

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges
Eigentum

Internationales Büro

(43) Internationales
Veröffentlichungsdatum
3. April 2014 (03.04.2014)



(10) Internationale Veröffentlichungsnummer
WO 2014/048693 A1

(51) Internationale Patentklassifikation:

G07F 7/10 (2006.01) G06Q 20/32 (2012.01)
G06F 21/36 (2013.01) G06Q 20/40 (2012.01)
G07F 19/00 (2006.01)

(74) Anwalt: 2K PATENTANWÄLTE BLASBERG
KEWITZ & REICHEL PARTNERSCHAFT;
Schumannstraße 27, 60325 Frankfurt am Main (DE).

(21) Internationales Aktenzeichen: PCT/EP2013/068381

(22) Internationales Anmeldedatum:
5. September 2013 (05.09.2013)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
12186008.4 26. September 2012 (26.09.2012) EP

(71) Anmelder: WINCOR NIXDORF INTERNATIONAL
GMBH [DE/DE]; Heinz-Nixdorf-Ring 1, 33106
Paderborn (DE).

(72) Erfinder: URBAN, Patrick; Rolandsweg 33, 33102
Paderborn (DE).

(81) Bestimmungsstaaten (soweit nicht anders angegeben, für
jede verfügbare nationale Schutzrechtsart): AE, AG, AL,
AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW,
BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK,
DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM,
GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP,
KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD,
ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI,
NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU,
RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH,
TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA,
ZM, ZW.

(84) Bestimmungsstaaten (soweit nicht anders angegeben, für
jede verfügbare regionale Schutzrechtsart): ARIPO (BW,
GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ,
TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ,

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD AND SYSTEM FOR SECURELY ENTERING IDENTIFICATION DATA IN ORDER TO
AUTHENTICATE A TRANSACTION CARRIED OUT BY MEANS OF A SELF-SERVICE TERMINAL

(54) Bezeichnung : VERFAHREN UND SYSTEM ZUR GESICHERTEN EINGABE VON IDENTIFIZIERUNGSDATEN FÜR
DIE AUTHENTIFIZIERUNG EINER MITTELS EINES SELBSTBEDIENUNGSTERMINALS DURCHFÜHRTEN
TRANSAKTION

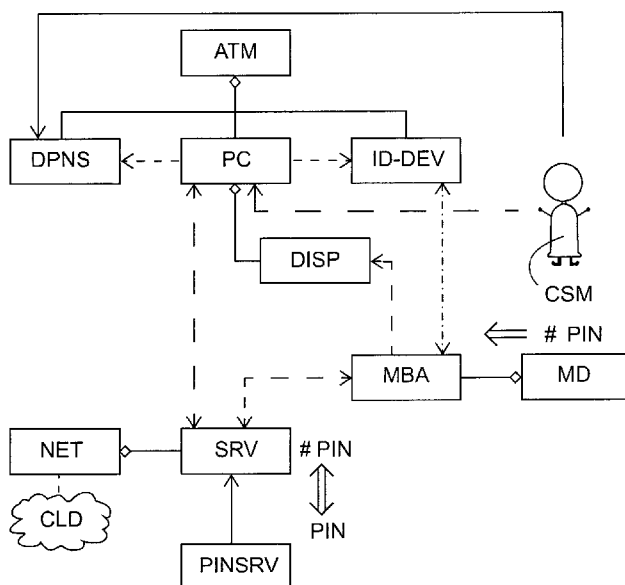


Fig.1

(57) Abstract: For self-service terminals, such as e.g. cash machines, identification data in the form of a PIN are usually entered on the keyboard of the cash machine. Said keyboards have encryption mechanisms, are produced as EPPs (Encrypting PIN Pads) and are very expensive. When a PIN is entered, being watched cannot be ruled out. In order to solve these problems, a method and a system for authenticating and carrying out a transaction at a self-service terminal, particularly a cash machine (ATM), is specified, wherein the system comprises the following system components: a first computer-supported unit (PINSRV), which forms a second data set containing second elements (A, B, C,... J) for a first data set containing first elements (0, 1, 2, 3,... 9) from which identification data (PIN) are formed, each of which second elements is allocated, on a one-to-one basis, to one of the first elements; a screen (DISP) which is structurally connected to the self-service terminal (ATM) and displays the one-to-one allocation of the second elements to the first elements; a user terminal (MD) which is structurally separate from the self-service terminal (ATM), is allocated to a user (CSM) and displays the second elements (A, B, C,... J) and not the first elements (0, 1, 2, 3,... 9), in order to enable the user to enter the input data (#PIN) on the user terminal (MD); wherein an application program (MBA) implemented on the user terminal transmits the input data (#PIN) to a second computer-supported unit (SRV) which carries out the authentication of the transaction, and wherein the first computer-supported unit (PINSRV) manages the one-to-one allocation of the second elements (A, B, C,... J) to the first elements (0, 1, 2, 3,... 9).

(57) Zusammenfassung:

[Fortsetzung auf der nächsten Seite]



RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— mit internationalem Recherchenbericht (Artikel 21 Absatz 3)

Bei Selbstbedienungsterminals, wie z.B. Geldautomaten, werden üblicherweise die Identifizierungsdaten in Form einer PIN an der Tastatur des Geldautomaten eingegeben. Diese Tastaturen haben Verschlüsselungsmechanismen, werden als EPP (Encrypting PIN Pad) hergestellt und sind recht teuer. Die PIN-Eingabe selbst wird durch Ausspähen bedroht. Um diese Probleme zu lösen, werden ein Verfahren und ein System zur Authentifizierung und Durchführung einer Transaktion an einem Selbstbedienungsterminal, insbesondere an einem Geldautomaten (ATM), vorgeschlagen, wobei das System folgende Systemkomponenten umfasst: eine erste rechnergestützte Einheit (PINSRV), die zu einer ersten Datenmenge mit ersten Elementen (0, 1, 2, 3,... 9), aus denen Identifizierungsdaten (PIN) gebildet werden, eine zweite Datenmenge mit zweiten Elementen (A, B, C,... J) bildet, welche jeweils einem der ersten Elemente eineindeutig zugeordnet sind; einen Bildschirm (DISP), der baulich mit dem Selbstbedienungsterminal (ATM) verbunden ist und die eineindeutige Zuordnung der zweiten Elemente zu den ersten Elementen anzeigt; ein Benutzer-Endgerät (MD), das baulich getrennt von dem Selbstbedienungsterminals (ATM) ist, einem Benutzer (CSM) zugeordnet ist und die zweiten Elemente (A, B, C,... J) und nicht die ersten Elemente (0, 1, 2, 3,... 9) anzeigt, um dem Benutzer zu ermöglichen, die Eingabedaten (#PIN) an dem Benutzer-Endgerät (MD) einzugeben; wobei ein auf dem Benutzer-Endgerät implementiertes Anwendungs-Programm (MBA) die Eingabedaten (#PIN) an eine zweite rechnergestützte Einheit (SRV) überträgt, die die Authentifizierung der Transaktion durchführt, und wobei die erste rechnergestützte Einheit (PINSRV) die eineindeutige Zuordnung der zweiten Elemente (A, B, C,... J) zu den ersten Elementen (0, 1, 2, 3,... 9) verwaltet.

5

**Verfahren und System zur gesicherten Eingabe von Identifizierungsdaten für die
Authentifizierung einer mittels eines Selbstbedienungsterminals durchgeführten
Transaktion**

10

Die Erfindung betrifft ein Verfahren zur gesicherten Eingabe von Identifizierungsdaten für die Authentifizierung einer Transaktion nach dem Oberbegriff des Verfahrensanspruchs 1 sowie ein zur Durchführung des Verfahrens geeignetes System nach dem Oberbegriff des
nebengeordneten Vorrichtungsanspruchs.

