que a pesar del entremezclado, las teclas relevantes se mantengan en su posición normal y un extraño pueda espiar el verdadero PIN.

El documento WO 2004/057516 A1 da a conocer un dispositivo y un procedimiento para la introducción de palabras clave en un cajero automático, una cerradura de puerta o similar, en que el dispositivo tiene una pantalla o respectivamente un visualizador con campo de teclas, donde los números o letras para palabras clave son dispuestos de forma aleatoria. El usuario puede introducir entonces, en vez de números de palabra clave, letras de palabra clave.

El documento DE 10 2007 043843 A1 da a conocer un procedimiento para la transmisión segura frente a escuchas de una serie de signos de un cliente a través de una red informática a un servidor de una cuenta en línea. Para una transmisión segura frente a escuchas de la serie de signos (palabra clave o respectivamente PIN) se realizan los siguientes pasos: a) generación de una imagen con áreas de accionamiento, que son etiquetadas con signos según el principio de aleatoriedad, por parte del servidor, b) comunicación de la imagen

generada en a) al cliente, c) generación de una imagen con áreas de accionamiento, que están dispuestas de forma similar a las áreas de accionamiento generadas en a), pero sin etiquetado, d) presentación de la imagen generada en c) en la pantalla del cliente, en que las áreas de accionamiento de la imagen son activables, e) introducción de una serie de n signos por el cliente mediante n activaciones de superficies de accionamiento no etiquetadas en la pantalla, mediante el recurso de que para cada signo del mensaje es activada el área de accionamiento no etiquetada que corresponde al área de accionamiento que está etiquetada con este signo en la imagen comunicada, f) transmisión al servidor de la información acerca de qué posiciones de imagen ha activado el cliente y en qué secuencia, y g) reconstrucción por parte del servidor de la serie de signos introducida por el cliente.

El documento GB 2 457 733 A da a conocer un procedimiento para asegurar la introducción de informaciones confidenciales por un usuario, en que el procedimiento comprende los siguientes pasos: generación de una asociación, que liga cada símbolo de una pluralidad de símbolos a un respectivo lugar o posición, en el que debe ser mostrado en una pantalla o respectivamente un visualizador, y presentación de la pluralidad de símbolos al usuario. Por parte del usuario se pone a disposición una secuencia de selecciones, en que cada selección representa una selección de un correspondiente lugar/posición. Entonces se produce una conversión de la secuencia de selecciones a una secuencia correspondiente de símbolos de entrada, que representan la introducción del usuario. La asociación de símbolos a lugares o posiciones sobre la pantalla puede producirse aleatoriamente.

El documento WO 2007/091869 A2 da a conocer un sistema de autenticación de usuario y un procedimiento, en el que encuentra aplicación un así denominado testigo OTP (del inglés “One-Time Password Token”, testigo de palabra clave de un sólo uso). El usuario configura una palabra clave de representación como clave fija; un dispositivo de consulta proporciona una pantalla de consulta, en la que un testigo OTP generado es descompuesto en partes, de forma ajustada a las representaciones de la clave fija. El usuario, que confirma la pantalla de consulta, introduce secuencialmente los números, que se ajustan a la palabra clave de representación, es decir la clave fija del usuario y el resultado de la autenticación del usuario son procesados dependiendo de si los números introducidos se ajustan a los valores de respuesta, que ha preparado el servidor.

El documento US 2008/0222048 A1 da a conocer un sistema de pago, en el que un dispositivo de comunicación móvil puede interactuar con una disposición de procesamiento de comercio y con una máquina de pago (“payment engine”, motor de pago). Un componente de comunicación, que está conectado a la máquina de pago, puede enviar códigos de barras demandados al dispositivo de comunicación móvil, puede recibir códigos de barras o códigos de producto universales alfanuméricos desde dispositivos de comunicación móvil de clientes, y puede procesar autorizaciones y transacciones de pago. Un componente de gestión de códigos de barras puede generar e interpretar códigos de barras sobre la base de ofertas de compra y demandas de clientes. Un componente de algoritmo de seguridad puede emplear un algoritmo de pares desplazados, para convertir cada cifra o cada dígito de una información de tarjeta bancaria en un par desplazado de cifras, para mejorar la seguridad en coincidencia con una forma de realización de la presente invención.

En el documento US 2012 / 0160912 A1 se describe un cajero automático, denominado abreviadamente ATM (del inglés “Automated Teller Machine”), que puede ser manejado también mediante un dispositivo terminal móvil de usuario. Aquí se trata del teléfono inteligente del usuario o respectivamente cliente de banco, que está equipado con una cámara, para escanear códigos gráficos de la pantalla del ATM. Además, en el teléfono inteligente está instalado un pequeño programa de aplicación (una así denominada app), el/la cual permite al usuario, a través de una conexión de comunicación móvil con el sistema de gestión de transacciones, realizar transacciones en el ATM sin tener que introducir la tarjeta bancaria en el lector de tarjetas del cajero automático. El usuario se autentica a través de su teléfono inteligente e induce por ejemplo una retirada de dinero, mediante el recurso de que con ayuda del teléfono móvil escanea un código de barras mostrado en la pantalla del ATM, cuyo código se refiere a la transacción, y el cual es enviado por el teléfono móvil al sistema de gestión de transacciones. A través de ello, el sistema de gestión de transacciones no sólo puede comprobar la autenticación del usuario, sino determinar también que el usuario se encuentra en el ATM que está asociado a la transacción (por ejemplo retirada de dinero). De acuerdo con ello, en el cajero automático ahí descrito podría prescindirse en principio del lector de tarjetas. Como se describe ahí en el párrafo de texto [0049], para dar vía libre a una transacción puede seguir siendo necesario que el usuario deba introducir en el teclado del ATM o en su teléfono inteligente datos de identificación en forma del así denominado PIN (número de identificación personal). El problema del espionaje de tales datos sensibles por parte de terceros no es tratado ahí.

El documento US 6.549.194 B1 describe un procedimiento para la introducción segura de datos de identificación en dispositivos terminales fijos o móviles. Ahí (véanse las figuras 2a-d y las figuras 3a-d) se describe una pantalla sensible al contacto, un denominado panel táctil (“touch-pad”), que tiene una configuración modificable dinámicamente, en la que puede modificarse la distribución espacial de las teclas blandas sobre el panel táctil. De acuerdo con ello se modifica la disposición de las teclas de cifras y con ello se dificulta el espionaje de introducciones de PIN.

