(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 October 2012 (18.10.2012)

WIPO | PCT

(10) International Publication Number
WO 2012/141588 A1

(51) **International Patent Classification**:
G06Q 30/00 (2012.01) ***G06Q 20/16*** (2012.01)
G06Q 20/00 (2012.01)

(21) **International Application Number**:
PCT/NL2012/050248

(22) **International Filing Date**:
16 April 2012 (16.04.2012)

(25) **Filing Language**: Dutch

(26) **Publication Language**: English

(30) **Priority Data**:
2006608 14 April 2011 (14.04.2011) NL

(71) **Applicant** *(for all designated States except US)*: **SEPASOFT B.V.** [NL/NL]; Vughterweg 5, NL-5211 CJ 's-hertogenbosch (NL).

(72) **Inventor; and**
(75) **Inventor/Applicant** *(for US only)*: **TEN CATE, Eugène Raymond** [NL/NL]; NL-2804 MT Gouda (NL).

(74) **Agent**: **HYLARIDES, Paul Jacques**; Sweelinckplein 1, NL-2517 GK Den Haag (NL).

(81) **Designated States** *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, 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, KM, 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, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (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, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report (Art. 21(3))*

WO 2012/141588 A1

(54) **Title**: ASSEMBLY AND METHOD OF HANDLING TRANSACTIONS

(57) **Abstract**: The invention relates to an assembly for handling transactions between a merchant and a consumer, comprising: - a payment terminal for generating and sending an electronic transaction order; - a payment system for electronic transfer of a transaction amount from the bank account of the consumer to the bank account of the merchant; - a transaction order processor for electronic clearing and settlement of the transaction amount, wherein the transaction order processor is adapted to control the payment system for transfer of the transaction amount, wherein the assembly comprises a group of transaction order processors, wherein each of the transaction order processors is connected to a payment system and wherein a payment management system (PMS) is arranged between the payment terminal and the transaction order processors which is adapted to select one transaction order processor from the group of transaction order processors and to control the associated payment system with the selected transaction order processor.

ASSEMBLY AND METHOD OF HANDLING TRANSACTIONS

The present invention relates to an assembly for handling transactions between at least one merchant and at least one consumer. The invention also relates to the payment management system of said assembly and to a method for handling such transactions.

For handling electronic transactions between a consumer and a merchant, (for instance a retailer) use is made of a system which is made up of inter alia a number of point of payment terminals, for instance a Point of Sale (POS) terminal, a number of banks and a transaction order processor which controls the electronic clearing and settlement of the transaction amount with the relevant banks. In general these systems are regionally oriented; each country has for instance its own transaction order processor and many of the banks involved are only operational in one or a limited number of countries.

Shown schematically in figure 1 is a typical set-up of such a system. The system is set up per region. The example shows only three regions (R1, R2 and R3), but this number can of course vary. When consumer 1 in the first region (R1) wishes to make a payment using his/her payment card 2 for the purchase of a product in a shop, the consumer inserts the card 2 into a payment terminal 4. The payment terminal disposed in the shop allows payments to be made according to one or more specific card schemes or card protocols. The terminal can optionally be coupled electronically to a cash register 3 which performs a part of the payment process. When the consumer 1 authorizes a payment, for instance by allowing his/her payment card to be read and entering a personal identification number (PIN) via a keyboard on the payment terminal, the payment terminal 4

generates an electronic transaction order. The payment terminal forwards the transaction order via a secure connection 9 to a so-called transaction order processor 5, also referred to here as the processor. This processor is in turn connected via secure connections 10 and 11 to a payment system. In the shown example the payment system comprises an issuer bank 6 and an acquirer bank 7. The transaction order now ensures that the transaction amount is debited from the account of the consumer at the issuer bank 6 and is credited (b) to the account of the merchant at the acquirer bank 7. A merchant in a specific area does not have a free choice of processor. The area in which the merchant is located determines the processor 5 (and thereby also the banks) with which the merchant has to do business.

The transaction order processor 5, more specifically the server handling the electronic transactions with the affiliated banks, and the payment system (i.e. the banks) normally operate in a limited geographical area. Banks within this limited geographical area have agreed to perform all their payment transfers via one central transaction order processor 5 and the merchants in this limited geographical area are obliged to work with payment terminals which have a one on one relation with said processor. It is therefore not possible for a merchant to personally select the processor handling the payment transfers. In the case of payments between various such geographical areas, for instance between the first region (R1) and the second region (R2), the processor 5 of the one area makes contact via a communication connection 39 with a processor 5' in the other area and the handling of the transaction is provided by two (of more) processors 5 and 5'. Nor does the merchant therefore have any freedom of choice in respect of the processor of the second area (R2).

This lack of freedom of choice is often not advantageous for the merchant for competitive reasons.

When the merchant, for instance a retailer, moreover has shops in various of such geographical areas (R1,R2,R3), he/she has to have contracts with the acquirer banks 7 so as to be able to make use of their services and with the associated processor 5 so as to make use of the payment terminal determined by processor 5. For a store chain with shops in two or more different regions contracts must therefore be concluded with different processors and banks to enable payments with the payment terminals in all these areas. The result hereof is that such store chains have to make extra costs. They often also need several regional bank accounts to be able to receive their payments, this resulting in inefficiencies in the management of cash flows of the merchants. It is further the case that each processor employs its own handling protocol and moreover prescribes which types of payment terminal may be used by the merchant. Processors in different countries may employ differing protocols and regulations here, so that the merchant must apply different types of payment terminal and/or different financial software for each country.

It is the object of the present invention to provide a system and method wherein at least one of the above stated drawbacks of the prior art is obviated or at least reduced.

It is a further object of the invention to provide a system and method with which the merchant has more freedom in the choice of transaction order processor allowed to handle the transactions and/or in the choice of the payment system allowed to transfer the transaction amounts.

It is a further object of the invention to provide a system and method with which a merchant can switch from

the one payment system to the other and/or from the one transaction order processor to the other, without needing to replace the existing payment terminals (e.g. POS terminals).

It is a further object of the invention to provide a system and method wherein the authentication of a transaction is performed by a processor.

Provided according to a first aspect of the present invention for the purpose of achieving at least one of the objects is an assembly for handling transactions between at least one merchant and at least one consumer, the assembly comprising:

- at least one payment terminal for generating and sending an electronic transaction order;
- a payment system for electronic transfer of a transaction amount from the bank account of the consumer to the bank account of the merchant;
- a transaction order processor connected to the payment system for electronic clearing and settlement of the transaction amount associated with the transaction order,

wherein the transaction order processor is adapted to receive and process an electronic transaction order and to control the payment system for transfer of the transaction amount associated with the transaction order generated by the payment terminal;

wherein the assembly comprises a group of transaction order processors, wherein each of the transaction order processors is connected to a payment system and wherein a payment management system (PMS) is arranged between the payment terminal and the transaction order processors which is adapted to select one transaction order processor from the group of transaction order processors and to control the associated payment system with the selected transaction order processor.

By arranging a payment management system in the transaction chain between the usual transaction order processor, also referred to here as the processor, and the payment terminal or payment terminals, an in principle free choice of the transaction order processor (i.e. a free processor choice) can be realized for the consumer and/or the merchant. According to embodiments of the invention, the system is flexible such that the payment terminals are no longer required to communicate with a single prescribed transaction order processor (usually operating in only a limited geographical area). It has now become possible, from the viewpoint of the payment terminal, to choose and select a desired transaction order processor from a number of transaction order processors. This makes it possible for instance for the merchant to negotiate with a number of transaction order processors in order to opt for the commercially most advantageous processor.

Transaction order processors often only operate regionally, for instance per country. For interregional payment transfers the transaction order processor which has received a transaction order for interregional payment has heretofore made contact with another transaction order processor. Together they control the payment system or systems. According to embodiments of the invention, it is however possible for the merchant (or the consumer) themselves to select the desired transaction order processor for the purpose of realizing such interregional transactions. It is for instance possible here to envisage a single transaction order processor which performs all regional and interregional transactions for a multinational.

It is noted that the authentication of the transactions continues to be performed by a transaction order processor itself. The usually secret identification

data and identification protocols can thus remain within the domain of the transaction order processor (for instance a card issuer).

According to embodiments of the invention, the transaction order processor is adapted to perform authentication of the received transaction order, in particular of the first and second transaction data described herein. The payment management system can for instance be linked as virtual payment terminal to a transaction order processor. The usual authentication steps, for instance checking identification data such as the PAN and PIN data of a card, are performed by the transaction order processor itself, optionally supplemented by an authentication by the payment terminal. In determined embodiments the payment management system does not perform authentication of these identification data (e.g. PIN and PAN data).

The transaction order processor subsequently sends an authentication signal to the payment management system which is representative of the approval or rejection of the transaction.

A further drawback of the existing systems in which the payment terminals are linked per region to a regional transaction order processor is that the payment terminals of different regions, in any case payment terminals associated with different transaction order processors, have to comply with different technical and/or non-technical requirements. According to embodiments of the invention, the payment management system can however ensure that the different types of payment terminal are nevertheless able to co-act with any random transaction order processor. This provides the merchant with the option of choosing which type of payment terminal he/she is going

to use. This moreover provides the option of certifying a determined type of payment terminal for a larger area.

In determined embodiments the payment management system (PMS) can form a virtual payment terminal. Instead of being connected via a communication connection to a physical payment terminal, a transaction order processor can be connected via the communication connection to a virtual payment terminal in the form of the payment management system. The transaction order processor thinks there is a connection to the physical payment terminal and does not in principle need to notice that there is in reality only a connection to the payment management system. This means that in determined embodiments there is no hardware and/or software modification of the transaction order processors required at all, or at least hardly any.

A payment system can be made up of at least one issuer bank subsystem which manages the bank account of the consumer and an acquirer bank subsystem which manages the bank account of the merchant. The transaction order processor is adapted here to control both subsystems for the purpose of transferring an amount of money from the issuer bank subsystem to the acquirer bank subsystem. When there are two or more different payment systems, according to an embodiment of the invention the payment management system (PMS) can be adapted to select one of the payment systems. This can for instance be realized by selecting one of the transaction order processors which are linked to the selected payment system. According to determined embodiments of the invention, a free bank choice can in principle hereby be realized.

Arranged between the payment terminal and the payment management system, between the payment management system and each of the transaction order processors, and

between the transaction order processors and payment systems (banks) are communication connections which enable a preferably secure mutual data communication.