15

Im Bereich des Automaten-gestützten Zahlungsverkehrs sind Verfahren und Selbstbedienungsterminals (auch kurz SB-Terminals genannt) der eingangs genannten Art hinlänglich bekannt. Als typische Beispiele für solche Selbstbedienungsterminals sind Geldautomaten zu nennen, die in Banken, Einkaufszentren usw. aufgestellt sind und es einem Benutzer ermöglichen durch Verwenden seiner Bankkarte, jederzeit Geld von seinem Konto abzuheben und sich bar auszahlen zu lassen. Auch sind SB-Terminals bekannt, die andere Transaktionen, wie z.B. die Überweisung von Geldbeträgen und/oder die Einzahlung von Bargeld ermöglichen. Um eine Transaktion gegen Missbrauch abzusichern, wird üblicherweise eine Authentifizierung mittels Identifizierungsdaten, insbesondere mittels einer sog. PIN (Personal Identification Number), durchgeführt, welcher der Bankkarte zugeordnet sind bzw. ist und welche der Benutzer am Geldautomaten korrekt eingeben muss. Hierzu verfügen die üblichen Geldautomaten und sonstigen SB-Terminals über ein Tastenfeld, das sog. EPP (Encrypting PIN Pad), welches die eingegebene PIN verschlüsselt an die Einheit(en), insbesondere an einen zentrale Server, überträgt, der die Authentifizierung durchführt.

20

25

30

In der Vergangenheit wurde bei der Konzeption von Geldautomaten häufig Wert auf hochwertige Komponenten und reichhaltige Ausstattung gelegt, was jedoch mit höheren Herstellungskosten einherging. Heutzutage zeichnet sich ein Trend hin zu kostengünstigeren Lösungen ab, insbesondere für den Einsatz in Schwellenländern und Wachstumsmärkten, wie den sog. "BRIC"-Staaten. Hier werden überwiegend Low-Cost-Systeme nachgefragt, d.h. SB-Terminals, welche möglichst preiswert gefertigt sind, aber die erforderlichen Anforderungen bezüglich der Sicherheit u.ä. bieten sollen. Für den Hersteller wirkt die Produktion (Verwendung kostengünstigerer Komponenten, Bezug von billigeren Lieferanten, Optimierung des Fertigungsprozesses, etc.) oftmals nur sehr geringen Profit ab. Zudem besteht die Gefahr, dass die Produkt-Qualität, Benutzerfreundlichkeit und Sicherheit in Mitleidenschaft gezogen wird. Daher sind alternative Lösungen erwünscht, die zwar niedrige Produktionskosten ermöglichen, ohne jedoch Einbußen bei der Qualität, Benutzerfreundlichkeit und Sicherheit hinnehmen zu müssen. Dabei gehört zur Sicherheit dazu, dass auch weiterhin ein Verfahren zur gesicherten Eingabe von Identifizierungsdaten für die Authentifizierung einer Transaktion durchgeführt werden kann.

In der US 2012 / 0160912 A1 wird ein Geldautomat, kurz ATM genannt, beschrieben, der auch mittels eines mobilen Benutzer-Endgeräts bedient werden kann. Dabei handelt es sich um das Smartphone des Benutzers bzw. Bankkunden, das mit einer Kamera ausgestattet ist, um grafische Codes vom Bildschirm des ATM zu scannen. Ferner ist auf dem Smartphone ein kleines Anwendungsprogramm (sog. App) installiert, das/die über eine mobile Kommunikationsverbindung mit dem Transaktions-Management-System es dem Benutzer ermöglicht, Transaktionen am ATM auszuführen, ohne die Bankkarte in den Kartenleser des Geldautomaten einführen zu müssen. Der Benutzer authentifiziert sich über sein Smartphone und veranlasst z.B. eine Geldauszahlung, indem er mit Hilfe des Smartphone einen auf dem ATM-Bildschirm angezeigten Barcode abscannt, der sich auf die Transaktion bezieht, und den das Smartphone an das Transaktions-Management-System sendet. Hierdurch kann das Transaktions-Management-System nicht nur die Authentifizierung des Benutzers prüfen, sondern auch feststellen, dass der Benutzer sich an dem ATM befindet, der in die Transaktion (z.B. Geldausgabe) eingebunden ist. Demnach könnte bei dem dort beschriebenen Geldautomat der Kartenleser prinzipiell eingespart werden. Wie dort im Textabschnitt [0049] beschrieben wird, kann zur Freigabe einer

Transaktion es weiterhin erforderlich sein, dass der Benutzer an der Tastatur des ATM oder an seinem Smartphone Identifizierungsdaten in Form der sog. PIN (Personal Identification Number) eingeben muss. Das Problem des Ausspähens von solchen sensitiven Daten durch Dritte wird dort nicht behandelt.

5

Die US 6,549,194 B1 beschreibt ein Verfahren zur sicheren Eingabe von Identifizierungsdaten an festen oder mobilen Endgeräten. Dort (s. Fig. 2a-d und Fig. 3a-d) wird ein berührungsempfindlicher Bildschirm, ein sog. Touch-PAD, beschrieben, welches ein dynamisch veränderbares Layout aufweist, bei dem sich die räumliche Verteilung der Soft-Tasten auf dem Touch-PAD ändern kann. Demnach ändert sich die Anordnung der Zifferntasten und somit wird das Ausspähen von PIN-Eingaben erschwert.

10

Die US 6,434,702 B1 (s. Fig. 1 und 2) beschreibt auch ein sich änderndes Tastatur-Layout für ein Tastenfeld mit Ziffernblock, wobei jedoch der Layout-Rahmen fest bestehen bleibt und sich nur die Reihenfolge der angezeigten Ziffern ändert. Das dort gezeigte Tastenfeld (Pad) kann z.B. das Touch Pad eines Geldautomaten sein (s. Text, Spalte 1, Zeilen 29-31).

15

Als weiteren Stand der Technik sind zu nennen:

US 2012/047564 A1, WO 2004/057516 A1; DE 10 2007 043843 A1; GB 2 457 733 A; WO 2007/091869 A2; US 2008/222048 A1.

20

Aufgabe der Erfindung ist es ein Verfahren und ein danach arbeitendes System vorzuschlagen, die zur gesicherten Eingabe von Identifizierungsdaten für die Authentifizierung einer Transaktion, die mittels eines Selbstbedienungsterminals durchgeführt wird, geeignet sind, und die das Ausspähen der Identifizierungsdaten unmöglich machen oder zumindest deutlich erschweren.

25

Gelöst wird die Aufgabe durch ein Verfahren mit den Merkmalen des Anspruchs 1 und durch ein nach dem Verfahren arbeitendes System mit den Merkmalen des nebengeordneten Anspruchs.

30

Demnach wird ein Verfahren zur gesicherten Eingabe von Identifizierungsdaten für die Authentifizierung einer Transaktion, die mittels eines Selbstbedienungsterminals durchgeführt wird, mit den folgenden Schritten vorgeschlagen:

zu einer ersten Datenmenge mit ersten Elementen, insbesondere Ziffern, aus denen die Identifizierungsdaten, insbesondere die PIN, gebildet werden, wird eine zweite Datenmenge mit zweiten Elementen, insbesondere Buchstaben und/oder Symbolen, gebildet, welche jeweils einem der ersten Elemente eineindeutig zugeordnet sind, wodurch aus den zweiten Elementen Eingabedaten erzeugbar sind, die einer bijektiven Abbildung der Identifizierungsdaten entsprechen;

die eineindeutige Zuordnung der zweiten Elemente zu den ersten Elementen wird auf einem Bildschirm angezeigt, der baulich mit dem Selbstbedienungsterminal verbunden ist; an einem Benutzer-Endgerät, das baulich getrennt von dem Selbstbedienungsterminal ist und einem Benutzer des Selbstbedienungsterminals zugeordnet ist, werden die zweiten Elemente und nicht die ersten Elemente angezeigt;

an dem Benutzer-Endgerät werden durch den Benutzer die Eingabedaten eingegeben; und die Eingabedaten werden an eine oder mehrere mit dem Selbstbedienungsterminal verbundene rechnergestützte Einheiten übertragen, die die eineindeutige Zuordnung der zweiten Elemente zu den ersten Elementen verwalten und die Authentifizierung der Transaktion durchführen.