El documento US 6.434.702 B1 (véanse las figuras 1 y 2) describe también una configuración variable de teclado para un teclado con bloque de cifras, en que sin embargo el marco de configuración se mantiene fijo y sólo varía la secuencia de las cifras mostradas. El campo de teclas (“pad”) ahí mostrado puede ser por ejemplo el panel táctil de un cajero automático (véase el texto, columna 1, líneas 29-31).

Constituye la tarea de la invención proponer un procedimiento y un sistema que opera según él, que sean apropiados para la introducción segura de datos de identificación para la autenticación de una transacción, que es realizada mediante un terminal de autoservicio, y que hagan imposible o al menos dificulten considerablemente el espionaje de los datos de identificación.

La tarea es resuelta mediante un procedimiento con las características de la reivindicación 1 y mediante un sistema que opera según el procedimiento con las características de la reivindicación principal asociada.

De acuerdo con ello se propone un procedimiento para la introducción segura de datos de identificación para la autenticación de una transacción, que es realizada mediante un terminal de autoservicio, con los siguientes pasos:

para un primer conjunto de datos con unos primeros elementos, en particular cifras, a partir de las cuales son formados los datos de identificación, en particular el PIN, es formado mediante una primera unidad asistida por ordenador un segundo conjunto de datos con unos segundos elementos, en particular letras y/o símbolos, los cuales están asociados biunívocamente a respectivamente uno de los primeros elementos, a través de lo cual son generables a partir de los segundos elementos datos de entrada, que constituyen una aplicación biyectiva de los datos de identificación, en que los segundos elementos son diferentes de los primeros elementos y en que la asociación del segundo conjunto de datos al primer conjunto de datos es formada nuevamente antes de cada realización de una nueva transacción mediante una asociación pseudo-aleatoria de los segundos elementos a los primeros elementos;

la asociación biunívoca de los segundos elementos a los primeros elementos es mostrada en una pantalla, que está unida constructivamente al terminal de autoservicio;

en un dispositivo terminal móvil de usuario, el cual está separado constructivamente del terminal de autoservicio, está conectado a través de canales seguros de una conexión de comunicación móvil a una segunda unidad asistida por ordenador y está asociado a un usuario del terminal de autoservicio, son mostrados los segundos elementos y no los primeros elementos;

en el dispositivo terminal móvil de usuario son introducidos los datos de entrada por el usuario; y

los datos de entrada son transmitidos a las unidades asistidas por ordenador conectadas al terminal de autoservicio, las cuales gestionan la asociación biunívoca de los segundos elementos a los primeros elementos y realizan la autenticación de la transacción.

El sistema propuesto está constituido para la autenticación y realización de una transacción así y comprende para ello varias unidades asistidas por ordenador, conectadas al terminal de autoservicio a través de canales de red seguros, y programas de aplicación, entre ellos los siguientes componentes de sistema:

una primera unidad asistida por ordenador, en particular un servidor, que para un primer conjunto de datos con unos primeros elementos, a partir de los que son formados los datos de identificación, forma un segundo conjunto de datos con unos segundos elementos, los cuales están asociados biunívocamente a respectivamente uno de los primeros elementos, a través de lo cual pueden ser generados a partir de los segundos elementos datos de entrada, que corresponden a una aplicación biyectiva de los datos de identificación, en que los segundos elementos son diferentes de los primeros elementos y en que la asociación del segundo conjunto de datos al primer conjunto de datos es formada nuevamente antes de cada realización de una nueva transacción mediante una asociación pseudo-aleatoria de los segundos elementos a los primeros elementos;

una pantalla, que está unida constructivamente al terminal de autoservicio y que muestra la asociación biunívoca de los segundos elementos a los primeros elementos;

un dispositivo terminal móvil de usuario, el cual está separado constructivamente del terminal de autoservicio, está conectado a través de canales seguros de una conexión de comunicación móvil a una segunda unidad asistida por ordenador y está asociado a un usuario del terminal de autoservicio, y que muestra los segundos elementos y no los primeros elementos, para permitir al usuario introducir los datos de entrada en el dispositivo terminal de usuario;

en que un programa de aplicación implementado en el dispositivo terminal móvil de usuario transmite los datos de entrada a una segunda unidad asistida por ordenador, que realiza la autenticación de la

transacción, y en que la primera unidad asistida por ordenador gestiona la asociación biunívoca de los segundos elementos a los primeros elementos.

La asociación del segundo conjunto de datos al primer conjunto de datos, que es formada nuevamente antes de cada realización de una nueva transacción mediante una asociación pseudo-aleatoria de los segundos elementos a los primeros elementos, es modificada más frecuentemente y a ser posible sin reglas fijas, en que la asociación dado el caso sólo es válida para una transacción.

De acuerdo con ello, por el lado del usuario, es decir en el dispositivo terminal de usuario, por ejemplo un teléfono inteligente, y/o en el terminal AS no se produce ninguna introducción de los datos de identificación sensibles, por ejemplo del PIN, sino solamente la introducción de datos de entrada, que corresponden a una aplicación biyectiva de los datos de identificación (PIN), en que la aplicación o asociación biunívoca sólo está almacenada de forma segura por el lado de red en la unidad asistida por ordenador. Ya que para el usuario es formado, para un primer conjunto de datos con unos primeros elementos, tales como por ejemplo las cifras de “0” a “9”, a partir de las que son formados los datos de identificación (PIN), un segundo conjunto de datos con unos segundos elementos, por ejemplo las primeras diez letras del alfabeto “A, B, C, ... hasta J”, existiendo una asociación biunívoca. Por ejemplo, la cifra “0” está asociada a la letra “I” y la cifra “1” está asociada a la letra “B”. Esta asociación biunívoca es mostrada en una pantalla del terminal AS. En el visualizador o panel táctil del dispositivo terminal de usuario (teléfono inteligente) no es mostrada sin embargo la asociación, ni tampoco son mostrados los primeros elementos (cifras “0” a “9”). Sólo son mostrados los segundos elementos, tales como por ejemplo las letras “A, B, C, ... J” en el teléfono inteligente, en que la disposición y secuencia pueden ser modificados arbitrariamente. Si el usuario debe introducir para la transacción los datos de identificación o respectivamente su PIN, introduce sólo los segundos elementos asociados, tales como por ejemplo letras, es decir casi un pseudo-PIN (#PIN), con el que un espía no puede hacer nada. Como la asociación está almacenada sólo por el lado de red en la unidad asistida por ordenador, en un servidor seguro, es prácticamente imposible deducir los datos de identificación, aquí por ejemplo el PIN verdadero. La invención puede funcionar sin un empleo adicional de hardware, ya que se emplean componentes habituales del sistema, tales como servidor y terminal AS, en que en el dispositivo terminal de usuario simplemente debe ejecutarse una pequeña aplicación de software (una así denominada app), que está en comunicación el servidor.