According to an embodiment of the invention, the payment terminal is adapted to generate and send information concerning the transaction order processor to be selected and/or concerning the payment system to be selected. This information can for instance be formed by an application identifier (ApID). Such an application identifier is representative of the application (e.g. payment product or payment method) used for paying. In determined embodiments the application identifier also determines the acquirer identifier (AID) of the acquiring bank which is going to perform the transaction.

The payment management system (PMS) can further be adapted to receive this information and, on the basis of the received information, to select the transaction order processor which must control the payment system and/or the payment system which must perform the transaction. At the instruction of for instance the merchant and/or the consumer, information can be generated on the payment terminal which influences or even determines the selection of the transaction order processor.

According to an embodiment of the invention the one or more payment terminals are each provided with a read unit for reading first identification data, which are stored on an electronic input carrier and which are representative of the bank account of the consumer. The first identification data can for instance be formed by the primary account number (PAN) of the relevant input carrier (e.g. a payment card). According to an embodiment of the invention, the one or more payment terminals are each provided with an input unit for entry by the consumer of

second identification data representative of the identity of the consumer. The second identification data can for instance be formed by the "personal identification number" (PIN) of the consumer.

The input carrier can be a payment card, more particularly a debit card or a credit card. In other embodiments the input carrier is a loyalty card or a smart card of a mobile telephone. This latter example can relate to a SIM card with EMV functionality. EMV is an acronym for EuroPay MasterCard and Visa which refers to the predetermined specifications defining the structure for international debit/credit cards. EMV relates particularly to the data and the protocol (standard) employed which provides for a relatively high level of data security.

According to embodiments of the invention, the electronic transaction order comprises:

- first transaction data representative of the transaction amount;
- second transaction data representative of the transaction method;
- third transaction data representative of the first identification data;
- fourth transaction data representative of the second identification data.

The payment terminal is preferably adapted to encrypt at least one (but still more preferably all) of the first, second, third and fourth transaction data. In a particularly advantageous embodiment the encryption is performed before sending to the payment management system (PMS) and/or before storing thereof on the payment terminal or on the PMS.

According to an embodiment of the invention, the payment management system (PMS) comprises a storage medium, on which is stored at least:

- unique master terminal identifiers (TID) which are representative of the payment terminals linked to the payment management system (PMS); and/or

- unique master merchant identifiers (MID) which are representative of the merchant associated with each of the payment terminals linked to the payment management system (PMS).

According to an embodiment the payment management system (PMS) comprises a storage medium on which is stored at least:

- a number of unique slave terminal identifiers per unique master TID, each of the slave terminal identifiers being associated with a different transaction order processor.

'Associated with' can be understood here to mean that the identifiers have a different configuration, for instance according to a differing protocol. The slave identifiers are configured (according to a suitable protocol) such that they can be used directly by the associated selected transaction order processor.

In an embodiment of the invention there is also stored on the storage medium:

- a number of unique slave merchant identifiers (slave MIDs) per unique master merchant identifier (master MID), each of the slave merchant identifiers being associated with a different payment system.

According to an embodiment of the invention the payment management system (PMS) is adapted to select a slave TID from the list of slave TIDs and/or to select a slave MID from the list of slave MIDs.

The payment terminal can be an automated teller machine (ATM) or a Point of Sale (POS) terminal which is optionally connected to a cash register, in particular an Electronic Cash Register (ECR). The above mentioned selection of the transaction order processor and/or the payment system by the payment management system (PMS) can be based here on instructions sent from the cash register (via the payment terminal). In the electronic interface between the payment terminal and the cash register a link can for instance be made to the list of possible application identifiers of the payment terminal. A menu can thus be presented on the cash register of the desired payment methods from which the merchant and consumer may choose.

The information stored on an input carrier, such as (but not limited to) the PAN, can be read in different ways depending on the type of input carrier. When the information is present in a magnetic strip provided on the carrier, this information can be read using a reader (i.e. a magnetic strip reader MSR) specially embodied for this purpose. When an EMV (in accordance with ISO/IEC 7816 standard) or similar chip is arranged on the card, it can be read with a special chip reader. The examples relate to readers for which a lesser or greater extent of contact is required between the card and the reader. In other embodiments the reading can take place in wholly contactless manner. When the input carrier is for instance provided with optical marks such as a bar code, the information can be read via an optical reader, in particular a bar code reader. In other further embodiments the system comprises a wireless receiver for reading a smart card via a wireless connection. A standard for contactless cards is formed for instance by ISO/IEC 14443. Use can for instance be made of a mobile telephone smart card, more particularly an EMV SIM card.

According to further embodiments of the invention the system comprises:

- a first payment terminal adapted to generate an electronic transaction order according to a first protocol which can only be handled by a first transaction order processor;

- a second payment terminal adapted to generate an electronic transaction order according to a second protocol which can only be handled by a second transaction order processor, wherein the second protocol differs from the first protocol;

wherein the payment management system (PMS) is adapted to receive a transaction order according to the first protocol and to have the second transaction order processor (or the first) handle the transaction and/or to receive the transaction order according to the second protocol and to have the first transaction order processor (or the second) handle the transaction.

This means that, irrespective of the type of payment terminal, i.e. irrespective of the protocol employed by the payment terminal, e.g. the protocol for the communication with the outside world, the transaction orders can in principle be processed by a random processor.

According to a further embodiment the payment management system (PMS) comprises a storage medium and the system is adapted to store a transaction certificate (TC) for each of the performed transactions, wherein the transaction certificate comprises merchant-specific identification data concerning the relevant transaction. This merchant-specific information can for instance comprise an invoice reference (number), a specification (text), an order number, an official report and the like. The merchant-specific information can now be linked directly to actually

performed past transactions. In determined embodiments it is made possible for the merchant (for instance via a so-called merchant portal) to log into the payment management system (PMS) and thus gain access to (a part of) the stored data, for instance in the case of an exchange for checking merchant-specific information stored on the storage medium in the form of an invoice. In addition to the merchant-specific information, the stored data can at least comprise one of the following data:

- first transaction data representative of the transaction amount;
- second transaction data representative of the transaction method;
- third transaction data representative of the first identification data;
- fourth transaction data representative of the second identification data;
- the terminal identifier (TID); and/or
- the merchant identifier (MID).

The financial management of the merchant and the monitoring thereof can hereby be greatly simplified. When for instance the TID is stored in combination with a transaction, it is possible at a later stage to collect and to analyse transaction-related details per payment terminal (or per group of payment terminals, for instance a number of payment terminals disposed in a determined shop).

According to another aspect of the invention, a method is provided for handling transactions between at least one merchant and at least one consumer, the method comprising of:

- receiving an electronic transaction order generated by a payment terminal;

- selecting a transaction order processor from a group of transaction order processors on the basis of the transaction order;

- controlling with the selected transaction order processor a payment system for electronic transfer of a transaction amount from the bank account of the consumer to the bank account of the merchant.

Further advantages, features and details of the present invention will be elucidated on the basis of the following description of some embodiments thereof. Reference is made in the following description to the figures, in which:

Figure 2 shows a schematic overview of a first embodiment of a system according to the invention;

Figure 3 shows a more detailed overview of the embodiment of figure 2;

Figure 4 shows schematically the information stored on the storage medium of the payment management system;

Figure 5 shows a schematic overview of a second embodiment of a system according to the invention;

Figure 6 shows a schematic overview of a third embodiment of a system according to the invention;

Figure 7 shows a more detailed diagram of the payment management system according to an embodiment of the invention.

An embodiment of the present invention is shown in figure 2 and, in more detail, in figure 3. Figures 2 and 3 show two payment systems. The first payment system 40 is located in the first region or the first area (R1), while the second payment system 40' is located in the second area (R2). Each of the payment systems comprises a number of servers with which the banks connected to the payment system

can perform their mutual payments. The first payment system 40 comprises a server 6 of an issuer bank, i.e. the bank at which the consumer holds an account, and a server 7 of an acquirer bank, i.e. the bank where the merchant holds his/her account. The servers are mutually linked via one or more communication networks. In practice there will usually be more than two servers, so that payment system 40 is suitable for making payments at each of the banks in the relevant area. The payment systems are connected via respective secure connections 10,11 to a first transaction order processor, also referred to in the field as the processor 18. This processor is adapted to control servers 6,7 of the payment system 11, i.e. to perform the required transactions. Instead of the processor being directly connected to one or more payment terminals as shown in figure 1, according to an embodiment of the invention processor 18 is connected via a secure connection 17 to a payment management system 16. The payment management system is also referred to here as the PMS system, PMS server or simply PMS. The payment management system is embodied such that it can control the above mentioned payment systems to perform a determined transaction. It is noted here that the payment in the payment management system stands for a transaction representing a determined value, of a financial or non-financial nature. Payment management system 16 is further connected with a secure connection 15 to one or more payment terminals 12.

A transaction order processor or processor 21 is provided in usual manner for the purpose of handling transactions in the second area (R2). According to the shown embodiment of the invention however, payment management server 16 is also connected via a secure connection 20 to one or more further transaction order processors, such as

the second transaction order processor or processor 21 shown in the figure.

Second processor 21 is connected in similar manner using secure connections 25, 26 to respective servers of second payment system 40'. Second payment system 40' consists in the shown embodiments of a server of an issuer bank 12 and a corresponding server of an acquirer bank 13, mutually connected via one or more electronic communication networks. It is noted that in other embodiments many more banks are linked to the second processor 21. It will further be apparent that the role played by a determined bank can change. On one occasion a bank forms the issuer bank, since the bank account of the consumer is registered at this bank, on another occasion it forms the acquirer bank because in this case the bank account of the merchant is registered at this bank. It is also possible for both the merchant and the consumer to have their bank account at the same bank.

Further shown in figures 2 and 3 is that second processor 21 can be connected not only to second payment system 40' of the second area (R2) but can also be linked, for instance via a secure connection 27, to one or more banks of first payment system 40 located in the first area (R1).

While in figures 2 and 3 there are two processors 18, 21 which are together connected to a single server of payment management system 16, this number can of course vary in accordance with the number of different processors in the overall area in which the transactions must be realized.

Payment terminal 12 is provided in usual manner with a slot 29 into which a bank card (B) can be inserted such that the magnetic strip or EMV chip © present on the bank card (B) can be read by a reader 30 arranged in terminal 12. Payment terminal 12 is also provided with,

among other components, a keyboard 28 with which the user can enter his/her PIN code and a display 23 on which texts, such as the transaction amount, can be displayed.

In determined embodiments, for instance the embodiment as shown in figure 3, payment terminal 12 is also linked via a connection 14 to a cash register 13, for instance an electronic cash register (ECR). This cash register can for instance send a signal to payment terminal 12 from which the payment terminal 12 can derive the amount to be paid. In other embodiments payment terminal 12 is however embodied as stand-alone device and the amount has to be entered via the keyboard 28 of the terminal 12 itself.