Das vorgeschlagene System ist zur Authentifizierung und Durchführung einer solchen Transaktion beschaffen und umfasst dazu eine oder mehrere mit dem Selbstbedienungsterminal verbundene rechnergestützte Einheiten und Anwendungs-Programme, darunter folgende Systemkomponenten:

eine erste rechnergestützte Einheit, insbesondere einen Server, die zu einer ersten Datenmenge mit ersten Elementen, aus denen die Identifizierungsdaten gebildet werden, eine zweite Datenmenge mit zweiten Elementen bildet, welche jeweils einem der ersten Elemente eineindeutig zugeordnet sind, wodurch aus den zweiten Elementen Eingabedaten erzeugbar sind, die einer bijektiven Abbildung der Identifizierungsdaten entsprechen;

einen Bildschirm, der baulich mit dem Selbstbedienungsterminal verbunden ist und die eineindeutige Zuordnung der zweiten Elemente zu den ersten Elementen anzeigt;

ein Benutzer-Endgerät, das baulich getrennt von dem Selbstbedienungsterminal ist, einem Benutzer des Selbstbedienungsterminals zugeordnet ist und die zweiten Elemente

und nicht die ersten Elemente anzeigt, um dem Benutzer zu ermöglichen, die Eingabedaten an dem Benutzer-Endgerät einzugeben;

wobei ein auf dem Benutzer-Endgerät implementiertes Anwendungs-Programm die Eingabedaten an eine zweite rechnergestützte Einheiten überträgt, die die

Authentifizierung der Transaktion durchführt, und wobei die erste rechnergestützte Einheit die eindeutige Zuordnung der zweiten Elemente zu den ersten Elementen verwaltet.

Demnach erfolgt auf der Benutzerseite, d.h. an dem Benutzer-Endgerät, z.B. Smartphone, und/oder an dem SB-Terminal keine Eingabe der sensitiven der Identifizierungsdaten, z.B. der PIN, sondern lediglich die Eingabe von Eingabedaten, die einer bijektiven Abbildung der Identifizierungsdaten (PIN) entsprechen, wobei die Abbildung bzw. eindeutige Zuordnung nur netzwerkseitig in der rechnergestützten Einheit gesichert hinterlegt ist. Denn für den Benutzer wird zu einer ersten Datenmenge mit ersten Elementen, wie z.B. den Ziffern von „0“ bis „9“, aus denen die Identifizierungsdaten (PIN) gebildet werden, eine zweite Datenmenge mit zweiten Elementen, z.B. den ersten zehn Buchstaben des Alphabets „A, B, C, ... bis J“ gebildet, wobei eine eindeutige Zugeordnung besteht. Beispielsweise ist die Ziffer „0“ dem Buchstaben „I“ zugeordnet und ist die Ziffer „1“ dem Buchstaben „B“ zugeordnet. Diese eindeutige Zuordnung wird auf einem Bildschirm des SB-Terminals angezeigt. Auf dem Display oder Touchpad des Benutzer-Endgerätes (Smartphone) wird die Zuordnung jedoch nicht angezeigt, auch werden nicht die ersten Elemente (Ziffern „0“ bis „9“) angezeigt. Es werden nur die zweiten Elemente, wie z.B. die Buchstaben „A, B, C, ... J“ auf dem Smartphone angezeigt, wobei die Anordnung und Reihenfolge beliebig verändert sein kann. Soll der Benutzer für die Transaktion die Identifizierungsdaten bzw. seine PIN eingeben, so gibt er nur die zugeordneten zweiten Elemente, wie z.B. Buchstaben ein, also quasi eine Pseudo-PIN (#PIN), mit der ein Ausspäher nichts anfangen kann. Da die Zuordnung nur netzwerkseitig in der rechnergestützten Einheit, einem gesicherten Server hinterlegt sind, ist ein Rückschluss auf die Identifizierungsdaten, hier z.B. der echten PIN, praktisch unmöglich. Die Erfindung kann ohne zusätzlichen Hardware-Einsatz auskommen, da übliche Systemkomponenten, wie Server, SB-Terminal genutzt werden, wobei auf dem Benutzer-Endgerät lediglich eine kleine Software-Applikation (sog. App) laufen muss, die in Kommunikation mit dem Server steht.

Vorteilhafte Ausgestaltungen der Erfindung ergeben sich aus den Unteransprüchen:

Demnach ist es vorteilhaft, wenn die ersten Elemente die Tastenwerte einer numerischen Tastatur umfassen und wenn die zweiten Elemente Komponenten eines vorgebbaren Schemas umfassen, insbesondere Symbole und/oder Buchstaben eines Alphabets, Graustufen einer Graustufenskala, Farben einer Farbskala und/oder Positionen eines Positionsschemas umfassen. Damit enthält die Pseudo-PIN (#PIN) keinerlei Ziffern bzw. numerischen Elemente. Dies hat den besonderen Vorteil, dass einem Ausspäher die Wahrnehmung einer Dateneingabe noch weiter erschwert werden, weil dieser ja die Eingabe von Ziffern erwartet und somit ggf. gar nicht wahrnimmt, dass der Benutzer momentan eine Eingabe macht, die die PIN betreffen könnte. Außerdem ist es für einen Ausspäher eher schwierig, sich Symbole oder gar Grauwerte zu merken. Die Zuordnung kennt er ohnehin nicht, so dass selbst ein erfolgreiches Ausspähen der Pseudo-PIN nicht zum Erfolg führen kann.

Weiterhin ist es vorteilhaft, wenn die Zuordnung der zweiten Datenmenge zu der ersten Datenmenge mittels einer Pseudo-Zufalls-Zuordnung der zweiten Elemente zu den ersten Elementen gebildet wird, insbesondere vor jeder Durchführung einer neuen Transaktion erneut gebildet wird. Hierdurch wird die Zuordnung häufiger geändert und möglichst ohne feste Regel, wobei die Zuordnung ggf. nur für eine Transaktion Gültigkeit hat.

Vorzugsweise ist das Benutzer-Endgerät ein mobiles Benutzer-Endgerät, insbesondere ein Smartphone, welches einen Berührungsbildschirm bzw. Touchscreen oder Touchpad aufweist, wobei die zweiten Elemente, insbesondere als Symbole des vorgebbaren Schemas, an dem Berührungsbildschirm angezeigt werden, und wobei die Eingabedaten an dem Berührungsbildschirm von dem Benutzer eingegeben werden. Der Benutzer kann also direkt auf dem Touchpad seines Smartphones innerhalb des angezeigten Schemas die Eingabe der Pseudo-PIN machen.

Von Vorteil ist es auch, wenn das Benutzer-Endgerät eine Kamera aufweist und wenn zur Überprüfung, ob sich das Benutzer-Endgerät in der Nähe des SB-Terminals befindet, auf dem Bildschirm ein grafischer Code, insbesondere ein Barcode, angezeigt wird, wobei der grafische Code von der Kamera des Benutzer-Endgerätes erfasst, insbesondere abgetastet,

wird; und wobei von dem Benutzer-Endgerät Kenndaten des erfassten grafischen Codes an die eine oder mehreren rechnergestützten Einheiten übertragen werden, die die Kenndaten des grafischen Codes verwalten und die Authentifizierung der Transaktion durchführen. Hierdurch kann sicher geprüft werden, dass der Benutzer sich an dem SB-Terminal befindet, an dem die Transaktion (z.B. Auszahlung von Bargeld) erfolgen soll.

Vorzugsweise ist das Selbstbedienungsterminal bzw. SB-Terminal ein Geldautomat, insbesondere ein Geldautomat, der keine Tastatur zur Eingabe der Identifizierungsdaten aufweist.