Estructuraciones ventajosas de la invención resultan de las reivindicaciones dependientes:

De acuerdo con ello es ventajoso que los primeros elementos comprendan los valores de tecla de un teclado numérico y que los segundos elementos comprendan componentes de un esquema prefijable, en particular símbolos y/o letras de un alfabeto, niveles de gris de una escala de niveles de gris, colores de una escala de colores y/o posiciones de un esquema de posiciones. Con ello, el pseudo-PIN (#PIN) no contiene ningún tipo de cifras o respectivamente elementos numéricos. Esto tiene la ventaja particular de que se dificulta adicionalmente a un espía la percepción de una introducción de datos, ya que éste espera la introducción de cifras y con ello dado el caso no percibe en absoluto que el usuario realiza en ese momento una introducción que podría referirse al PIN. Además, para un espía es más bien difícil detectar símbolos o incluso valores de gris. La asociación no la conoce de todos modos, por lo que incluso un espionaje exitoso del pseudo-PIN no puede llevarle a un éxito.

Preferentemente, el dispositivo terminal móvil de usuario es un teléfono inteligente, que tiene una pantalla táctil o “touchscreen” o panel táctil, en que los segundos elementos, en particular como símbolos del esquema prefijable, son mostrados en la pantalla táctil, y en que los datos de entrada son introducidos por el usuario en la pantalla táctil. El usuario puede realizar por lo tanto la introducción del pseudo-PIN directamente en el panel táctil de su teléfono inteligente dentro del esquema mostrado.

Es ventajoso también que el dispositivo terminal de usuario tenga una cámara, y que para la comprobación de si el dispositivo terminal de usuario se encuentra cerca del terminal AS sea mostrado en la pantalla un código gráfico, en particular un código de barras, en que el código gráfico es captado, en particular escaneado, por la cámara del dispositivo terminal de usuario; y en que por parte del dispositivo terminal de usuario sean transmitidos datos característicos del código gráfico captado a la o a las diversas unidades asistidas por ordenador, que gestionan los datos característicos del código gráfico y realizan la autenticación de la transacción. A través de ello puede comprobarse de forma segura que el usuario se encuentra junto al terminal AS, en el que debe producirse la transacción (por ejemplo, la retirada de efectivo).

Preferentemente, el terminal de autoservicio o terminal AS es un cajero automático, en particular un cajero automático que no tiene teclado para la introducción de los datos de identificación.

La invención y las ventajas que resultan de ella son descritas entonces a continuación en detalle y con ayuda de los dibujos adjuntos, que reproducen lo siguiente:

la figura 1 muestra en forma de un diagrama de bloques la estructura de principio de un sistema conforme a la invención;

la figura 2 muestra en forma de un diagrama de flujo los pasos de un procedimiento conforme a la invención;

la figura 3 muestra la presentación de una asociación en la pantalla de un terminal AS, que constituye un componente del sistema según la figura 1; y

las figuras 4a-c muestran en tres variantes la presentación de un esquema de introducción en el panel táctil de un dispositivo terminal móvil de usuario, que constituye un componente del sistema según la figura 1.

La figura 1 muestra la estructura de principio de un sistema conforme a la invención para la autenticación y realización de una transacción en un terminal de autoservicio, denominado también abreviadamente terminal AS, del sistema. Como terminal AS se muestra a modo de ejemplo un cajero automático ATM, que puede realizar transacciones para la retirada de efectivo. Además de ello están representados los siguiente componentes del cajero automático: una bandeja de salida de dinero DPNS, un dispositivo de identificación ID-DEV, aquí en forma de un lector de tarjetas para tarjetas de chip, y una pantalla DISP así como un ordenador o computadora PC, que controla los flujos en el cajero automático y está en conexión con las unidades del lado de red. El ordenador PC y la pantalla DISP forman la unidad central del cajero automático ATM. El dispositivo de identificación ID-DEV sirve aquí para la lectura de tarjetas de cliente y forma con ello parte de un canal de seguridad adicional (“security channel”), que está previsto junto a la entrada de PIN.

Entre las unidades del sistema situadas por el lado de red se cuentan: un servidor central SRV, que es responsable de un gran número de cajeros automáticos, un servidor de PIN PINSRV, que comprueba la introducción de datos de identificación. El servidor SRV está conectado a una red de servidores NET, que es responsable de cajeros automáticos adicionales y puede formar una así denominada nube.

El usuario CSM del cajero automático ATM tiene un dispositivo terminal móvil de usuario MD, por ejemplo un teléfono inteligente, en el que está instalada una aplicación MBA para poder realizar la transacción desde este teléfono inteligente, como se describe a continuación. Esta aplicación es denominada a continuación también aplicación de banca móvil MBA (del inglés “Mobile Banking Application”), y se ejecuta en el teléfono inteligente del cliente, para reproducir la interfaz de usuario (“user interface”) para la transacción. El cajero automático ATM puede estar muy alejado del servidor SRV. En conjunto, los servidores y los cajeros automáticos así como los dispositivos terminales móviles de usuario están conectados a través de canales (de red) seguros, tales como por ejemplo a través de conexiones 3G, 4G, WIFI y WAN (del inglés “Wide Area Network”, red de área extensa), que están protegidos respectivamente con el protocolo SSL (del inglés “Secure Sockets Layer”, capa de puertos seguros) o TLS (del inglés “Transport Layer Security”, seguridad de la capa de transporte). No existe sin embargo ninguna conexión de red directa entre el cajero automático ATM y el dispositivo terminal móvil MD.