In the configuration phase, in which a number of computer programs 24,24' are loaded and installed onto payment terminals 12,12' from the payment management system or PMS system 16, a connected payment terminal is assigned a unique code from PMS system 16. This code, also referred to as the terminal identifier (TID), is stored on storage medium 31 of PMS system 16 as a master TID 50, as shown in more detail in figure 4, and is used by PMS 16 to identify the relevant payment terminal.

A unique code or identifier can be assigned in similar manner to the merchant associated with payment terminal 12, i.e. for instance the retailer in whose shop the payment terminal is disposed. The assignment of this code is carried out by the acquirer bank with which the merchant has a contract. This identifier, also referred to as the master merchant identifier MID 51, is likewise stored on storage medium 31 of PMS system 16 in the above stated configuration phase.

In the configuration phase the payment terminal 12, more particularly the representative master TID 50, is further linked to one or more corresponding codes (derived

or slave TIDs 52,53) with which the payment terminal is designated by the different processors 18,21. The payment terminal 12 identified using a master TID 50 has for instance a determined unique first terminal identifier TID_A 52,53 (figure 4) for first processor 18 and a determined unique second terminal identifier TID_B 54,55 for second processor 21.

The merchant designated with the master MID 51 can be designated in similar manner with different slave MIDs. The merchant does after all have different contracts at the different banks for the handling of the payment transfers. The merchant can be assigned different MIDs at the banks. Stored on storage medium 31 of PMS server 16 are the master MID 51, the slave MIDs 56-59 and the relations existing between them.

In the shown example the acquiring bank 7 has for instance a contract with the merchant of payment terminal 12 and this merchant has obtained the unique merchant identifier (MID) 56. The same merchant has been given another unique identifier from another bank 13, for instance merchant identifier MID 57. Both identifiers MID 56,57 therefore designate the same merchant, but can relate to different handling protocols. In similar manner the bank 13, which is also connected to second processor 21, can have designated the same merchant with a third merchant identifier MID 58.

Via the table stored on storage medium 31 (figure 4) it is thus possible in each case to find the relation between on the one hand the merchant and/or payment terminal with which the transaction is requested, and on the other the respective processor and/or bank (in particular the acquiring bank) with which the transaction can be performed. In other words, processor 18 can communicate with PMS 16 as

if it were the payment terminal 12 itself. The same applies for second processor 21. Second processor 21 can also communicate with PMS 16 as if it were the payment terminal 12 itself. PMS 16 therefore functions here as a kind of virtual payment terminal arranged between the physical payment terminal 12 and processor 18, 21. Modifications to the hardware and/or software of the processors are in principle therefore not necessary to enable control of the transaction.

When a consumer wishes to carry out a transaction in the user phase (following the above stated configuration phase), he/she places the card (B) into the slot of payment terminal 12. Reader 30 reads a number of data from the card in usual manner. Payment terminal 12 more particularly recognizes that a card has been inserted into the terminal via the Client software running on the payment terminal.

A part of the data read by the payment terminal is formed by the so-called application identifier (AID). Described in the above mentioned ISO/IEC standard 7816 is the process for the selection of the different applications supported by the card. Applications can refer here to wholly differing applications such as GSM and EMV, although an application can also be a product type supported by a determined product issuer (e.g. banks issuing a Visa, Mastercard, etc.). The product issuer of a Visa card may support different applications, such as Visa credit/debit, Visa Electron, V PAY, etc., while the product issuer of a MasterCard card may support the applications credit/debit, Maestro, Cirrus, etc. Each product issuer has in general one or more of its own product types or applications. In order to enable selection of an application use is made of the above mentioned application identifier (AID). An AID consists of a registered application provider identifier

(RID), which is issued by the standardization organization and which designates the relevant product issuer in unique manner, as well as a proprietary application identifier extension (PIX) to enable differentiation in unique manner within the product types or applications supported by the product issuer. The AID thus designates both the product issuer (Visa, MasterCard, etc.) and the associated product type (Visa credit debit, V PAY, Cirrus, etc.).

The Client software running on the payment terminal controls the reader such that the card is read. The reader reads from the card the possible card payment applications (Application ID of the card). This produces a list consisting of one or more possible application IDs for the card. This card application ID list is subsequently compared by the payment terminal to a prestored list on the payment terminal (consisting of one or more IDs) of applications supported by the payment terminal.

If no match is found between the card ApIDs and payment terminal AIDs, a message is sent back via the display of the payment terminal that payment has to be made in another way. In the case of a match the consumer is provided with the option of selecting one of the possible card application IDs (i.e. one of the card ApIDs for which a match has been found). The selected ApID is subsequently incorporated in an electronic payment order, for instance in the form of transaction data, as described in more detail below.

In addition to the application identifier (ApID) defining the product issuer and product type/application, other data is read such as the PAN code. PAN stands for Primary Account Number, i.e. the bank account number of the card holder, more particularly the bank account number of the consumer. Via keyboard 28 and/or via cash register 13

the amount to be paid is subsequently displayed on display 23. The consumer can then give his consent and enter the personal identification code (i.e. the PIN code (PIN)) unique to the consumer.

Payment terminal 12 collects the PAN and PIN codes, encrypts them and sends them, together with transaction data representative of the transaction amount and the transaction data representative of the desired application (the ApID data), to PMS 16.

PMS 16 determines on the basis of the received ApID data designating the desired application (for instance the Visa VPAY application) (and optionally the master TID 50 and master MID 51 already stored in the configuration phase) which of the processors 18,21 should be selected to handle the transaction. A determined processor is for instance adapted to process VISA VPAY transactions, while yet another processor is adapted to process Mastercard credit/debit transactions. The choice of the processor can likewise depend on the area in which the payment terminal is situated (which area can be derived from the TID of the payment terminal stored in the configuration phase, since the area in which the payment terminal is situated is known beforehand) and/or on the issuer bank which must ultimately perform the transaction (which bank can be derived from the PAN data of the consumer).

In a determined exemplary embodiment tables are stored on PMS 16, at least in the electronic storage medium connected thereto, on the basis of which a number of possible methods of payment can be selected in accordance with the ApID data for each payment terminal (i.e. for each master TID 50). When for instance the received ApID data correspond to AID_1, the transaction will be handled by first processor 18 together with issuing bank 6 of payment system

40. The payment terminal has a TID 52 in first processor 18 and the merchant has a MID 56. When the AID data correspond to AID_2, the transaction will be performed by the same processor 18, but the transfer of amounts takes place via one or more other banks, for which the merchant is designated with the unique designation MID_2. When the AID data correspond to AID_3, use is however made of second processor 21 (wherein the payment terminal is designated in unique manner with TID_B) and a further acquirer bank 13 in which the merchant is designated with MID_3. Finally, when the AID data correspond to AID_4, second processor 21 will be used while a bank from the first payment system 11 will perform the actual transaction. The merchant is again characterized here by MID_1 59.

Once processor 18, 21 has been chosen with which the payment is controlled and the acquirers, in particular the acquiring bank 21, 23 have moreover been selected in the above described manner, a transaction order is generated in a so-called protocol adapter 35 of PMS 16 in accordance with the relevant protocol for the associated processor 18, 21 and the associated acquirers. A transaction signal is then sent to the relevant processor 18,21 in accordance with the generated transaction order, which further handles the transaction in the usual manner.

The application ID (ApID, sometimes also abbreviated to AID) received from the payment terminal is more particularly associated with a specific acquiring zone. The acquiring zone is related to a determined processor and to the associated Acquirers (acquiring and issuing banks). Each processor has its own application ApID and several Acquirers, each employing their own MIDs, are active within this environment.

PMS 16 subsequently links the application identifier (ApID) received from the payment terminal to the correct acquirer zone. Found within the linked acquirer zone is the associated acquirer identifier (AID) of the processor associated with the relevant payment method, and the communication with the processor is started for the purpose of handling the payment transaction via the selected payment method.

The processor sends the transaction data over the communication network here to the issuing and acquiring banks relevant for authorization of the PIN associated with a specific PAN and transaction amount, including all transaction data between card and payment terminal. The processor receives a response from the issuer that the authorization of both is accepted and the transaction amount is reserved at the acquirer bank. An authorization code is sent back to the payment terminal and linked to a transaction certificate (TC) which is associated with the relevant payment and is stored as such. This communication between processor 18,21 on the one hand and the issuer and acquirer banks on the other is known in the field under the terms clearing and settlement. The communication can take place online and/or offline.

It is thus possible to ensure in the above described manner, simply by also sending a preference via the AID data, that the merchant him/herself can determine via which route (processor/acquirer) the transaction is handled.

Because PMS server 16 is as it were placed as virtual payment terminal between the physical payment terminal 12 and processors 18, 21, there is also a greater freedom of choice for the merchant in the selection of the desired type of payment terminal. Where according to the

prior art the types of payment terminal to be used were determined by the requirements set by the relevant processor 18, according to embodiments of the invention the PMS 16 can be adapted such that different types of payment terminal (not the type of payment terminal prescribed by the relevant processor) can be used as long as PMS 16 is capable of making the correct translation so as to enable processor 18, 21 to be controlled in the desired manner (as if it were being controlled by a prescribed payment terminal).

Shown for instance in figure 5 is a further embodiment of the invention which largely corresponds to the embodiment shown in fig. 2, but wherein more than one payment terminal is linked to PMS 16. In addition to the above mentioned payment terminal 12 of a first type, in the shown embodiment a second payment terminal 12' is linked of another type differing from the above mentioned type. Because PMS 16 is adapted to make a correct translation of the signals coming from the different types of payment terminal to the format suitable for the relevant processor 18, 21, according to the embodiment of the invention the merchant him/herself can choose the type of payment terminal (12, 12') he/she will use to perform the transactions.

In a further embodiment PMS 16 is adapted to handle not only financial transactions but also non-financial transactions, for instance transactions related to loyalty cards, bonus cards, etc. In these embodiments contact is made with PMS 16 by payment terminal 12. On the basis of the provided PAN codes, after a possible authentication step, PMS 16 can store information about the relevant consumer on storage medium 31 of PMS 16. This information can for instance comprise loyalty information, for instance data received from the cash register system which are representative of the articles purchased by the

consumer. This loyalty information can for instance be used to give discount on possible further financial transactions.