Die Erfindung und die sich daraus ergebenden Vorteile werden nun nachfolgend im Detail und anhand der beiliegenden Zeichnungen beschrieben, welche folgendes wiedergeben:

Fig. 1 zeigt in Form eines Blockdiagramms den prinzipiellen Aufbau eines erfindungsgemäßen Systems;

Fig. 2 zeigt in Form eines Ablaufdiagramms die Schritte eines erfindungsgemäßen Verfahrens;

Fig. 3 zeigt die Anzeige einer Zuordnung auf dem Bildschirm eines SB-Terminals, das eine Systemkomponente des Systems nach Fig. 1 darstellt; und

Fig. 4a-c zeigen in drei Varianten die Anzeige eines Eingabeschemas auf dem Touchpad eines mobilen Benutzer-Endgerätes, das eine Systemkomponente des Systems nach Fig. 1 darstellt;

Die Fig. 1 zeigt den prinzipiellen Aufbau eines erfindungsgemäßen Systems zur Authentifizierung und Durchführung einer Transaktion an einem Selbstbedienungsterminal, auch kurz SB-Terminal genannt, des Systems. Als SB-Terminal ist beispielhaft ein Geldautomat ATM gezeigt, der Transaktionen zur Auszahlung von Bargeld durchführen kann. Außerdem sind folgende Komponenten des Geldautomaten dargestellt: ein Geldausgabeschacht DPNS, ein Identifikations-Vorrichtung ID-DEV, hier in Gestalt

eines Kartenlesers für Chip-Karten, und ein Bildschirm DISP sowie ein Rechner bzw. Computer PC, der die Abläufe in dem Geldautomaten steuert und in Verbindung mit netzwerkseitigen Einheiten steht. Der Rechner PC und der Bildschirm DISP bilden die Zentraleinheit des Geldautomaten ATM. Die Identifikations-Vorrichtung ID-DEV dient hier zum Lesen von Kundenkarten und ist somit Teil eines zusätzlichen Sicherheitskanals (Security Channel), der neben der PIN-Eingabe vorgesehen ist.

Zu den netzwerkseitigen Einheiten des Systems zählen: ein zentraler Server SRV, der für eine größere Anzahl von Geldautomaten zuständig ist, ein PIN-Server PINSRV, der die Eingabe von Identifizierungsdaten prüft. Der Server SRV ist mit einem Server-Netzwerk NET verbunden, welches für weitere Geldautomaten zuständig ist und eine sog. Cloud bilden kann.

Der Benutzer CSM des Geldautomaten ATM hat ein mobiles Benutzer-Endgerät MD, z.B. ein Smartphone, auf dem eine Applikation MBA installiert ist, um die Transaktion, wie nachfolgend beschrieben, von seinem Smartphone aus durchführen zu können. Diese Applikation wird nachfolgend auch Mobile Banking Application MBA genannt und läuft auf dem Smartphone des Kunden, um das Benutzer-Interface (User Interface) für die Transaktion wiederzugeben. Der Geldautomat ATM kann sehr weit entfernt vom Server SRV sein. Insgesamt sind die Server und Geldautomaten sowie die mobilen Benutzer-Endgeräte über sichere (Netzwerk-) Kanäle verbunden, die wie z.B. über 3G, 4G, WIFI und WAN-Verbindungen, die jeweils z.B. mit SSL oder TLS abgesichert sind. Es besteht aber keine direkte Netzwerkverbindung zwischen Geldautomat ATM und mobilen Endgerät MD.

Das erfindungsgemäße Verfahren 100 wird anhand der Fig. 2 beschrieben, wobei auch auf die Fig. 1 Bezug genommen wird. Die Schritte des Verfahrens sind spaltenweise angeordnet und den jeweiligen Systemkomponenten MBA, ATM und SRV / NET bzw. dem beteiligten Benutzer CSM zugewiesen.

In einem ersten Schritt 101 veranlasst der Benutzer CSM den Beginn einer neuen Transaktion, hier einer Bargeldauszahlung. Dazu startet der Kunde die App MBA auf

seinem Smartphone und loggt sich dort ein, z.B. über sein MBA-Passwort, wodurch die Verbindung zum Server hergestellt wird.

Der Geldautomaten ATM fragt im Schritt 102 nach Identifizierungsdaten, die auch die sog. PAN (primary account number) der Kundenbankkarte enthalten können. Der Benutzer führt seine Bankkarte in den Kartenleser ID-DEV ein. Alternativ dazu hält er seine NFC-Karte an den Kartenleser. Dieser Schritt der ID-Prüfung über einen zweiten Sicherheits-Kanal ist optional und dient der zusätzlichen Sicherheit.

Der ATM prüft nun im Schritt 104, ob der Benutzer sich tatsächlich vor dem Geldautomaten befindet. Dazu wird vom Server ein zufälligen mehrstelliger Zahlencode erzeugt und an den Geldautomaten ATM. übertragen, welcher einen passenden grafisch darstellbarer Code (Barcode, QR-Code) erzeugt und auf dem Bildschirm DISP angezeigt. Der Kunde hält sein Smartphone MD bzw. dessen Kamera so an den Bildschirm, dass die App MBA mittels der Kamera Barcode lesen bzw. einscannen und in den passenden Zahlencode umwandeln. Die auf dem Smartphone des Benutzers installierte App. MBA scannt im Schritt 105 mit Hilfe der Smartphone-Kamera den Code vom Bildschirm ab und sendet das Ergebnis über eine Mobilkommunikationsverbindung an den Server bzw. das Netzwerk SRV / NET, wo geprüft wird, ob die Ergebnisdaten zu dem angezeigten Code passen. Wenn dies der Fall ist, dann wird festgestellt, dass der Benutzer sich tatsächlich am Geldautomaten befindet. Die Transaktion wird dann weitergeführt. Auch dieser Schritt ist optional und richtet sich je nach den Sicherheitsvorschriften der Bank oder internationaler bzw. landestypischer Institutionen. Möglicherweise genügt auch ein in dem Smartphone ggf. vorhandener Chip für NFC (Nahfeldkommunikation). Außerdem ist das Erzeugen und Scannen eines Barcodes nur eine von vielen Möglichkeiten. Es könnte auch eine zufällig generierte Grafik genutzt werden. Oder es könnte auf das Anzeigen und Abtasten grafischer Kennungen verzichtet werden. Stattdessen könnten die Daten des Kunden auch über das Smartphone zusammen mit einer Ortsangabe (z.B. GPS/GSMIWIWI) an den Server gesendet werden, um zu prüfen, ob der Kunde sich am Ort des betreffenden Geldautomaten ATM befindet.

Was die Identität des Servers angeht, so wird diese von der App MBA z.B. mittels SSL-Zertifikat festgestellt. Alternativ könnte ein optisches Barcode-Verfahren, wie zuvor

beschrieben, verwendet werden. Dann würde die App zwei Barcodes scannen müssen. In diesem Fall sollten beide Scanvorgänge unmittelbar nacheinander durchgeführt werden. Dann dürften sie vom Kunden kaum wahrgenommen, geschweige denn als störend empfunden werden. Ein Zertifikat hat jedoch den Vorteil, dass es sicher ist gegenüber einem Angriff per Fake-ATM nebst Fake-Server.

In den nächsten Schritten 107 – 111 wird die Anfrage und sichere Eingabe von Identifizierungsdaten bezüglich der PIN durchgeführt. Hierzu wird auch auf die Fig. 3 und Fig. 4a-c Bezug genommen:

Im Schritt 107 wird auf dem Bildschirm des Geldautomaten ATM eine Zuordnung von ersten Elementen, nämlich Ziffern 0, 1, 2, ...9, zu zweiten Elementen, nämlich Buchstaben A, B, C, D J, angezeigt und zwar in einer vorzugsweise pseudo-zufälligen Reihenfolge. Dazu generiert der Server eine Permutation der Ziffern von 0 bis 9 und sendet diese an den Geldautomaten ATM, der dann Buchstaben und Zahlen wie in Fig. 3 gezeigt, anzeigt. Die Zuordnung ist nur dem PIN-Server PINSRV bekannt und wird nicht über das Mobilkommunikationsnetz oder andere unsichere Netzwerk übertragen. Innerhalb der Zuordnung repräsentiert jeder Buchstabe dabei eine Positionsangabe (s. Fig. 3). Bezogen auf die Ziffern-Anordnung auf einem EPP bedeutet dies, dass jede Ziffer einer Position bzw. einem Buchstaben eineindeutig zugeordnet ist, z.B. ist 5 auf Position D und 4 auf Position H. Die Zuordnung wird lediglich auf dem Bildschirm des Geldautomaten ATM für eine vorgebbare Zeitdauer angezeigt, so dass der Benutzer sich die Zuordnung einprägen kann bzw. anhand der Zuordnung seine PIN in Buchstaben chiffrieren kann. Beispielsweise lautet die vierstellige PIN wie folgt „3456“. Der Benutzer erkennt anhand der in Fig. 3 dargestellten Zuordnung, dass die Buchstabenfolge wie folgt sein muss: A-H-D-J.