El procedimiento 100 conforme a la invención es descrito con ayuda de la figura 2, haciéndose referencia también a la figura 1. Los pasos del procedimiento están dispuestos por columnas y asignados a los respectivos componentes de sistema MBA, ATM y SRV / NET o respectivamente al usuario CSM implicado.

En un primer paso 101, el usuario CSM induce el comienzo de una nueva transacción, aquí una retirada de efectivo. Para ello, el cliente da comienzo a la app MBA en su teléfono inteligente e inicia sesión en ella, por ejemplo a través de su palabra clave de MBA, mediante lo cual es establecida la conexión al servidor.

El cajero automático ATM solicita en el paso 102 datos de identificación, que pueden contener también el denominado PAN (del inglés “Primary Account Number”, número de cuenta principal) de la tarjeta bancaria del cliente. El usuario inserta su tarjeta bancaria en el lector de tarjetas ID-DEV. Alternativamente a ello, coloca su tarjeta NFC (del inglés “Near Field Communication”, comunicación de campo cercano) sobre el lector de tarjetas. Este paso de la comprobación de identidad a través de un segundo canal de seguridad es opcional y sirve para una seguridad adicional.

El ATM comprueba entonces en el paso 104 si el usuario se encuentra realmente delante del cajero automático. Para ello, desde el servidor es generado un código aleatorio de números de varias cifras y es transmitido al cajero automático ATM, que genera un código congruente y gráficamente representable (código de barras, código QR (del inglés “Quick Response”, de respuesta rápida)) y lo muestra en la pantalla DISP. El cliente coloca su teléfono inteligente MD o respectivamente su cámara de tal manera sobre la pantalla que la app MBA puede leer o respectivamente escanear mediante la cámara el código de barras y convertirlo al código numérico congruente. La app MBA instalada en el teléfono inteligente del usuario escanea en el paso 105 con ayuda de la cámara del teléfono inteligente el código de la pantalla y envía el resultado a través de una conexión de comunicación móvil al servidor o respectivamente a la red SRV / NET, donde se comprueba si los datos del resultado son congruentes con el código mostrado. Cuando es éste el caso, se determina que el usuario se encuentra realmente junto al cajero automático. La transacción es entonces continuada. También este paso es opcional y se orienta según las prescripciones de seguridad del banco o de instituciones internacionales o respectivamente propias del país. Posiblemente es suficiente también un chip para NFC (comunicación de

campo cercano) que dado el caso se halla en el teléfono inteligente. Además de ello, la generación y el escaneado de un código de barras es sólo una de muchas posibilidades. Podría emplearse también un gráfico generado aleatoriamente. O podría renunciarse a la presentación y escaneado de características gráficas. En vez de ello, los datos del cliente podrían ser enviados también a través del teléfono inteligente junto con una información de localización (por ejemplo GPS/GSMIWIFI) al servidor, para comprobar si el cliente se encuentra en el lugar del cajero automático ATM en cuestión.

En lo referente a la identidad del servidor, ésta es determinada por la app MBA por ejemplo mediante un certificado SSL. Alternativamente, podría emplearse un procedimiento de código de barras óptico, como se ha descrito anteriormente. Entonces, la app tendría que escanear dos códigos de barras. En este caso, los dos procesos de escaneado deberían ser realizados de forma inmediatamente consecutiva. Entonces, apenas deberían ser notados por el cliente, y menos como algo molesto. Un certificado tiene sin embargo la ventaja de que es seguro frente a un ataque mediante ATM falso junto a servidor falso.

En los siguientes pasos 107 – 111 se realiza la solicitud y la introducción segura de datos de identificación relativos al PIN. Para ello se hace referencia también a la figura 3 y a las figuras 4a-c:

En el paso 107, es mostrada en la pantalla del cajero automático ATM una asociación de unos primeros elementos, a saber cifras 0, 1, 2, ..., 9, a unos segundos elementos, a saber letras A, B, C, D, ..., J, y concretamente en una secuencia preferentemente pseudo-aleatoria. Para ello, el servidor genera una permutación de las cifras 0 a 9 y envía ésta al cajero automático ATM, que presenta entonces letras y números como se muestra en la figura 3. La asociación es conocida sólo para el servidor de PIN PINSRV y no es transmitida a través de la red de comunicación móvil u otra red insegura. Dentro de la asociación, cada letra representa entonces una indicación de posición (véase la figura 3). Con respecto a la disposición de cifras en un teclado EPP, esto significa que cada cifra está asociada biunívocamente a una posición o respectivamente a una letra, por ejemplo el 5 está asociado a la posición D y el 4 a la posición H. La asociación es mostrada solamente en la pantalla del cajero automático ATM durante un periodo de tiempo prefijable, de modo que el usuario puede memorizar la asociación o respectivamente puede cifrar su PIN en letras con ayuda de la asociación. Por ejemplo, el PIN de cuatro cifras es como sigue, “3456”. El usuario reconoce con ayuda de la asociación representada en la figura 3 que la secuencia de letras debe ser como sigue: A-H-D-J.

Ahora, en el paso 108 es mostrado por la app MBA un esquema de introducción en el panel táctil del teléfono inteligente, tal como está representado en tres ejemplos en las figuras 4a-c. De acuerdo con ello, no se muestra la asociación ni tampoco el teclado de PIN, sino una disposición de los segundos elementos (aquí de las letras), en que la disposición puede ser generada también pseudo-aleatoriamente. La figura 4a, para una mejor comprensión de la invención, no muestra ninguna disposición pseudo-aleatoria, sino la disposición de las letras correspondientemente a su orden alfabético, es decir: A-B-C-D-...-J.

Para la consulta del PIN, se solicita al usuario en el paso 109 que introduzca las letras correspondientes en el panel táctil de su teléfono inteligente. En el ejemplo actual, introduciría la secuencia de letras: A-H-D-J. La app MBA envía entonces en el paso 110 cada letra individualmente o toda la secuencia (todos los cuatro datos cifrados) al servidor SRV o respectivamente al servidor de PIN. Éste puede desencriptar entonces los datos cifrados y determinar cuál es el verdadero PIN (paso 111).