In determined embodiments use is made by the system of only the PAN data (and not also the PIN data). The PAN data can be stored on the magnetic strip of the electronic input carrier. On the basis of the PAN data (and so without requiring a PIN code) the card can be recognized via BIN from the CST (Card System Table) as being a loyalty card. In consultation with an acquirer bank a determined card range can even be reserved for loyalty purposes. The card data can subsequently be sent directly to the loyalty host and processed and, if desired or supported, linked to the financial transaction and the associated transaction amount. Value points can in this way be saved or redeemed with the loyalty card. The loyalty host keeps track of the conversion rate and the balance total. Using this solution the retailer is able to influence the behaviour of the consumer. For instance 200 points if the consumer opts to pay with a first application (for instance Maestro) and only 50 points for paying with a second application (for instance with Visa or MasterCard credit cards).

In the embodiments of figures 2-5 discussed up to this point the payment terminal 12, 12' is coupled electronically to PMS server 16 via a wire connection. Communication connection 15 between payment terminal 12 and PMS server 16 forms a secure connection according to a predetermined protocol, for instance the transport layer security (TLS) or the secure socket layer (SSL) cryptographic protocol, so that secure data communication is realized over the electronic communication connection (in particular the internet). Further described up to this point is that the input carrier is a payment card, loyalty card or the like, wherein the data representative of the client,

such as the PAN code, are stored on a magnetic strip or on a microchip (for instance an EMV chip). These cards can be read by placing the relevant card in a slot of the payment terminal or guiding it along a slot. There must in any case be some contact between the card and the payment terminal. In other embodiments however, the input carrier (card) can be read, for instance by detecting a bar code provided on the card by means of an optical bar code reader or by making use of an electromagnetic sensor for reading a resonance circuit (for instance an RFID tag or the like). In yet another embodiment use can be made of NFC technology, which is provided for instance on a mobile platform, such as a mobile phone, PDA or the like. An EMV functionality can for instance be arranged in the SIM card of the mobile phone so that reading the SIM card, or at least a part thereof, can be seen as a reading of the EMV chip used which is provided on a payment card.

Figure 6 shows an example of performing a financial transaction remotely using a mobile platform. Shown in the figure is a PMS server 60 which is connected in known manner via a secure data connection 61 to a payment terminal 62. PMS server 60 is further linked in the above described manner to one or more processors 65,66 which in turn control one or more transaction systems (acquirers) 67-70. Further shown is a mobile phone 71 which establishes a wireless connection 73 to payment terminal 62 using an NFC transmitter/receiver. Because the smart card (SIM card) provided in the mobile phone is provided with EMV functionality, it is possible to have the mobile phone 71 function as a payment terminal. In similar manner as described above, payment terminal 62 reads the mobile phone (payment card) and here collects inter alia the PIN code

unique to the consumer and the PAN code representative of the bank account of the user.

In order to provide extra security, mobile phone 71 makes contact via a wireless network transmitter/receiver 75 with the mobile network (for instance a GSM network, 3G network, etc.) and establishes an internet connection 77 with PMS server 60. When the internet connection is made between phone 71 and PMS server 60, PMS server 60 can determine the mobile phone number (M) of the phone 71 (with a standard number recognition technique). This mobile telephone number (M) can subsequently be compared to a list 80 of prestored mobile phone numbers (M_1-M_n). Mobile phone numbers can be stored on PMS server 60 or, as in the shown embodiment, on a separate storage medium 82. The list of telephone numbers 80 originates from the mobile network operator (MNO) managing the network with which the internet connection has been made. PMS 60 can for this purpose be directly connected to a server 85 of the mobile network operator (MNO). In addition to the check of the PIN and PAN code via processor 65,66 and the payment systems of the bank, an additional check can thus be performed by comparing the telephone number of the consumer with a list of prestored telephone numbers of the mobile network operator (MNO). When the telephone number of the mobile phone is not stored in the list 80 for the storage medium 82, in a determined embodiment the PMS can conclude that the transaction is not allowed to take place. In another embodiment the PMS 60 will however decide that a transaction is allowed to take place, but that this transaction has a higher risk profile. Depending on the size of the amount and possible other parameters, it is then possible for instance to decide to allow the transaction to continue, but at relatively high costs.

A more detailed description of the specific embodiment for handling transactions is given hereinbelow.

Table 1 gives an explanation of different components of the transaction system according to an embodiment of the invention. Reference is made in the table to figure 7 in which a more detailed diagram of the PMS system is shown.

Table 1

16	Payment management system PMS: the central software core on the central host system which has control over the payment logic and controls the hardware
12	Input hardware device: the input hardware which comprises the readers (readers for smart card, magnetic strips, NFC, RFID, bar code) which can read the required input data. The input hardware has to comply with the general requirements of the Payments Card Industry (PCI) standards: PCI PTS (PIN Transaction Security devices = PTS). This means that the hardware must be secured in order to secure the input data.
13	Electronic Cash Register (ECR): the interface of the ECT system of the merchant which also provides data input to the PMS system. The ECR interface has the option of linking a unique merchant identifier to the transaction data.
40	Acquirer hosts: the host systems of the processors. The processor controls the processing of clearing and settlement files between the acquiring banks and the issuing banks. In other words they provide for the mechanism in which the transaction amount to be paid by the consumer at the POS in the shop of the merchant is transferred in electronic manner from the bank account

	of the consumer to the bank account of the merchant.
1	Consumer: the person starting the electronic transaction at the POS (including e.g. a physical payment terminal or a webshop or the like) in order to obtain goods or services in exchange for money or for a value transfer accepted in similar manner.
	Merchant is for instance the retailer (organization or person) accepting electronic payments in the virtual and/or physical shop(s)

013	Terminal Management System: the TMS (terminal management system) subsystem provides for the remote configurations and secure software and firmware downloads of the input hardware. The Client profiles (behaviour of the input hardware on the input products: how for instance does the payment terminal deal with the EMV payment cards that are used, risk management) are exported from the PMS to the TMS system and subsequently configured for the specific type of input hardware.
014	Key Management System: The Key Management System (KMS) controls all keys in the PMS. The KMS is used to create, store, import, export, store and use as back-up the keys of the POS terminals, OMS, TMS, third-party systems and the like in secure manner.

021	DeMultiplexer: The (De)Multiplexer has the task of routing messages as follows: • route TMS messages from the TMS to the correct LW-POS; • route TMS messages from the LW-POS to the TMS; • route PMS messages from the LW-POS to the correct POS instance; • route PMS messages from the POS instance to the correct LW-POS. To enable the (De)Multiplexer setup the TLS-based secure tunnels with the LW-POS terminals, the keys in the HSM are used.
022	HSM: The Keys are always located in a secure environment. This secure environment is implemented using a Hardware Secure Module (HSM). Such a HSM is a "Common Off The Shelf" (COTS) device specifically designed as a secure container for keys. The HSM is able to wrap/encrypt keys using a Loading Key. This mechanism is used to back up all the wrapped keys in the database. A group of key custodians will be used to create a paper backup of the Loading Key for the HSM. In the case the HSM of the key manager breaks down, the key custodians are able to fill a new HSM with the loading key. The new HSM is then able to load all the wrapped keys from the database. Operations such as creating or destroying keys, are handled by Security Officers. All the actions performed by the KMS are logged into an audit trail that is stored in the database. This audit trail makes sure that the KMS can be audited by external parties to ensure that the Security Officers and Key Custodians have carried out no illegitimate actions.

023	POS instances: as mentioned above, the architecture aims at offloading complexity from the LW-POS or input hardware device to the PMS. The LW-POS communicates with a counterpart in the PMS referred to as the POS instances or virtual POS terminal. Every connected LW-POS has its own POS instance. The POS instance contains most of the payment flow and generates the content of host messages that are sent to the acquirer host via the protocol adaptor during a transaction.
024	Protocol adaptor: the protocol adaptor formats the host message in the correct format for the intended acquirer and adds the security to these messages (MAC, encryption, etc). The ability to switch between protocol adaptors enables switching between acquirers.
025	POS manager: the POS Manager manages all the POS instances in the PMS and connects them to the correct protocol adapter. It keeps a POS profile with third party trusted relations when an LW-POS is connected and disables them when an LW-POS is disconnected. The POS Manager also serves a role as overall guard. It will not allow unknown LW-POS instances to connect.
026	System log: the System Log module stores all the log information produced by other modules in the PMS, in the database. This information can be used for analysis and debugging of the PMS system.
027	Database: all LW-POS or input hardware Client and POS profiles with configuration and trusted relation parameters (who is the merchant of the LW-POS, who services it, what cards can it accept, etc.) and all transaction results are stored in the database. The data in the database is used for the various reporting functions (Merchant reporting, Service Provider reporting and System reporting).

028	Merchant reporting: the configuration can be seen by the merchant. It also provides usage data per device and location. See 008.
029	Service Provider reporting: this is the location where a service provider can configure the input hardware and ECR devices. It can also provide usage statistics for preventive maintenance. See 009.
030	Acquirer reporting: The acquirer can generate usage statistics. See 010.
031	System service: The Service console can be used to manage the configurations of the LW-POS terminals attached and other system settings.
032	PMS Operator: see 005

According to embodiments of the invention a method and system is provided for realizing freedom of choice in a flexible manner in the secure relations an electronic transaction system maintains with third parties. The electronic transactions processed via the system comprise data representing a specific value of a financial or non-financial nature. In the operational environment this value is accepted by all users as a valid electronic means of payment. Value is transferred in electronic manner from the one user to the other. At the beginning of the system the identity of the user is determined on the basis of a unique physical carrier and a unique code linked to this carrier. Linked to these two entities is a transaction amount which is exchanged with a third party which validates and approves the transfer of the value. In order to prevent fraud and manipulation the electronic transaction is handled wholly within a secure environment. For this purpose the physical data of the carrier and the associated unique code are basically secured immediately at input, including the

associated electronic value. The validation and the authorization of the value transfer via an encrypted and secure relation with a third party is subsequently realized and this results in a successful transfer. This all starts in a hardware input environment which is specifically designed for this purpose and complies with the international guidelines, standards and specifications (PCI PTS, EMV level 1 and 2, and SEPA FAST volume 1). In the classic traditional setup only one on one secure relations are possible between the input hardware and the relevant third party, wherein the third party imposes and determines the secure relation.

Some of the described embodiments make it possible to enter simultaneously into a plurality of secure relations with third parties, thus enabling the end user to make a choice from the diverse parties. In this case the input hardware determines with the security software with whom it maintains a secure relation by realizing the secure relations with the third parties from the input hardware. An important distinction is that the secure relation is reversed 180 degrees and is now set up from the end user with the associated preferred parties, and no longer the other way around.