Nun wird im Schritt 108 durch die App MBA ein Eingabeschema auf dem Touchpad des Smartphones angezeigt, so wie dies in den Fig. 4a-c an drei Beispielen dargestellt ist. Demnach wird nicht die Zuordnung und auch nicht die PIN-Tastatur angezeigt, sondern eine Anordnung der zweiten Elemente (hier der Buchstaben), wobei die Anordnung auch pseudo-zufällig erzeugt werden kann. Die Fig. 4a zeigt zum besseren Verständnis der

Erfindung nur keine pseudo-zufällige Anordnung, sondern die Anordnung der Buchstaben entsprechend ihrer alphabetischen Rangfolge, also: A-B-C-D-....-J.

5 Zur Abfrage der PIN wird der Benutzer im Schritt 109 aufgefordert die entsprechenden Buchstaben am Touchpad seines Smartphones einzugeben. Im Beispiel hier würde er die Buchstabenfolge: A-H-D-J eingeben. Die App. MBA sendet dann im Schritt 110 jeden Buchstaben einzeln oder die gesamte Folge (alle vier chiffrierten Daten) an den Server SRV bzw. PIN-Server. Dieser kann dann die chiffrierten Daten entschlüsseln und feststellen, wie die echte PIN lautet. Im Schritt 112, d.h. in der eigentlichen
10 Authentifizierung, kann dann die Transaktion freigegeben werden. Der Geldautomat zahlt im Schritt 113 das gewünschte Bargeld aus, und der Benutzer entnimmt es im Schritt 114 aus dem Geldausgabefach.

15 Anstelle eines streng geordneten Eingabeschemas, wie es in Fig. 4a dargestellt ist, können auch ungeordnete Eingabeschemen bzw. Anordnungen der Buchstaben angezeigt werden, so wie es die Fig. 4b und 4c beispielhaft zeigen. Die Anordnung wird vorzugsweise über einen Pseudo-Zufallsprozess erzeugt und als Bildschirmtastatur auf dem Touchpad des Smartphones angezeigt. Die Erzeugung der Bildschirmtastatur kann für jede neue Transaktion durchgeführt werden, wobei die große Kombinationsmöglichkeit der
20 angeordneten Tasten ganz ausgeschöpft werden kann.

Die Erfindung kann insbesondere bei SB-Terminals realisiert werden, bei denen auf eine eigene PIN-Eingabetastatur und die dafür erforderliche EPP-Sonderelektronik verzichtet wurde. Die Erfindung ermöglicht es, dass mithilfe des Smartphones des Kunden eine
25 sichere PINEingabe durchgeführt werden kann. Dabei kann auch sicher festgestellt werden, dass sich das Smartphone des Kunden tatsächlich in unmittelbarer Nähe des Geldautomaten ATMs befindet. Das beschriebene Verfahren ist weitaus weniger anfällig für Manipulationen und Skimming, als bei der klassischen Eingabe einer PIN über ein EPP der Fall ist.

30 Die obige Beschreibung zusammenfassend wird zur sicheren Eingabe einer PIN oder anderen Identifizierungsdaten eine dynamisch vorgebbare Zuordnung von Tastenposition und Tastenwert in Form eines flexiblen Eingabeschemas vorgeschlagen. Dazu wird auf

dem Geldautomaten-Bildschirm eine vorgegebene, vorzugsweise pseudo-zufällig erzeugte, Zuordnung von Tastenwerten bzw. Ziffern aus dem Zahlenraum 0-9 zu Tastenposition in Form von Symbolen, Buchstaben A, B, C... oder dergleichen angezeigt. Allerdings werden auf dem Benutzer-Smartphone nur die Tastenpositionen, d.h. die Symbole, Buchstaben oder dergleichen in Form eines Eingabeschemas angezeigt. Der Benutzer gibt nicht seine PIN (z.B. „3456“) ein, sondern gibt nur die entsprechend dem Eingabeschema zugeordneten Tastenpositionen („AHDJ“) ein. Dies hat den Vorteil, dass durch den Benutzer keine PIN-Eingabe mehr erfolgt, die ausgespäht werden könnte. Es werden nur die Daten (Buchstaben) der zugehörigen Tastenpositionen („AHDJ“) eingegeben. Das Smartphone kennt die PIN nicht, auch der Geldautomat ATM kennt die PIN nicht, sondern lediglich das Schema. Allein der Server kennt Schema und PIN und kann die Transaktion freigeben. Dieses Verfahren ist deshalb sehr sicher.

Mit anderen Worten: Jeder Buchstabe repräsentiert eineindeutig eine Positionsangabe. Auf dem Smartphone werden nur Positionsangaben (Buchstaben A-J) gezeigt, nicht aber die zugeordneten Ziffern. Jede vom Benutzer eingetippte Positionsangabe wird von der App MBA an den Server übermittelt. Da der Server sowohl die PIN kennt, als auch die an den Geldautomaten ATM übermittelte Permutation der Ziffern 0-9, kann er nun vergleichen, ob der Kunde die korrekte PIN eingegeben hat. Der Geldautomat ATM hat keinerlei Informationen über die PIN des Kunden, ihm wurde lediglich eine zufällige Permutation gesendet. Die App MBA hat lediglich Positionsangaben vom Kunden erhalten, hat aber mangels Kenntnis der Permutation keinerlei Möglichkeiten auf die Zugehörige PIN zu schließen. Die PIN ist ausschließlich dem Kunden und dem Server bekannt! Das Anzeigen der Positionen mittels Buchstaben ist nur ein möglicher Weg. Genauso könnten z.B. die Positionen mit verschiedenen Grafiken, geometrischen Figuren oder Grauwerten dargestellt werden.

Da die Erfindung für eine Transaktion das Smartphone des jeweiligen Benutzers einsetzt, können am Geldautomaten ATM insbesondere das PIN-Pad / EPP eingespart werden.

Die Sicherheit des Verfahrens lässt sich bei Bedarf weiter erhöhen, indem für jede Ziffer neue Permutationen generiert und angezeigt werden. Auch hier werden die Permutationen wieder im Server gespeichert, um dann später den Vergleich der vom Kunden

einggegebenen PIN mit der im Server gespeicherten PIN durchführen zu können. Da diese Informationen über das Smartphone des Kunden eingegeben werden, ist Skimming wesentlich schwieriger zu realisieren, da es mangels EPP keine fest installierte Tastatur am Geldautomaten ATM gibt. Auch müssten sowohl das Display des ATMs als auch das Smartphone samt Finger des Kunden "überwacht" werden.

Optional kann zur Überprüfung, ob das Smartphone sich im unmittelbaren Bedienbereich des Geldautomaten ATM befindet, ein optisch scannbarer Code (Barcode / QR-Code oder allg. auch eine Grafik) erzeugt und auf dem Bildschirm des Geldautomaten angezeigt werden. Dann erfolgt das Scannen des Codes mit dem Smartphone und Senden der Daten an einen Server, der schließlich die Daten mit dem im Server hinterlegten Code vergleicht. Somit kann einfach festgestellt, dass das Smartphone sich im unmittelbaren Bedienbereich des Geldautomaten befindet und somit wohl zu dem Benutzer gehört.