En el paso 112, es decir en la autenticación propiamente dicha, puede darse vía libre a la transacción. El cajero automático proporciona en el paso 113 el efectivo deseado, y el usuario lo retira en el paso 114 de la bandeja de salida de dinero.

En vez de un esquema de introducción estrictamente ordenado, como se representa en la figura 4a, pueden mostrarse también esquemas de introducción o respectivamente disposiciones de letras no ordenados, tal como muestran a modo de ejemplo las figuras 4b y 4c. La disposición es generada preferentemente a través de un proceso pseudo-aleatorio y es mostrada como teclado de pantalla en el panel táctil del teléfono inteligente. La generación del teclado de pantalla puede realizarse para cada nueva transacción, pudiendo aprovecharse totalmente las grandes posibilidades de combinación de las teclas dispuestas.

La invención puede aplicarse en particular en terminales AS, en las cuales se ha prescindido de un teclado de introducción de PIN propio y del sistema electrónico especial de teclado EPP necesario para ello. La invención hace posible que se pueda realizar una introducción de PIN segura con ayuda del teléfono inteligente del cliente. Aquí puede determinarse también de forma segura que el teléfono inteligente del cliente se encuentra realmente en las proximidades inmediatas del cajero automático ATM. El procedimiento descrito es claramente menos susceptible de manipulaciones y clonado que en el caso de la introducción clásica de un PIN a través de un teclado EPP.

Como resumen de la descripción anterior, para la introducción segura de un PIN o de otros datos de identificación se propone una asociación dinámicamente prefijable de posición de tecla y valor de tecla en forma de un esquema de introducción flexible. Para ello, en la pantalla del cajero automático es mostrada una

asociación prefijada, generada preferentemente de forma pseudo-aleatoria, de valores de tecla o respectivamente cifras del intervalo numérico 0-9 a posiciones de tecla en forma de símbolos, letras A, B, C ... o similares. No obstante, en el teléfono móvil de usuario sólo son mostradas las posiciones de tecla, es decir los símbolos, letras o similares en forma de un esquema de introducción. El usuario no introduce su PIN (por ejemplo “3456”), sino que introduce sólo las posiciones de tecla asociadas (“AHDJ”) correspondientemente al esquema de introducción. Esto tiene la ventaja de que por parte del usuario no se produce ya ninguna introducción de PIN que pudiera ser espiada. Sólo son introducidos los datos (letras) de las correspondientes posiciones de tecla (“AHDJ”). El teléfono móvil no conoce el PIN, tampoco el cajero automático ATM conoce el PIN, sino simplemente el esquema. Sólo el servidor conoce el esquema y el PIN y puede dar vía libre a la transacción. Este procedimiento es por ello muy seguro.

En otras palabras: cada letra representa biunívocamente una indicación de posición. En el teléfono inteligente sólo son mostradas indicaciones de posición (letras A-J), pero no las cifras asociadas. Cada indicación de posición tecleada por el usuario es transmitida por la app MBA al servidor. Como el servidor conoce tanto el PIN como la permutación de las cifras 0-9 transmitida al cajero automático ATM, puede comparar entonces si el cliente ha introducido el PIN correcto. El cajero automático ATM no tiene información de ningún tipo sobre el PIN del cliente, a él sólo se le envió una permutación aleatoria. La app MBA ha recibido simplemente indicaciones de posición del cliente, pero debido a la ausencia de conocimiento de la permutación no tiene ninguna posibilidad de deducir el correspondiente PIN. ¡El PIN es conocido exclusivamente por el cliente y el servidor! La indicación de posiciones mediante letras es sólo una vía posible. Igualmente podrían representarse las posiciones con diferentes gráficos, figuras geométricas o niveles de gris.

Como la invención emplea para una transacción el teléfono inteligente del respectivo usuario, puede prescindirse en el cajero automático ATM en particular del teclado de PIN / EPP.

La seguridad del procedimiento puede aumentarse en caso necesario adicionalmente mediante el recurso de que para cada cifra son generadas y mostradas nuevas permutaciones. También aquí son almacenadas las permutaciones nuevamente en el servidor, para poder realizar posteriormente la comparación del PIN introducido por el cliente con el PIN almacenado en el servidor. Como estas informaciones son introducidas a través del teléfono inteligente del cliente, el clonado es considerablemente más difícil de llevar a cabo, ya que debido a la ausencia de teclado EPP no existe ningún teclado instalado fijamente en el cajero automático ATM. También deberían ser “vigilados” tanto la pantalla del ATM como el teléfono inteligente incluyendo los dedos del cliente.

Opcionalmente, para la comprobación de si el teléfono inteligente se encuentra en la zona de servicio inmediata del cajero automático ATM, puede ser generado y mostrado en la pantalla del cajero automático un código ópticamente escaneable (código de barras / código QR o en general también un gráfico). Entonces se produce el escaneado del código con el teléfono inteligente y el envío de los datos a un servidor, que compara finalmente los datos con el código almacenado en el servidor. Con ello puede determinarse de forma sencilla que el teléfono inteligente se encuentra en la zona de servicio inmediata del cajero automático y con ello pertenece probablemente al usuario.

REIVINDICACIONES

1. Procedimiento (100) para la introducción segura de datos de identificación (PIN) de un usuario (CSM) de un terminal de autoservicio (ATM) para la autenticación de una transacción, que es realizada mediante el terminal de autoservicio (ATM), que está conectado a través de canales seguros a varias unidades asistidas por ordenador (PINSRV, SRV), en que las diversas unidades asistidas por ordenador (PINSRV, SRV) comprenden al menos una primera unidad asistida por ordenador (PINSRV) y una segunda unidad asistida por ordenador (SRV), **caracterizado por** los siguientes pasos:

para un primer conjunto de datos con unos primeros elementos, que comprenden valores de tecla (0, 1, 2, 3, ..., 9) de un teclado numérico, a partir de los cuales son formados los datos de identificación (PIN), es formado en la primera unidad asistida por ordenador (PINSRV) un segundo conjunto de datos con unos segundos elementos, que comprenden componentes (A, B, C, ..., J) de un esquema prefijable, los cuales están asociados biunívocamente a respectivamente uno de los primeros elementos (0, 1, 2, 3, ..., 9), a través de lo cual son generables a partir de los segundos elementos datos de entrada (#PIN), que corresponden a una aplicación biyectiva de los datos de identificación (PIN), en que los segundos elementos son diferentes de los primeros elementos y en que la asociación del segundo conjunto de datos al primer conjunto de datos es formada nuevamente antes de cada realización de una nueva transacción mediante una asociación pseudo-aleatoria de los segundos elementos (A, B, C, ..., J) a los primeros elementos (0, 1, 2, 3, ..., 9), en que por parte de la primera unidad asistida por ordenador (PINSRV) es generada una permutación de los primeros elementos (0, 1, 2, 3, ..., 9) y es enviada al terminal de autoservicio (ATM); la asociación biunívoca de los segundos elementos (A, B, C, ..., J) a los primeros elementos (0, 1, 2, 3, ..., 9) es mostrada en una pantalla (DISP), que está unida constructivamente al terminal de autoservicio (ATM) (paso 107);

en un dispositivo terminal móvil de usuario (MD), el cual está separado constructivamente del terminal de autoservicio (ATM), está conectado a través de canales seguros de una conexión de comunicación móvil a la segunda unidad asistida por ordenador (SRV) y está asociado al usuario (CSM) del terminal de autoservicio (ATM), son mostrados los segundos elementos (A, B, C, ..., J) y no los primeros elementos (0, 1, 2, 3, ..., 9) a través de un programa de aplicación implementado en el dispositivo terminal móvil de usuario (paso 108); en el dispositivo terminal móvil de usuario (MD) son introducidos los datos de entrada (#PIN) por el usuario (CSM) (paso 109); y

los datos de entrada (#PIN), que son generados a partir de los segundos elementos, son transmitidos mediante el programa de aplicación (MBA) a las unidades asistidas por ordenador (PINSRV; SRV), conectadas al terminal de autoservicio (ATM) a través de los canales de red seguros (paso 110), en que la segunda unidad asistida por ordenador (SRV) realiza la autenticación de la transacción y en que la primera unidad asistida por ordenador (PINSRV), que gestiona la asociación biunívoca de los segundos elementos (A, B, C, ..., J) a los primeros elementos (0, 1, 2, 3, ..., 9), comprueba los datos de entrada (#PIN) (paso 111).

2. Procedimiento (100) según la reivindicación 1, **caracterizado porque** los segundos elementos comprenden componentes de un esquema prefijable, que son símbolos, en particular letras (A, B, C, ..., J) de un alfabeto, niveles de gris de una escala de niveles de gris, colores de una escala de colores y/o posiciones de un esquema de posiciones.

3. Procedimiento (100) según una reivindicación precedente, **caracterizado porque** el dispositivo terminal móvil de usuario es un teléfono inteligente (MD) con una pantalla táctil o “touchscreen”, porque los segundos elementos, en particular como símbolos (A, B, C, ..., J) del esquema prefijable, son mostrados en la pantalla táctil (paso 107), y porque los datos de entrada (#PIN) son introducidos en la pantalla táctil por el usuario (CSM) (paso 108).

4. Procedimiento (100) según una de las reivindicaciones precedentes, **caracterizado porque** el dispositivo terminal móvil de usuario (MD) tiene una cámara, y porque antes de la realización de la transacción es realizada una comprobación de si el dispositivo terminal móvil de usuario (MD) se encuentra cerca del terminal de autoservicio (ATM), en que en la pantalla (DISP) es mostrado un código gráfico, en particular un código de barras (paso 104); en que el código gráfico es captado, en particular escaneado, por la cámara del dispositivo terminal de usuario (MD) (paso 105); y en que por parte del dispositivo terminal de usuario (MD) son transmitidos datos característicos del código gráfico captado a las diversas unidades asistidas por ordenador (PINSRV; SRV) conectadas al terminal de autoservicio (ATM), las cuales gestionan los datos característicos del código gráfico y realizan la comprobación.

5. Sistema para la autenticación y realización de una transacción en un terminal de autoservicio (ATM) del sistema, en que el sistema para la autenticación de la transacción mediante una introducción segura de datos de

identificación (PIN) de un usuario (CSM) del terminal de autoservicio (ATM) comprende varias unidades asistidas por ordenador (PINSRV; SRV) conectadas al terminal de autoservicio (ATM) a través de canales de red seguros, en que las diversas unidades asistidas por ordenador (PINSRV, SRV) comprenden al menos una primera unidad asistida por ordenador (PINSRV) y una segunda unidad asistida por ordenador (SRV), 10 **caracterizado por** los siguientes componentes de sistema:

la primera unidad asistida por ordenador (PINSRV), que para un primer conjunto de datos con unos primeros elementos, que comprenden valores de tecla (0, 1, 2, 3, ..., 9) de un teclado numérico, a partir de los que son formados los datos de identificación (PIN), forma un segundo conjunto de datos con unos segundos elementos, que comprenden componentes (A, B, C, ..., J) de un esquema prefijable, los cuales están asociados biunívocamente a respectivamente uno de los primeros elementos (0, 1, 2, 3, ..., 9), a través de lo cual pueden ser generados a partir de los segundos elementos datos de entrada (#PIN), que corresponden a una aplicación biyectiva de los datos de identificación (PIN), en que los segundos elementos son diferentes de los primeros elementos y en que la asociación del segundo conjunto de datos al primer conjunto de datos es formada nuevamente antes de cada realización de una nueva transacción mediante una asociación pseudo-aleatoria de los segundos elementos (A, B, C, ..., J) a los primeros elementos (0, 1, 2, 3, ..., 9), en que la primera unidad asistida por ordenador (PINSRV) genera una permutación de los primeros elementos (0, 1, 2, 3, ..., 9) y la envía al terminal de autoservicio (ATM); una pantalla (DISP), que está unida constructivamente al terminal de autoservicio (ATM) y muestra la asociación biunívoca de los segundos elementos (A, B, C, ..., J) a los primeros elementos (0, 1, 2, 3, ..., 9);