The system enabling the freedom of choice comprises in determined embodiments a central secure software bus which has a number of specific branches for handling specific tasks. The front end software operating on the input hardware provides for the secure input, storage, output and communication. The central software likewise provides for the secure input, storage, output and communication. The difference here is that the central part fully controls and checks the front end. The principle of the Client-Server technology is applied for this purpose.

Immediately following input of a card (payment card, credit card, etc.) and of the PIN and PAN data the relevant data is encrypted via the Client software running on the payment terminal and thereby made inaccessible to the outside world. The encrypted data are then sent in tunnelled manner (via a secure connection) to the secure memory part of the payment management system (PMS). The PMS forwards these data (in a protocol selected from a list of possible protocols) in an authentication request via a secure connection to the selected transaction order processor. This processor subsequently performs a check (authentication), for instance on the authenticity of the card and on the PIN code. As supplement to this check the payment terminal can also perform a first check. In determined embodiments the authenticity of a card is checked in the first instance by the Client on the payment terminal. A PIN code can for instance be checked in an offline mode with the encrypted PIN on the card itself, and be directly validated and checked in an online mode by the card issuer (i.e. the transaction order processor) which has issued the relevant card. In both modes the PMS always submits an authentication request (also referred to as authorization request) to the card issuer(s). The identification data such as the PAN and PIN data are not saved or stored by the payment management system. The secrets of the card and associated PIN validation remain in the domain of the card issuers.

Further details of embodiments of the invention are discussed further in enclosure I.

The present invention is not limited to the embodiments thereof described herein. The rights sought are defined by the following claims, within the scope of which numerous adjustments and modifications can be envisaged.

ENCLOSURE 1:

The tables below provide a further overview of the application of the principle of freedom of action within the above stated framework.

100	Web service ensures that, from a management viewpoint, all users gain access to the controlled subsystems and data. For each type of user a separate application is started so that a physical separation is realized between the different domains. Each type of user assigns his/her own user management and access rights at application level and data level. The Administrator of the Payment Management System, the central software is at the top of the hierarchy and, via the local system on a local network, has access to all subsystems and user domains.
101	This is the PMS Administrator console, a local PC in the local network, which is in direct secure connection with the PMS system which takes a redundant form and is located and operates in a hosted, secure environment. Via the console and the web service the Administrator also has access to the input hardware at different locations in specific environments and countries. In this description we use the example of the payment terminal as hardware input device for the handling, validation, authorization and verification of both financial and non-financial electronic transactions in the cash register environment.
102	The configuration process starts with the Administrator logging into the PMS system via the console. Following validation the Administrator gains access to the PMS and specific subsystems.

103	Visualization of the PMS system and the associated subsystems necessary to create and realize the Freedom or Choice, the secure relations with the desired third parties.
103 A	Subsystem POS instances and POS profiles manager: this subsystem creates the virtual payment terminals, instances, on the PMS system and links the Profiles of the Acquirer Zones to the terminals. For a single instance or payment terminal a profile can consist of several Acquirer Zones. An Acquirer zone virtualizes a single secure relation comprising a specific route for the processing and the supported electronic payment products valid for this route. An Acquirer Zone has its own unique identifiers: TID terminal identifier, uniquely linked to a payment terminal and MID merchant identifier representing a payment product which is supported. A TID can have several MIDs.
103 B	Subsystem KMS + HSM security manager: this subsystem provides for the security of the overall PMS system. From this system the security certificates are issued and the security keys realized and distributed. The keys and certificates ensure that secure relations can be entered into and implemented between the physical input hardware and virtual payment terminal on the one hand and between the virtual payment terminal and the relevant third parties on the other. Two core security systems can be distinguished, the one, a security module, is particularly concerned with the securing and encryption of the data of the unique identifier of the user, the so-called PIN (personal identification number), and in combination with the associated unique carrier in the form of a PAN (personal account number) and of course the associated electronic transaction

	amount. This encrypted data in the form of a PIN Block is formed on the input hardware via the specific security software of the hardware, and subsequently undergoes in the PMS security module a translation for the purpose of establishing a secure relation with a third party. The second module provides for the certificates and keys for the secure connections between the systems mutually and all external connections, as well as the loading of keys and certificates on the physical input hardware environments. The combined security modules also ensure that the PAN is already stored at application level in masked form within the relevant transaction data (and/or in combination with other sensitive transaction data). In the case of theft of the databases this prevents the data files being read, even with a correct viewer.
103 C	Subsystem Configuration and Client profiles manager: this subsystem provides a behaviour profile for the input hardware of how to deal with the diverse input means and how to handle these via the security software and open software of the relevant hardware. Applicable for the payment terminal is for instance how the PIN is presented in the dialogue between user and input hardware, as well as that for security reasons an on-line PIN and authorization is always enforced. Also envisage here however a selection list of payment products with a preferred selection of a payment product from which the user can choose. In addition to the configuration of the Client this data is prepared for input via the TMS (terminal management system) into the input hardware. The profile also comprises the software versions which are realized the

	first time via personalisation of the input hardware and, once operational, can be maintained securely and remotely via the TMS. From a Client profile a physical link is subsequently made to a POS instance and associated POS profile.
103 D	Subsystem Payment or Transaction device manager: this subsystem ensures that a physical input hardware is linked to a Client, POS instance and POS profile. Subsequently generated from the PMS via the KMS+HSM subsystem is a unique master TID linked to a master MID, both of which are linked to a Master key with which the Slave keys are generated for the associated relations with the third parties which have been created from the POS profile.
104	Administrator follows the login procedure via the GUI on the console and opts for the setup procedure TID (freedom of choice menu). Steps which now follow describe only the manner in which the freedom of choice is realized using the diverse subsystems. At the end of the procedure there must be an operationally active payment terminal in the field which can process secure transactions via the diverse established secure relations with third parties for the purpose of processing the electronic transactions.
105	From the login procedure for the freedom of choice a connection is made with subsystems for starting the different sub-processes, being preparation of the Master TID list as well as the Client list, POS instance and profile list, and user name (USN) and password (PW) are checked in parallel. In addition to USN and PW the Administrator will first gain access to the console and the associated data structures via a unique card and finger scan.

	Preparation for access to the Master TID lists and later storage and saving of the performed actions.
106	Preparation for access to the Client profile lists and later storage and saving of the performed actions.
107	Preparation for access to the POS instances and profile lists and later storage and saving of the performed actions.
108	Preparation for access to PMS system wherein a check is first made via the console of the Administrator on the basis of unique card and finger scan. All login procedures are provided with a date time stamp.
109	Start login procedure for USN and PW. Start date and time stamp procedure for access to the diverse data structures of the different subsystems.
110	Universal secure communication between the client console and the PMS with the diverse subsystems.
111	User management service ensures that on the basis of USN and PW a user profile is activated for access to the PMS system, with access to the diverse data structures of the different subsystems. Important here in addition to the date time stamp is the service per user which serves the purpose of logging which data have been accessed and subsequently which data structures have been modified or changed.
112	Login process result keeps track of whether the login has been successful and keeps track of the number of login attempts and whether the date procedure must start to run and provides for interim data storage of and for the log file.
113	Login procedure has not been successful, the procedure is then repeated up to a maximum number of attempts (adjustable). When the maximum number has been exceeded, a timer function ensures that the procedure

	may be repeated, starting from 108, only after an x number of minutes.
114	From the TID process the Administrator can create and/or check Master TIDs with associated Master Merchant IDs, activate and/or deactivate, change and delete them. Only TIDs which have been created on the system and come from the creation list can be set up and used for deployment.
115	TID seeding process ensures that Master TIDs are created on the PMS system. Master TID is later linked uniquely to an input hardware device. In this specific case the physical payment terminal at the Merchant location.
116	TID seeding process result produces a list with Master TIDs which can be set up and activated via the PMS. This list is stored within the relevant subsystem of the PMS. Master TIDs always remain saved, even if they have been deleted.
117	Master TIDs are then known, and the Administrator can then begin to prepare a new Master TID for activation on the PMS system. If a Master TID is not known from the active list, the procedure is repeated. If a selected Master TID remains unrecognised the procedure will be discontinued after timer interval and restarted. Administrator will have to select a new Master TID. If successful, it is possible to start the following step, the assigning of a Client profile.
118	On a subsystem an overview of all Master TIDs is maintained via a black and white list system. Via the Master TID list it is possible to check whether a physical payment terminal at the Merchant location is allowed to start or perform electronic transactions.

	An example is the case where a physical payment terminal, in the case of a malfunction which cannot be remedied remotely, is replaced on site by a new physical payment terminal. The new physical payment terminal may then be activated only after the old terminal has been returned. Another example is when a physical payment terminal which cannot maintain an online connection with the PMS is temporarily deactivated and, when connected, can only be reactivated using the service provider interface.
118 A	Subsystem which tracks the status of the Master TIDs and responds via pre-programmed settings and can temporarily deactivate or render the Master TIDs inoperative. Via the Master TID the same is done for the diverse Acquirer zones, wherein a request may also come from the Acquirer zone for a TID to deactivate a Master TID. There will be interaction with the different third parties.
119	Start of the Client profile process wherein, on the basis of a Master Merchant ID, a configuration is determined for the Client, the physical payment terminal on the counter in the shop. This configuration file must then be made ready for use by the TMS system.
120	Master TID associated with the profile must be stored.
121	KMS + HSM ensures that the Client profile data are stored in secure manner.
122	Client profile for the merchant ensures that determined preferences in behaviour are prepared in the form of configuration parameters for use by the TMS. That the specific Client Profile is then stored properly on the relevant subsystem. Administrator can make use of created standard profiles and

	configurations.
123	POS instance, virtual payment terminal which has to be linked to the Client profile must be stored.
124	Client profile must also be linked to the physical input hardware and stored.
125	Start Client Profile process wherein a profile for a Master Merchant can be started. Note that a profile for the physical payment terminal at shop level can be determined per region and per country. A single Client profile can be used for several Master TIDs.
126	Client and configuration process involves a form completion task wherein a table is compiled and made ready for further processing via the TMS system to the hardware input device.
127	Client profile process result is a list which can be stored on the relevant subsystem and produces a file which can be read by TMS and linked to unique hardware ID of the input hardware.
128	If the result of Client profile process is not successful, previous process steps can be repeated. Timer indicates that, if repeat steps are not performed correctly within x minutes, profile process must be restarted.
129	Start Payment / Transaction device process, within this process a choice is made for the input hardware linked to the created Client Profile.
130	The hardware service ensures that a relation is established between the unique ID of the hardware and the Client profile. All hardware of the different suppliers has a unique hardware ID. During manufacture and transport lists are provided and the hardware provided with transport keys. The manufacturing process must comply with TQM process wherein assembly

	process is secured. The purpose is that, upon arrival of the hardware at SEPASoft, the integrity of the hardware can be determined and no tampering has occurred. It is the case here for the payment terminal that the production process is monitored and that tamper-responsive measures are taken which come into effect in the case of unauthorized use. Measures include: opening the payment terminal, drilling holes in the payment terminal etc. In all cases the secure memory must be immediately deleted and this must be shown in the display when power is supplied to the hardware. A list of available hardware IDs will be available from the TMS for the PMS, and vice versa.
131	Hardware selection result is that a physical hardware ID can be linked to a specific Client profile with associated Master Merchant ID. Result is then stored for further use.
132	If Hardware selection is not successful, a new process will be started. If it is not possible to select hardware ID the procedure will be discontinued after an x number of attempts, and restarted with a different physical hardware ID. Variation will then be logged.
133	Start Master key management process. Within this process a Master key is generated from the KMS + HMS subsystem. Using this unique Master key all the necessary derived keys can be determined that are required for the purpose of facilitating secure relations with third parties. For the payment terminal and the PIN encryption DUKPT is used for the key management.
133	