Patentansprüche

1. Verfahren (100) zur gesicherten Eingabe von Identifizierungsdaten (PIN) für die Authentifizierung einer Transaktion, die mittels eines Selbstbedienungsterminals (ATM) durchgeführt wird, gekennzeichnet durch folgende Schritte:

5 zu einer ersten Datenmenge mit ersten Elementen (0, 1, 2, 3, ... 9), aus denen die Identifizierungsdaten (PIN) gebildet werden, wird eine zweite Datenmenge mit zweiten Elementen (A, B, C, ... J) gebildet, welche jeweils einem der ersten Elemente (0, 1, 2, 3, ... 9) eineindeutig zugeordnet sind, wodurch aus den zweiten
10 Elementen Eingabedaten (#PIN) erzeugbar sind, die einer bijektiven Abbildung der Identifizierungsdaten (PIN) entsprechen (Schritt 201);

die eineindeutige Zuordnung der zweiten Elemente (A, B, C, ... J) zu den ersten Elementen (0, 1, 2, 3, ... 9) wird auf einem Bildschirm (DISP) angezeigt, der baulich mit dem Selbstbedienungsterminal (ATM) verbunden ist (Schritt 207);

15 an einem Benutzer-Endgerät (MD), das baulich getrennt von dem Selbstbedienungsterminal (ATM) ist und einem Benutzer (CSM) des Selbstbedienungsterminals (ATM) zugeordnet ist, werden die zweiten Elemente (A, B, C, ... J) und nicht die ersten Elemente (0, 1, 2, 3, ... 9) angezeigt (Schritt 208);

an dem Benutzer-Endgerät (MD) werden durch den Benutzer (CSM) die
20 Eingabedaten (#PIN) eingegeben (Schritt 209); und

die Eingabedaten (#PIN) werden mittels eines Anwendungs-Programms (MBA) an eine oder mehrere mit dem Selbstbedienungsterminal (ATM) verbundene rechnergestützte Einheiten (SRV; PINSRV) übertragen, die die eineindeutige Zuordnung der zweiten Elemente (A, B, C, ... J) zu den ersten Elementen (0, 1, 2,
25 3, ... 9) verwalten und die Authentifizierung der Transaktion durchführen (Schritt 209).
2. Verfahren (100) nach Anspruch 1, dadurch gekennzeichnet, dass die ersten Elemente die Tastenwerte (0, 1, 2, ... 9) einer numerischen Tastatur umfassen und
30 dass die zweiten Elemente Komponenten eines vorgebbaren Schemas umfassen, insbesondere Symbole, insbesondere Buchstaben (A, B, C...J) eines Alphabets, Graustufen einer Graustufenskala, Farben einer Farbskala und/oder Positionen

eines Positionsschemas umfassen.

3. Verfahren (100) nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die Zuordnung der zweiten Datenmenge zu der ersten Datenmenge mittels einer Pseudo-Zufalls-Zuordnung der zweiten Elemente (A, B, C, ... J) zu den ersten Elementen (0, 1, 2, 3, ... 9) gebildet wird, insbesondere vor jeder Durchführung einer neuen Transaktion erneut gebildet wird (Schritt 201).
4. Verfahren (100) nach einem vorhergehenden Anspruch, dadurch gekennzeichnet, dass das Benutzer-Endgerät ein mobiles Benutzer-Endgerät, insbesondere ein Smartphone (MD), mit einem Berührungsbildschirm bzw. Touchscreen ist, dass die zweiten Elemente, insbesondere als Symbole (A, B, C, ... J) des vorgebbaren Schemas, an dem Berührungsbildschirm angezeigt werden (Schritt 208), und dass die Eingabedaten (#PIN) an dem Berührungsbildschirm von dem Benutzer (CSM) eingegeben werden (Schritt 209).
5. Verfahren (100) nach einem vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das Benutzer-Endgerät (MD) eine Kamera aufweist und dass zur Überprüfung, ob sich das Benutzer-Endgerät (MD) in der Nähe des Selbstbedienungsterminals (ATM) befindet, auf dem Bildschirm (DISP) ein grafischer Code, insbesondere ein Barcode, angezeigt wird (Schritt 204); dass der grafische Code von der Kamera des Benutzer-Endgerätes (MD) erfasst, insbesondere abgetastet, wird (Schritt 205); und dass von dem Benutzer-Endgerät (MD) Kenndaten des erfassten grafischen Codes an die eine oder mehreren mit dem Selbstbedienungsterminal (ATM) verbundenen rechnergestützten Einheiten (MBA; SRV; PINSRV) übertragen werden, die die Kenndaten des grafischen Codes verwalten und die Authentifizierung der Transaktion durchführen (Schritt 206).
6. System zur Authentifizierung und Durchführung einer Transaktion an einem Selbstbedienungsterminal (ATM) des Systems, wobei das System zur Authentifizierung der Transaktion mittels einer gesicherten Eingabe von Identifizierungsdaten (PIN) eine oder mehrere mit dem Selbstbedienungsterminal (ATM) verbundene rechnergestützte Einheiten (SRV; PINSRV) umfasst,

gekennzeichnet durch folgende Systemkomponenten:

eine erste rechnergestützte Einheit (PINSRV), die zu einer ersten Datenmenge mit ersten Elementen (0, 1, 2, 3, ... 9), aus denen die Identifizierungsdaten (PIN) gebildet werden, eine zweite Datenmenge mit zweiten Elementen (A, B, C, ... J) bildet, welche jeweils einem der ersten Elemente (0, 1, 2, 3, ... 9) eineindeutig zugeordnet sind, wodurch aus den zweiten Elementen Eingabedaten (#PIN) erzeugbar sind, die einer bijektiven Abbildung der Identifizierungsdaten (PIN) entsprechen;

einen Bildschirm (DISP), der baulich mit dem Selbstbedienungsterminal (ATM) verbunden ist und die eineindeutige Zuordnung der zweiten Elemente (A, B, C, ... J) zu den ersten Elementen (0, 1, 2, 3, ... 9) anzeigt;

ein Benutzer-Endgerät (MD), das baulich getrennt von dem Selbstbedienungsterminal (ATM) ist, einem Benutzer (CSM) des Selbstbedienungsterminals (ATM) zugeordnet ist und die zweiten Elemente (A, B, C, ... J) und nicht die ersten Elemente (0, 1, 2, 3, ... 9) anzeigt, um dem Benutzer (CSM) zu ermöglichen, die Eingabedaten (#PIN) an dem Benutzer-Endgerät (MD) einzugeben;

wobei ein auf dem Benutzer-Endgerät (MD) implementiertes Anwendungs-Programm (MBA) die Eingabedaten (#PIN) an eine zweite rechnergestützte Einheiten (SRV) überträgt, die die Authentifizierung der Transaktion durchführt, und wobei die erste rechnergestützte Einheit (PINSRV) die eineindeutige Zuordnung der zweiten Elemente (A, B, C, ... J) zu den ersten Elementen (0, 1, 2, 3, ... 9) verwaltet.

7. System nach Anspruch 6, dadurch gekennzeichnet, dass das Selbstbedienungsterminal ein Geldautomat (ATM) ist, insbesondere ein Geldautomat (ATM) ist, der keine Tastatur zur Eingabe der Identifizierungsdaten (PIN) aufweist.
8. System nach Anspruch 6 oder 7, dadurch gekennzeichnet, dass das Benutzer-Endgerät ein mobiles Benutzer-Endgerät, insbesondere ein Smartphone (MD), mit einem Berührungsbildschirm bzw. Touchscreen ist, das die zweiten Elemente (A, B, C, ... J), insbesondere entsprechend einem vorgebbaren Schema, an dem

Berührungsbildschirm anzeigt, um dem Benutzer (CSM) zu ermöglichen, die Eingabedaten (#PIN) an dem Berührungsbildschirm anstelle der Identifizierungsdaten (PIN) einzugeben.

- 5 9. System nach einem der Ansprüche 6 bis 8, dadurch gekennzeichnet, dass das
Benutzer-Endgerät (MD) eine Kamera aufweist und dass zur Überprüfung, ob sich
das Benutzer-Endgerät (MD) in der Nähe des Selbstbedienungsterminals (ATM)
befindet, der Bildschirm (DISP) des Selbstbedienungsterminals (ATM) einen
grafischen Code, insbesondere einen Barcode, anzeigt; dass die Kamera des
10 Benutzer-Endgerätes (MD) den grafische Code erfasst, insbesondere abgetastet;
und dass das Benutzer-Endgerät (MD) Kenndaten des erfassten grafischen Codes
an die eine oder mehreren mit dem Selbstbedienungsterminal (ATM) verbundenen
rechnergestützten Einheiten (SRV; PINSRV) überträgt, die die Authentifizierung
der Transaktion durchführen und die Kenndaten des grafischen Codes verwalten.