un dispositivo terminal móvil de usuario (MD), el cual está separado constructivamente del terminal de autoservicio (ATM), está conectado a través de canales seguros de una conexión de comunicación móvil a la segunda unidad asistida por ordenador (SRV) y está asociado al usuario (CSM) del terminal de autoservicio (ATM), y que muestra los segundos elementos (A, B, C, ..., J) y no los primeros elementos (0, 1, 2, 3, ..., 9) a través de un programa de aplicación (MBA), para permitir al usuario (CSM) introducir los datos de entrada (#PIN) en el dispositivo terminal de usuario (MD); en que el programa de aplicación (MBA) está implementado en el dispositivo terminal móvil de usuario (MD) y en que el programa de aplicación (MBA) transmite los datos de entrada (#PIN), que están generados a partir de los segundos elementos, a las unidades asistidas por ordenador (PINSRV; SRV), en que la segunda unidad asistida por ordenador (SRV) realiza la autenticación de la transacción, y en que la primera unidad asistida por ordenador (PINSRV), que gestiona la asociación biunívoca de los segundos elementos (A, B, C, ..., J) a los primeros elementos (0, 1, 2, 3, ..., 9), comprueba los datos de entrada (#PIN).

6. Sistema según la reivindicación 5, **caracterizado porque** el terminal de autoservicio es un cajero automático (ATM), en particular un cajero automático (ATM) que no tiene teclado para la introducción de los datos de identificación (PIN).

7. Sistema según la reivindicación 5 ó 6, **caracterizado porque** el dispositivo terminal móvil de usuario es un teléfono inteligente (MD) con una pantalla táctil o “touchscreen”, que muestra en la pantalla táctil los segundos elementos (A, B, C, ..., J) correspondientemente al esquema prefijable, para permitir al usuario (CSM) introducir los datos de entrada (#PIN) en la pantalla táctil en vez de los datos de identificación (PIN).

8. Sistema según una de las reivindicaciones 5 a 7, **caracterizado porque** el dispositivo terminal de usuario (MD) tiene una cámara, y porque para la comprobación de si el dispositivo terminal de usuario (MD) se encuentra cerca del terminal de autoservicio (ATM), la pantalla (DISP) del terminal de autoservicio (ATM) muestra un código gráfico, en particular un código de barras; porque la cámara del dispositivo terminal de usuario (MD) capta, en particular escanea, el código gráfico; y porque el dispositivo terminal de usuario (MD) transmite datos característicos del código gráfico captado a las diversas unidades asistidas por ordenador (PINSRV; SRV), conectadas al terminal de autoservicio (ATM), que realizan la comprobación y gestionan los datos característicos del código gráfico.