A	
134	
135	Master Key management process result is that, on the basis of a Master key structure, the Administrator can create, assign, activate, change and store different Acquirer zones.
136	Master key successful has two results. Firstly, if Administrator is unable to make a Master Key profile, an x number of attempts to make a profile are in this case allowed. If this is not realized within the x attempts, the current process will be discontinued and restarted with a different profile. If making of a Master key profile has been successful, the following process step can be started.
137	Start POS instances and profiles process. Within this process the virtual payment terminals are set up (POS instances) and the associated POS profiles comprising the derived Slave relations with the third parties said Acquirer zones are determined and set up.
138	Processor list (AID) or Acquirer zones: a list of third processing parties will have to be set up. These are, in the example of the payment terminal, the parties which ultimately handle the transactions via a clearing and settlement mechanism with the issuing and accepting banks / financial institutions of the relevant payment product. The PMS system supports both an online and file-oriented mechanism. This list must then be maintained: it must be possible to add, modify or remove Acquirer zones. The processing parties each have their own specific ID on the basis of an AID characteristic.
139	Acquirer list: a list of acquirers, banks will have to be set up which are fixed behind a determined secure

	processing relation and transaction route. The end user, in the case of the payment terminal the Retailer, will enter into the Merchant contract with an Acquirer / Bank for acceptance of electronic payment in the cash register environment for a specific payment product. This list must then be maintained: it must be possible to add, modify or remove Acquirers / Banks. It must similarly be possible to track / modify the list of payment products associated with a specific acquirer / bank. Each acquirer has their own specific ID on the basis of slave TIDs and MIDs.
140	TID list: a list of Master TIDs will be set up which are associated with specific input hardware. It must then be possible to link these Master TIDs to the POS instances and associated POS profiles. The result of linking different profiles will be stored.
141	Merchant list: an associated Merchant list will also be set up from the Master TID list. For the payment terminal this is the list of the retailers or retail merchants. The result of linking different profiles will be stored.
142	Client profiles list: a Client profile list will be set up from a previous process. From this list a profile can specifically be made for a Master Merchant with associated POS instance and POS profile. The result of linking different profiles will be stored.
143	Start POS profile process: within this process the third or derived relations with the third parties are determined: the processing parties and acquirers / banks with the associated payment products. The POS profiles can then be linked to the list of virtual

	payment terminals and the POS instances. The outcome is a list of Acquirer zones with the payment products linked here per Acquirer / bank. The separate derived TIDs and MIDs are known per Acquirer zone. The POS profiles and POS instances are now also linked: POS instance = POS profile (Acquirer zones n+1 = TID n+1 + (m+1) MIDs). See example below for the payment terminal: AID TID MID Merchant Omnipay EMS Mastercardx Visa x PaySquare Maestro x Visa PayPass x
144	POS profile service: the service ensures that the POS profiles can be created and are maintained.
145	POS profile result: result is a POS profile which can be linked to virtual payment terminals, the POS instances, and this profile can be drawn up, maintained and stored.
146	POS profile successful: if not successful and no profile can be made, the session is repeated x times. The service is then discontinued and restarted. If successful, the following process can then be started.
147	Start Slave Key management process: within this process the derived keys are determined on the basis of the BDK, the Master key determined per Acquirer zone.
148	Derived key management service: service (automated process) runs via KMS + HMS subsystem which provides for generation of derived keys on the basis of the BDK for a Acquirer zone.
149	Derived key management result is that the

	Administrator can create, maintain and store the POS instances and POS profile lists.
150	Hardware device process result: has the result that the physical input hardware devices are set up within the TMS system and PMS system.
150 A	The TMS (terminal management system) subsystem provides for the remote configurations and secure software and firmware downloads of the input hardware. The Client profiles (behaviour of the input hardware on the input products: how in our example does the payment terminal deal with the EMV payment cards that are used, risk management) are exported from the PMS to the TMS system and subsequently configured for the specific type of input hardware.
151	Slave key management successful: if not successful, the procedure is then repeated x times. After the final attempt the procedure is discontinued and restarted. If the process has been successful, the profile(s) of the derived keys can be stored and saved within the secure memory environment of the HSMs. The result is that a Master key of an Aquirer zone is linked to a number of IPEK with which the derived keys are determined for the derived TIDs and MIDs.
152	TMS configuration result: the outcome of this process is that the Client profile can be exported from the PMS system to the TMS. TMS system then links the configuration file to a specific input hardware device.
153	Start payment transaction device key loading process: within this process all lists and keys which are linked in a logical manner to each other are made ready for use within the operational environment. The Master Merchant ID and Master TID form the highest

	order in the tree structure, followed by that of the derived Acquirer zones with their own TIDs and MIDs.
153 A	Key loading device subsystem: this system (hardware + software) ensures that the Master and Slave keys are made ready in a controlled secure manner for loading of the keys into the input hardware. These keys ensure that a hardware input device in combination with the associated POS instance (the virtual payment terminal) on the PMS can together (operating as central software bus from the PMS with the different subsystems) maintain a secure relation with determined Acquirer zones.
154	Master TID list: this is the list of Master TIDs and Master Merchant IDs set up/compiled in an earlier process (114). The process tree is now assembled in combination with the derived relations: keys and profiles. Specific lists are now placed within the tree for further processing within the operational environment. Tree structures are stored.
155	Master + Slave key lists: this is the list of Master Keys and Slave Keys set up/compiled in an earlier process (133+147). Specific keys are now placed within the tree for further processing within the operational environment. Tree structures are stored.
156	Client profile lists: this the list of Client profiles set up/compiled in an earlier process (125). Specific lists are now placed within the tree for further processing within the operational environment. Tree structures are stored.
157	POS profile + POS instances lists: this is the list of POS profiles and POS instances set up/compiled in an earlier process (137). Specific lists are now placed within the tree for further processing within the

	operational environment. Tree structures are stored.
158	Start payment transaction device personalisation process: within this process the payment terminals (physical + virtual) are made customer-specific.
158 A	See 153A + 150A + 133A for the system descriptions of the input for this subsystem.
159	Personalisation service: within this service the lists and keys are linked to and made specific for the operational use with an end customer at a specific location. For the payment terminal the shop location and configuration of the behaviour of the terminal with the relations which must maintain the terminal with the third parties and the payment products offered per party via the terminal.
160	Personalisation process result: result of the service is the different profiles and keys being made customer-specific.
161	Personalisation successful: if not successful, the process is repeated x times. At the last attempt the process is discontinued after x minutes and restarted. If successful, the payment terminal (physical + virtual) is then made specific for an end customer as unit within the PMS system and prepared for operational use. Administrator can start the following process.
162	Start secure device preparation process: all lists and keys are converted and distributed to the correct subsystems for activation on the operational system.
162 A	TMS system: Client profile is converted to a configuration file for the relevant hardware input device.
162 B	PMS system: POS profile and POS instance profile are linked to the correct Client profile.

163	TID list: this is the Master TID and Merchant list which are made specific for the end customer per shop location and per country.
164	TMS list: list of Client profiles sent as configuration file to the correct input hardware devices.
165	PMS list: list of POS instances and profiles linked to the correct Client profiles.
166	Device list: list of input hardware devices to which the correct Configuration files are linked.
167	Software list: list of open and security software applications which must be loaded to the correct input hardware devices.
168	Start secure device keys + software loading process: within this process the correct keys and software applications are loaded to the hardware input devices. This loading process takes place wholly within a secure space in accordance with the security procedures drawn up for this loading process.
168 A	Key loading system: subsystem of the PMS which injects the keys into the input hardware devices. Described above in process (153 A).
169	Software + keyload+testing service: automated service which makes it possible under software control to load the software and keys to the input hardware devices via a loading facility. A test procedure then also takes place which checks whether the correct software versions have been loaded, and the hardware can start up.
170	Software+keys+testing result: result of the service is that the correct keys and software are loaded to the input hardware with the associated POS instance (virtual payment terminal) coupling.