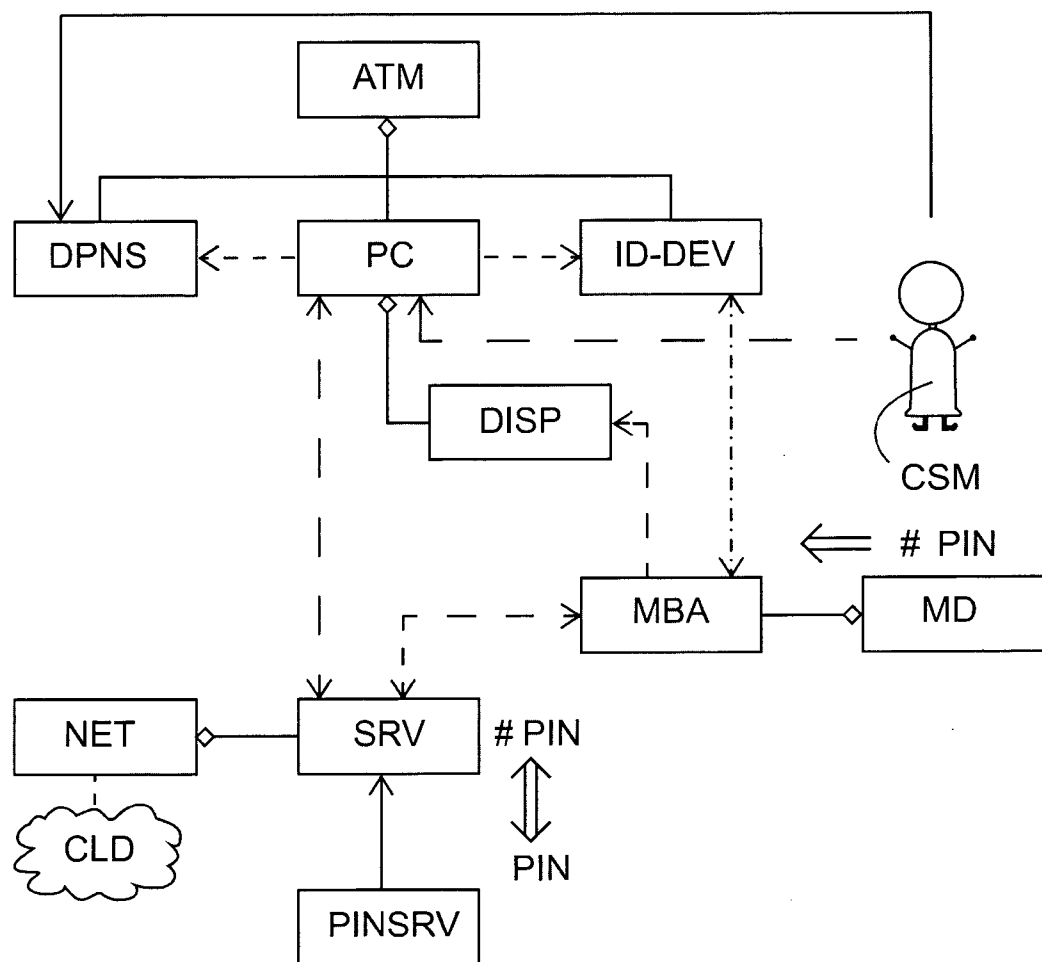


Fig.1

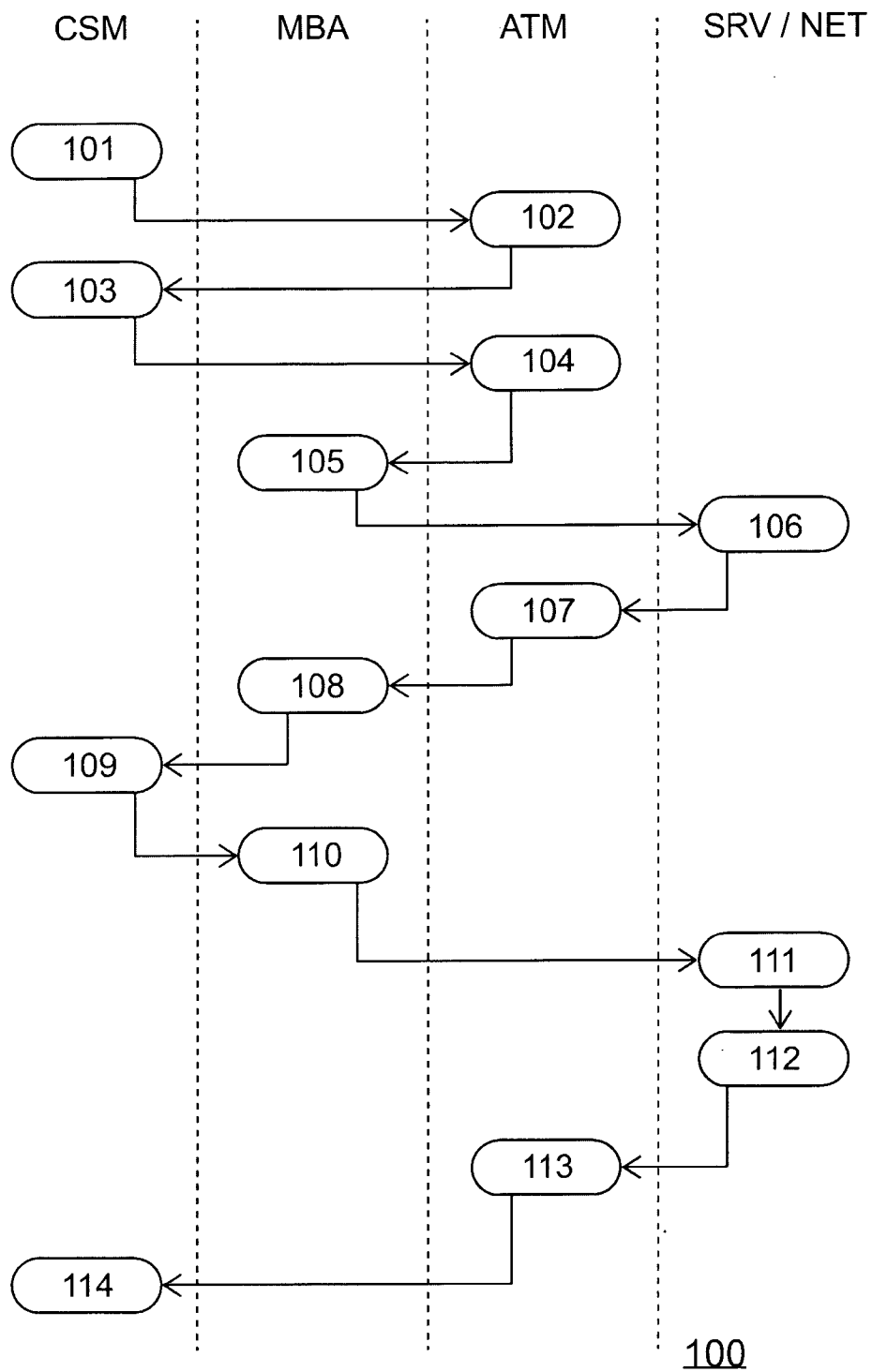


Fig.2

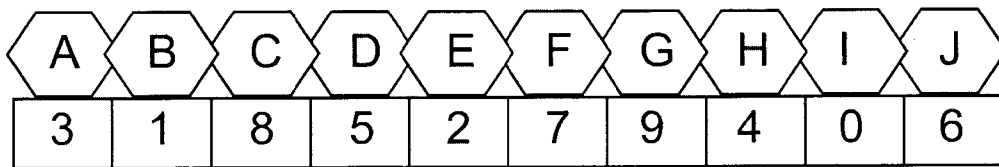


Fig.3

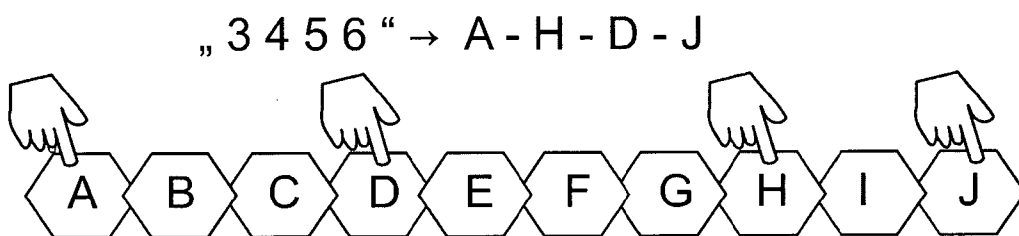


Fig.4a

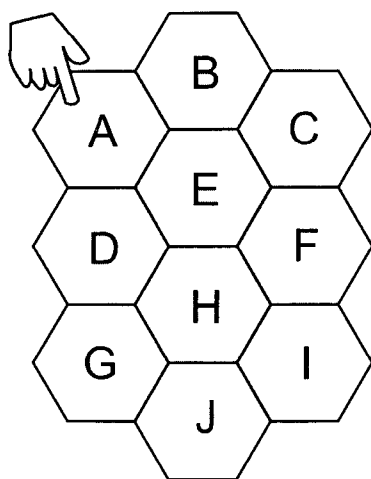


Fig.4b

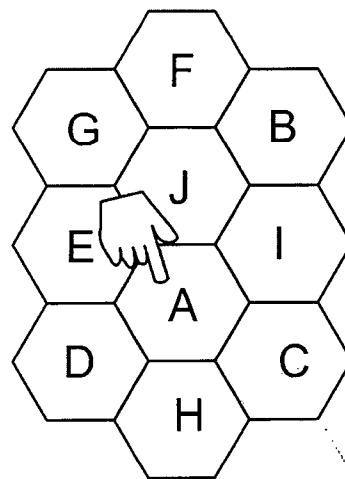


Fig.4c

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2013/068381

A. CLASSIFICATION OF SUBJECT MATTER INV. G07F7/10 G06F21/36 G07F19/00 G06Q20/32 G06Q20/40 ADD.		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) G07F G06Q G06F		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) EPO-Internal, WPI Data		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2012/047564 A1 (LIU SHIH-LIANG [ZA]) 23 February 2012 (2012-02-23) abstract; figures paragraphs [0044] - [0048], [0053], [0056] - [0074], [0085] - [0094] -----	1-9
A	WO 2004/057516 A1 (SHIN HWA-SHIK [KR]) 8 July 2004 (2004-07-08) abstract; figures page 7, line 5 - page 11, line 6 -----	1-9
A	DE 10 2007 043843 A1 (BORCHERT BERND [DE]) 22 January 2009 (2009-01-22) abstract; figures paragraphs [0011] - [0019], [0023], [0026], [0035] - [0038], [0046] ----- -/--	1-9
☒ Further documents are listed in the continuation of Box C. ☒ See patent family annex.		
* Special categories of cited documents : "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search		Date of mailing of the international search report
26 September 2013		04/10/2013
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Authorized officer Breugelmans, Jan

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2013/068381

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	GB 2 457 733 A (MOBANK LTD [GB]) 26 August 2009 (2009-08-26) abstract; figures page 2, line 26 - page 3, line 31 page 13, lines 15-26 page 14, line 8 - page 15, line 24 page 16, line 5 - page 17, line 25 page 18, line 25 - page 19, line 5 page 20, line 16 - page 22, line 28 -----	1-9
A	WO 2007/091869 A2 (HWANG JAY-YEOB [KR]) 16 August 2007 (2007-08-16) abstract; figures paragraphs [0009], [0019] - [0048], [0060] - [0061] -----	1-9
A	US 2008/222048 A1 (HIGGINS KEVIN L [US] ET AL) 11 September 2008 (2008-09-11) abstract; figures -----	1-9

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2013/068381

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2012047564 A1	23-02-2012	AU 2010247014 A1 CA 2760200 A1 CN 102422302 A EP 2430587 A1 RU 2011150620 A US 2012047564 A1 WO 2010131218 A1	24-11-2011 18-11-2010 18-04-2012 21-03-2012 20-06-2013 23-02-2012 18-11-2010
WO 2004057516 A1	08-07-2004	AU 2003289512 A1 KR 20040056273 A US 2006053301 A1 WO 2004057516 A1	14-07-2004 30-06-2004 09-03-2006 08-07-2004
DE 102007043843 A1	22-01-2009	NONE	
GB 2457733 A	26-08-2009	EP 2260432 A1 GB 2457733 A US 2011191856 A1 WO 2009106800 A1	15-12-2010 26-08-2009 04-08-2011 03-09-2009
WO 2007091869 A2	16-08-2007	EP 1987435 A2 KR 20070081048 A US 2009300732 A1 WO 2007091869 A2	05-11-2008 14-08-2007 03-12-2009 16-08-2007
US 2008222048 A1	11-09-2008	NONE	

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/EP2013/068381

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES INV. G07F7/10 G06F21/36 G07F19/00 G06Q20/32 G06Q20/40 ADD.		
Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC		
B. RECHERCHIERTE GEBIETE Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole) G07F G06Q G06F		
Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen		
Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe) EPO-Internal, WPI Data		
C. ALS WESENTLICH ANGESEHENE UNTERLAGEN		
Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 2012/047564 A1 (LIU SHIH-LIANG [ZA]) 23. Februar 2012 (2012-02-23) Zusammenfassung; Abbildungen Absätze [0044] - [0048], [0053], [0056] - [0074], [0085] - [0094] -----	1-9
A	WO 2004/057516 A1 (SHIN HWA-SHIK [KR]) 8. Juli 2004 (2004-07-08) Zusammenfassung; Abbildungen Seite 7, Zeile 5 - Seite 11, Zeile 6 -----	1-9
A	DE 10 2007 043843 A1 (BORCHERT BERND [DE]) 22. Januar 2009 (2009-01-22) Zusammenfassung; Abbildungen Absätze [0011] - [0019], [0023], [0026], [0035] - [0038], [0046] ----- -/--	1-9
☒ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen ☒ Siehe Anhang Patentfamilie		
* Besondere Kategorien von angegebenen Veröffentlichungen : "A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist "E" frühere Anmeldung oder Patent, die bzw. das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist "L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt) "O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht "P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist "T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist "X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden "Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist "&" Veröffentlichung, die Mitglied derselben Patentfamilie ist		
Datum des Abschlusses der internationalen Recherche 26. September 2013		Absendedatum des internationalen Recherchenberichts 04/10/2013
Name und Postanschrift der Internationalen Recherchenbehörde Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Bevollmächtigter Bediensteter Breugelmans, Jan

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN		
Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	GB 2 457 733 A (MOBANK LTD [GB]) 26. August 2009 (2009-08-26) Zusammenfassung; Abbildungen Seite 2, Zeile 26 - Seite 3, Zeile 31 Seite 13, Zeilen 15-26 Seite 14, Zeile 8 - Seite 15, Zeile 24 Seite 16, Zeile 5 - Seite 17, Zeile 25 Seite 18, Zeile 25 - Seite 19, Zeile 5 Seite 20, Zeile 16 - Seite 22, Zeile 28 -----	1-9
A	WO 2007/091869 A2 (HWANG JAY-YEOB [KR]) 16. August 2007 (2007-08-16) Zusammenfassung; Abbildungen Absätze [0009], [0019] - [0048], [0060] - [0061] -----	1-9
A	US 2008/222048 A1 (HIGGINS KEVIN L [US] ET AL) 11. September 2008 (2008-09-11) Zusammenfassung; Abbildungen -----	1-9

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP2013/068381

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
US 2012047564	A1	23-02-2012	AU	2010247014 A1	24-11-2011
			CA	2760200 A1	18-11-2010
			CN	102422302 A	18-04-2012
			EP	2430587 A1	21-03-2012
			RU	2011150620 A	20-06-2013
			US	2012047564 A1	23-02-2012
			WO	2010131218 A1	18-11-2010

WO 2004057516	A1	08-07-2004	AU	2003289512 A1	14-07-2004
			KR	20040056273 A	30-06-2004
			US	2006053301 A1	09-03-2006
			WO	2004057516 A1	08-07-2004

DE 102007043843	A1	22-01-2009	KEINE		

GB 2457733	A	26-08-2009	EP	2260432 A1	15-12-2010
			GB	2457733 A	26-08-2009
			US	2011191856 A1	04-08-2011
			WO	2009106800 A1	03-09-2009

WO 2007091869	A2	16-08-2007	EP	1987435 A2	05-11-2008
			KR	20070081048 A	14-08-2007
			US	2009300732 A1	03-12-2009
			WO	2007091869 A2	16-08-2007

US 2008222048	A1	11-09-2008	KEINE		