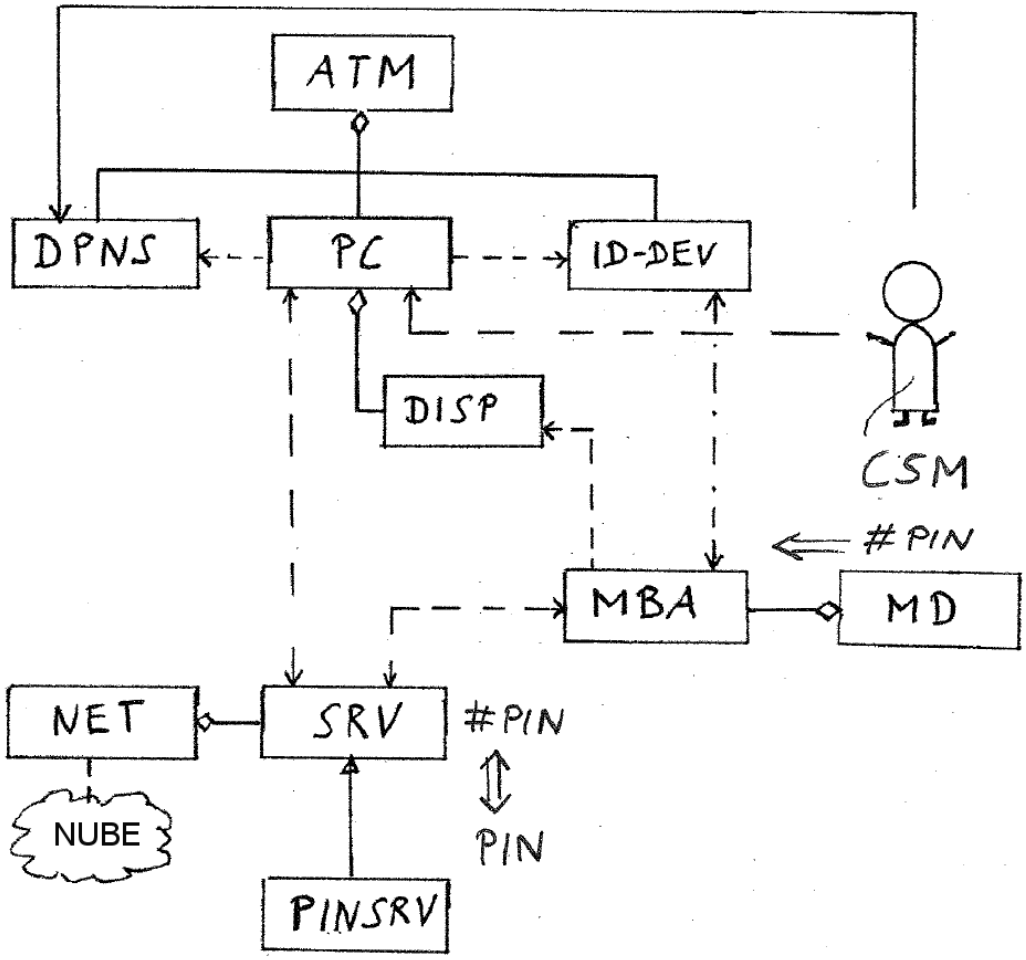
ATM
DPNS
PC
ID-DEV
DISP
CSM
#PIN
MBA
MD
NET
SRV
#PIN
PIN
NUBE
PINSRV

Fig. 1

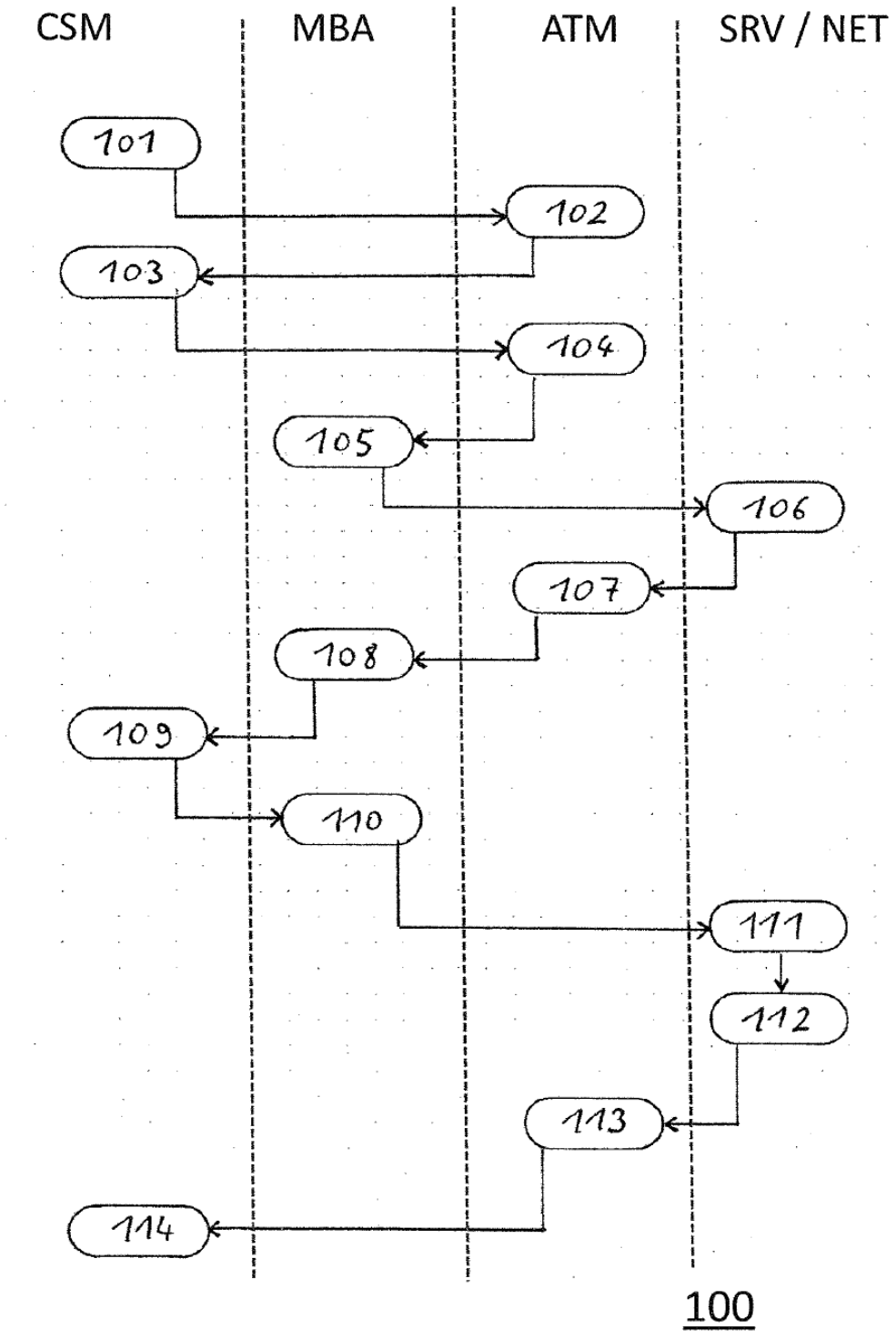
CSM
MBA
ATM
SRV / NET
101
102
103
104
105
106
107
108
109
110
111
112
113
114
100

Fig. 2

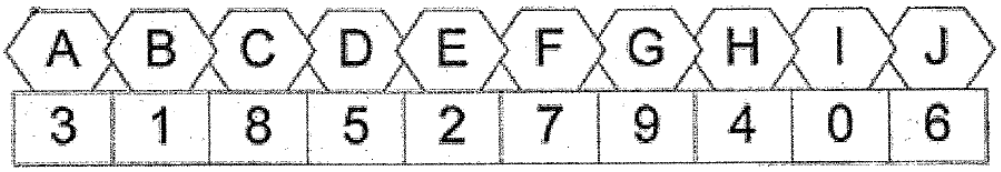

Fig. 3

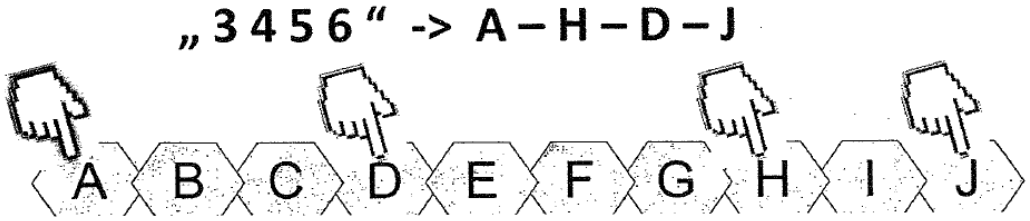

Fig. 4a

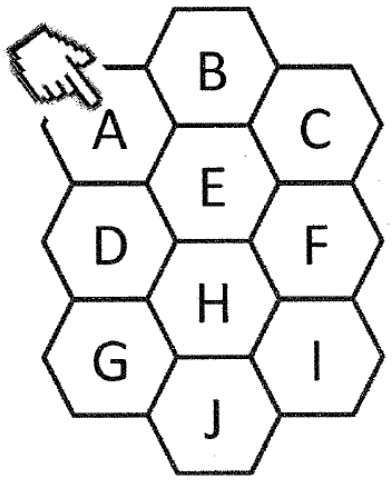

Fig. 4b

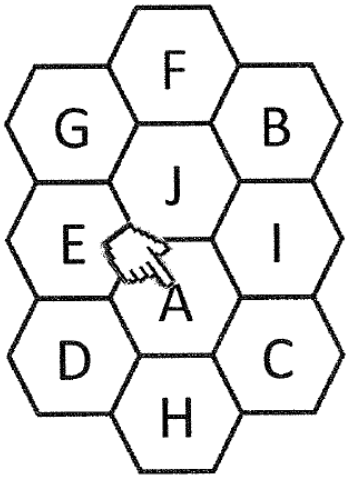

Fig. 4c