171	Software+keys+testing successful: if not successful, the procedure will be repeated x times and at the final attempt be discontinued within x minutes and restarted. In this case the software will first have to be removed in order to be able to continue and in worst case, the keys procedure will also have to be restarted. If successful, the physical payment terminals are then ready to be sent to the customer or service provider which provides the physical installation at the shop location.
172	Start device deployment proces: within this process the customer-specific aspects for delivery process are activated in terms of issue and receipt procedures.
172 A	TMS + PMS systems: within the operational systems the customer domain is provided with the necessary Master TIDs and Merchant IDs.
173	Deployment service: service which shows that a batch of input hardware devices has been sent to the customer, optionally via the service provider providing for the installation. Customer or Service provider must confirm receipt. Following on from this service is the procedure for acceptance of the payment terminals and the delivery to the shops.
174	Deployment result: result of the service is a batch delivery of the payment terminals accepted by the customer.
175	Deployment process successful: if not successful during transport, then direct blocking of payment terminals on PMS system. If not successful during acceptance process customer, return physical payment terminals and replace with new payment terminals or, worst case, completely new batch. If successful, the Administrator can then start with the installation

	procedure.
176	Start device installation process: in this process the payment terminals are installed within the shop environment. The two pairs of eyes rule is applied for this process. An FSE (field service engineer) can only install and configure. The help-desk observes remotely and can activate the physical payment terminal and associated POS instance on the PMS system.
176 A	TMS+PMS systems: on both systems the physical and virtual payment terminal is now activated for operational use.
177	Install service: the service makes it possible to install and link the physical payment terminal to the virtual payment terminal and subsequently activate the whole via the help-desk. A test transaction carried out by the FSE, having as result a copy of a transaction receipt, must show that the end-to-end solution works and is operational.
178	Install result: result of the service is that the physical and virtual payment terminal are set up and activated on the system and become operational via a test transaction.
179	Install process successful: if not successful, the FSE can look at whether this is due to the physical payment terminal, and remedy the malfunction via configuration and software updates or modification. If not successful on the virtual payment terminal side, the help-desk can look at whether this is due to the POS profile and or the POS instance. The help-desk can look at whether these malfunctions can be remedied remotely. Install process is discontinued if PMS cannot reach the physical payment terminal. If successful, the payment terminal is then wholly ready

	for operational use.
180	Start device transaction process: in this process the whole payment terminal is active in the operational mode. Different transaction types are performed and handled daily via the payment terminal.
180 A	TMS+PMS systems: within these systems the first transaction results are now processed and stored with the diverse Acquirer zones. A specific clearing and settlement procedure can be employed per Acquirer zone. It is important that from the PMS system forced online PIN verification and authorization are in the first instance always used. After approval of the PIN and authorization, the transaction data can then be sent batchwise/filewise or directly to the Acquirer zone.
181	Transaction service: the service shows that active transactions are in progress over the whole payment terminal.
182	Transaction result: result of the service is that transactions are stored within the PMS system. Transaction Certificates and Authorization Codes per payment terminal of a customer are saved per book entry period, wherein the PAN data is always stored in masked manner within the PMS.
183	Transaction process successful: if not successful, the cashier will once again ask the customer via the application selection table how he/she wishes to pay, wherein the retail customer can express a determined preference for the payment method of the consumer. Selection can be repeated until a payment product can complete a transaction. If not the case, the customer can abort the transaction. When successful, the customer receives a copy receipt of the payment

	transaction. The PAN will be shown in masked form on copy receipt of both the customer and the merchant. The receipt shows which payment product has been used and which acquirer zone has been used.
184	Start device operational process: with the above operation the FOC process for the payment terminal has entered the operational mode. Changes to profiles and configurations can now be realized via the different service portals. Depending on the type of service which must be provided, another service provider will be used.
184 A	TMS+PMS system: systems are adapted such that each logical user has their own portal has for access to the system. Customer is starting point and indicates who the Service provider is and which contracts are associated with which Aquirer zones. Each portal has its own specific function geared to the role assigned in respect of the payment terminal via the portal.
184 B	Service Provider Portal: via this portal remote service can be provided at the physical payment terminals. The Health status ensures that preventive action can be taken, since this system keeps track of how many card inserts have been realized, whether a payment terminal does or does not maintain a permanent connection with PMS, whether Cash register coupling link is active etc etc. Service provider can hereby act more quickly and more efficiently on behalf of the customer in the field of service. Service provider, provided it is trained, can itself manage and maintain the profiles and configurations of the customer domain on behalf of the end customer.
184 C	Merchant Portal: via this portal the merchant can keep track per book entry period of his/her turnover per

	shop, region, country, countries. He/she can also update his/her own MSC (merchant service charge) table, wherein he/she can display transaction costs. On the other side the Merchant administrator portal makes it possible to make electronic repayments for transactions performed previously within the shop environment with the physical payment terminal.
184 D	Acquirer Portal: via this portal the Acquirer, the processing party, can see how their installed base of physical payment terminals behave. PMS system will measure and keep track of the host to host transaction times in order to see how the PIN and Authorization response times are behaving. Acquirer also gains access to the Transaction Certificates and Authorization codes if transactions are nevertheless rejected during clearing and settlement by the issuing or accepting banks.
184 E	Administrator Portal: via this portal SEPASoft can make changes within all portals and supervise the end-to-end system.
185	Operational process service: within this service the customer comes with a change or malfunction on the payment terminal. On behalf of the customer the service provider maintains the configurations and profiles for the customer domain and can remedy the malfunction independently using the PMS system.
186	Operational process result: result of the service is that a modification, change is made as a consequence of a malfunction or customer request and stored within the customer domain.
187	Operational process successful: if not successful and Service provider cannot remedy the change or malfunction independently, the help-desk of SEPASoft

	is called in and the malfunction or change is remedied or made in accordance with SLA. If successful, the payment terminal returns to its operational mode.
188	End Freedom or Choice (FOC) process: result of this process is that the end customer has obtained the freedom of choice in the processing parties and the banks he/she wishes to use for the acceptance of electronic payment within his/her environment. The solution provides both at the front and back end a freedom of choice in which a secure solution is provided end-to-end, wherein the integrity of the transaction data remains guaranteed from the moment of data input, processing and storage.

CLAIMS

1. Assembly for handling transactions between at least one merchant and at least one consumer, the assembly comprising:

- at least one payment terminal for generating and sending an electronic transaction order;

- a payment system for electronic transfer of a transaction amount from the bank account of the consumer to the bank account of the merchant;

- a transaction order processor connected to the payment system for electronic clearing and settlement of the transaction amount associated with the transaction order, wherein the transaction order processor is adapted to receive and process an electronic transaction order and to control the payment system for transfer of the transaction amount associated with the transaction order generated by the payment terminal;

wherein the assembly comprises a group of transaction order processors, wherein each of the transaction order processors is connected to a payment system and wherein a payment management system (PMS) is arranged between the payment terminal and the transaction order processors which is adapted to select one transaction order processor from the group of transaction order processors and to control the associated payment system with the selected transaction order processor.

2. Assembly as claimed in claim 1, comprising a number of payment systems, wherein the payment management system (PMS) is adapted to select one of the payment systems, to optionally select one of the payment systems and to select

one of the transaction order processors linked to the selected payment system.

3. Assembly as claimed in claim 1 or 2, wherein the payment terminal is adapted to generate and send information concerning the transaction order processor to be selected and/or concerning the payment system to be selected, wherein the payment management system (PMS) is adapted to perform the selection of the transaction order processor on the basis of the information received, wherein the information preferably comprises the product type.

4. Assembly as claimed in any of the foregoing claims, wherein the payment terminal comprises:

- a read unit for reading first identification data, which are stored on an electronic input carrier and which are representative of the bank account of the consumer;
- an input unit for entry by the consumer of second identification data representative of the identity of the consumer.

5. Assembly as claimed in any of the foregoing claims, wherein the input carrier is a payment card, more particularly a debit card or a credit card, a loyalty card or an EMV or a SIM unit.

6. Assembly as claimed in claim 5, wherein the electronic transaction order comprises:

- first transaction data representative of the transaction amount;
- second transaction data representative of the transaction method;

- third transaction data representative of the first identification data;

- fourth transaction data representative of the second identification data.

7. Assembly as claimed in any of the claims 4-6, wherein the first identification data are formed by data representative of the bank account number of the consumer, particularly in the form of the primary account number (PAN).

8. Assembly as claimed in any of the claims 4-7, wherein the second identification data are formed by data representative of the identity of the consumer, particularly in the form of a personal identification number (PIN).

9. Assembly as claimed in any of the foregoing claims, wherein the transaction order processor is adapted to perform authentication of the received transaction order, in particular of the first and second transaction data, and is preferably also adapted to send an authentication signal to the payment management system.

10. Assembly as claimed in claim 9, wherein the payment terminal is adapted to perform an additional authentication, in particular of the first and second transaction data, and is preferably also adapted to send an authentication signal to the payment management system.

11. Assembly as claimed in any of the foregoing claims, wherein the payment management system is linked via one or more communication connections to two or more transaction order processors.

12. Assembly as claimed in any of the foregoing claims, wherein a payment system comprises:

- an issuer bank subsystem which manages the bank account of the consumer; and
- an acquirer bank subsystem which manages the bank account of the merchant;

wherein a transaction order processor is adapted to control both subsystems for the purpose of transferring an amount of money from the issuer bank subsystem to the acquirer bank subsystem.

13. System as claimed in any of the foregoing claims, wherein the payment management system (PMS) comprises a storage medium, on which is stored at least:

- unique master terminal identifiers (TID) which are representative of the payment terminals linked to the payment management system (PMS); and/or
- unique master merchant identifiers (MID) which are representative of the merchant associated with each of the payment terminals linked to the payment management system (PMS).

14. System as claimed in any of the foregoing claims, wherein the payment management system (PMS) comprises a storage medium, on which is stored at least:

- a number of unique slave terminal identifiers per unique master TID, each of the slave terminal identifiers being associated with a different transaction order processor.

15. System as claimed in claim 13 or 14, wherein there is also stored on the storage medium:

- a number of unique slave merchant identifiers (slave MIDs) per unique master merchant identifier (master MID), each of the slave merchant identifiers being associated with a different payment system.

16. System as claimed in any of the claims 13-15, wherein the payment management system (PMS) is adapted to select a slave TID from the list of slave TIDs and/or to select a slave MID from the list of slave MIDs.

17. System as claimed in any of the foregoing claims, wherein the payment terminal is linked to a cash register, in particular an Electronic Cash Register (ECR) of the merchant and wherein the selection of the transaction order processor and/or the payment system by the payment management system (PMS) is based on instructions sent from the cash register.

18. System as claimed in any of the foregoing claims, wherein the payment terminal is adapted to encrypt at least one of the first, second, third and fourth transaction data.

19. System as claimed in claims 9, 10 and 18, embodied to send the first, second, third and fourth transaction data encrypted and via a secure connection from and to the payment management system and to perform the authentication of the transaction order by the transaction order processor, optionally in combination with the payment terminal.

20. System as claimed in any of the foregoing claims, wherein the payment terminal is a Point of Sale (POS) terminal.

21. System as claimed in any of the foregoing claims, comprising a magnetic strip reader (MSR) and/or a chip reader for reading respectively a magnetic strip and/or chip, in particular an EMV chip, of a payment card and/or loyalty card.

22. System as claimed in any of the claims 1-20, comprising a wireless receiver for reading a smart card via a wireless connection, in particular a mobile telephone smart card, more particularly an EMV SIM card.

23. System as claimed in any of the foregoing claims, wherein the payment management system (PMS) is adapted to form a virtual payment terminal.

24. System as claimed in any of the foregoing claims, comprising:

- a first payment terminal adapted to generate an electronic transaction order according to a first protocol which can only be handled by a first transaction order processor;

- a second payment terminal adapted to generate an electronic transaction order according to a second protocol which can only be handled by a second transaction order processor, wherein the second protocol differs from the first protocol;

wherein the payment management system (PMS) is adapted to receive a transaction order according to the first protocol and to have the second transaction order processor handle the transaction and/or to receive the transaction order according to the second protocol and to have the first transaction order processor handle the transaction.

25. System as claimed in any of the foregoing claims, comprising of:

- storing on a storage medium of the payment management system (PMS) a transaction certificate (TC) for each of the performed transactions, wherein the transaction certificate comprises merchant-specific identification data concerning the relevant transaction and also comprises at least one of the following data:

- first transaction data representative of the transaction amount;

- second transaction data representative of the transaction method;

- third transaction data representative of the first identification data;

- fourth transaction data representative of the second identification data;

- the terminal identifier (TID);

- the merchant identifier (MID).

26. System as claimed in claim 25, comprising a communication unit (merchant portal) linked to the storage medium for providing external access to one or more of the transaction certificates (TCs).

27. Method for handling transactions between at least one merchant and at least one consumer, the method comprising of:

- receiving an electronic transaction order generated by a payment terminal;

- selecting a transaction order processor from a group of transaction order processors on the basis of the transaction order;

- controlling with the selected transaction order processor a payment system for electronic transfer of a transaction amount from the bank account of the consumer to the bank account of the merchant.

28. Method as claimed in claim 27, comprising of selecting a payment system from a group of payment systems which are connected to the selected transaction order processor.

29. Method as claimed in claim 27 or 28, comprising of receiving information from a payment terminal concerning the transaction order processor to be selected and/or concerning the payment system to be selected, and performing the selection of the transaction order processor and/or the payment system on the basis of this received information.

30. Method as claimed in any of the claims 27-29, comprising:

- reading first identification data representative of the bank account of the consumer from an input carrier using a read unit;

- receiving with a keyboard second identification data representative of the identity of the consumer.

31. Method as claimed in claim 30, comprising of:

- receiving first transaction data representative of the transaction amount;

- receiving second transaction data representative of the transaction method;

- receiving third transaction data representative of the first identification data;

- receiving fourth transaction data representative of the second identification data.

32. Method as claimed in any of the claims 27-31, wherein the system according to any of the claims 1-26 is applied.

33. Payment management system as defined in any of the claims 1-26.

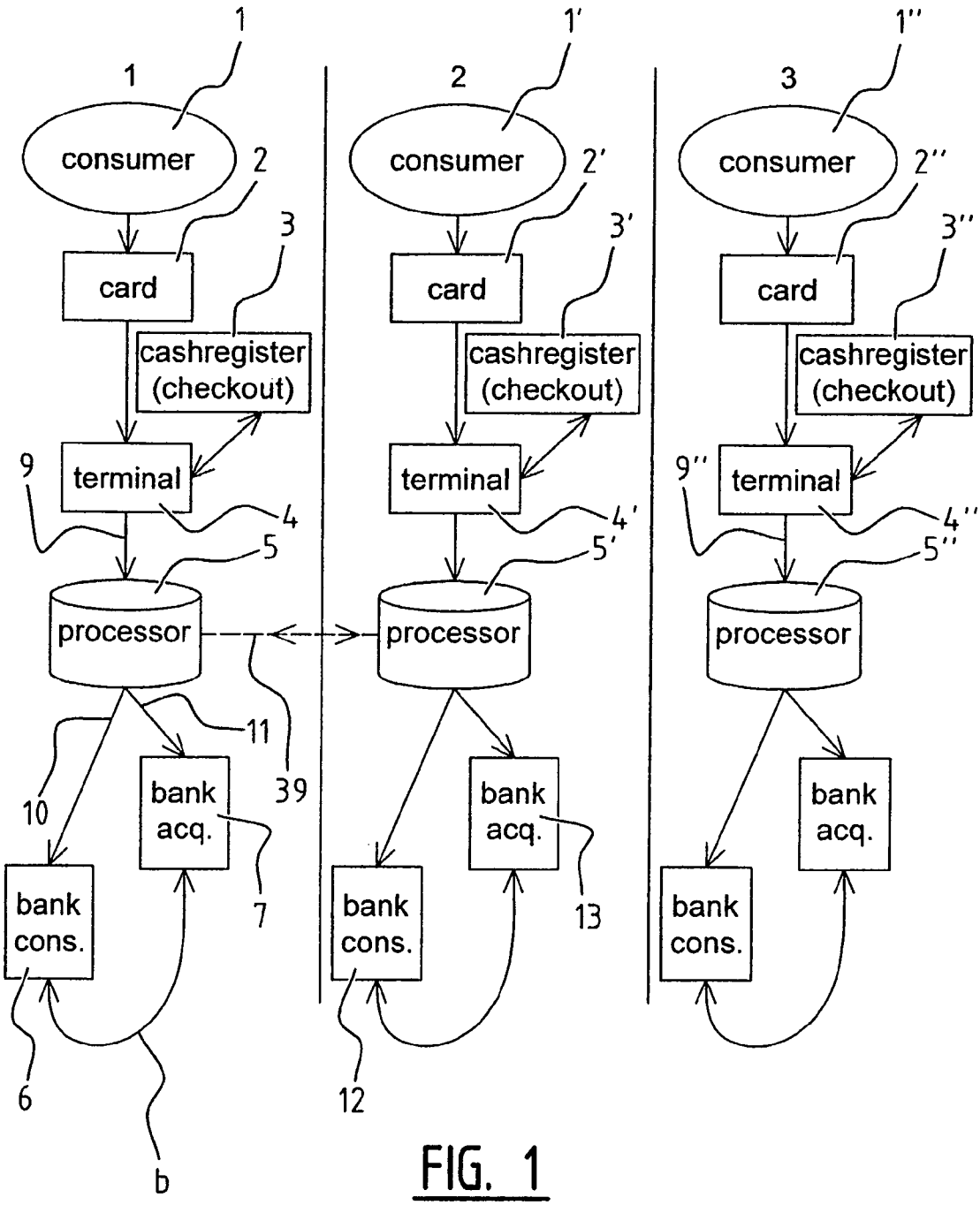

1
1
consumer
2
card
3
cashregister
(checkout)
9
terminal
4
5
processor
11
10
39
bank
acq.
7
bank
cons.
6
b
1'
2
consumer
2'
3'
card
cashregister
(checkout)
terminal
4'
5'
processor
bank
acq.
13
bank
cons.
12
1''
3
consumer
2''
3''
card
cashregister
(checkout)
9''
terminal
4''
5''
processor
bank
acq.
bank
cons.

FIG. 1

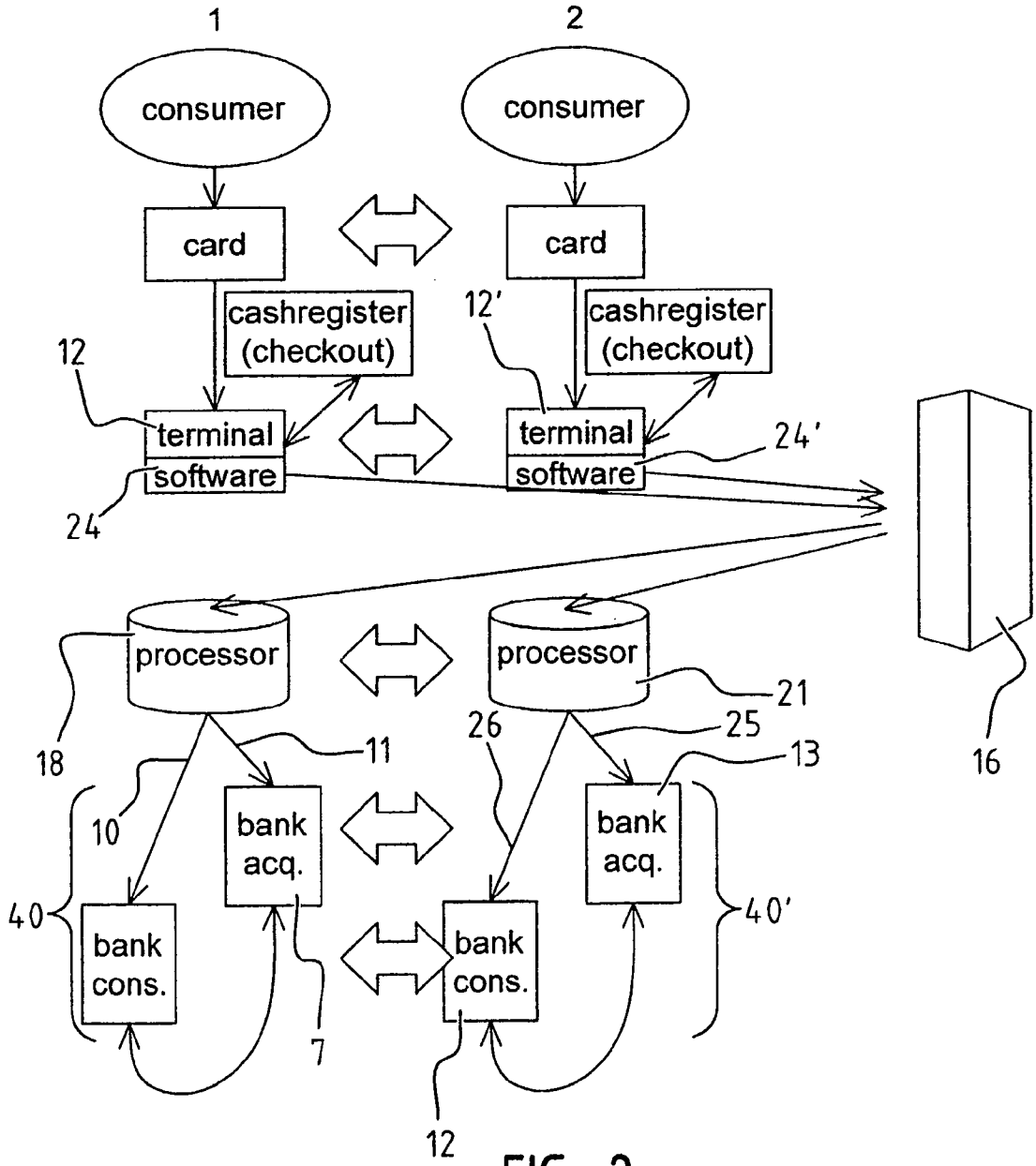

1
2
consumer
consumer
card
card
cashregister (checkout)
cashregister (checkout)
12
12'
terminal
software
terminal
software
24
24'
processor
processor
18
21
11
26
25
13
16
10
bank acq.
bank acq.
40
40'
bank cons.
bank cons.
7
12

FIG. 2

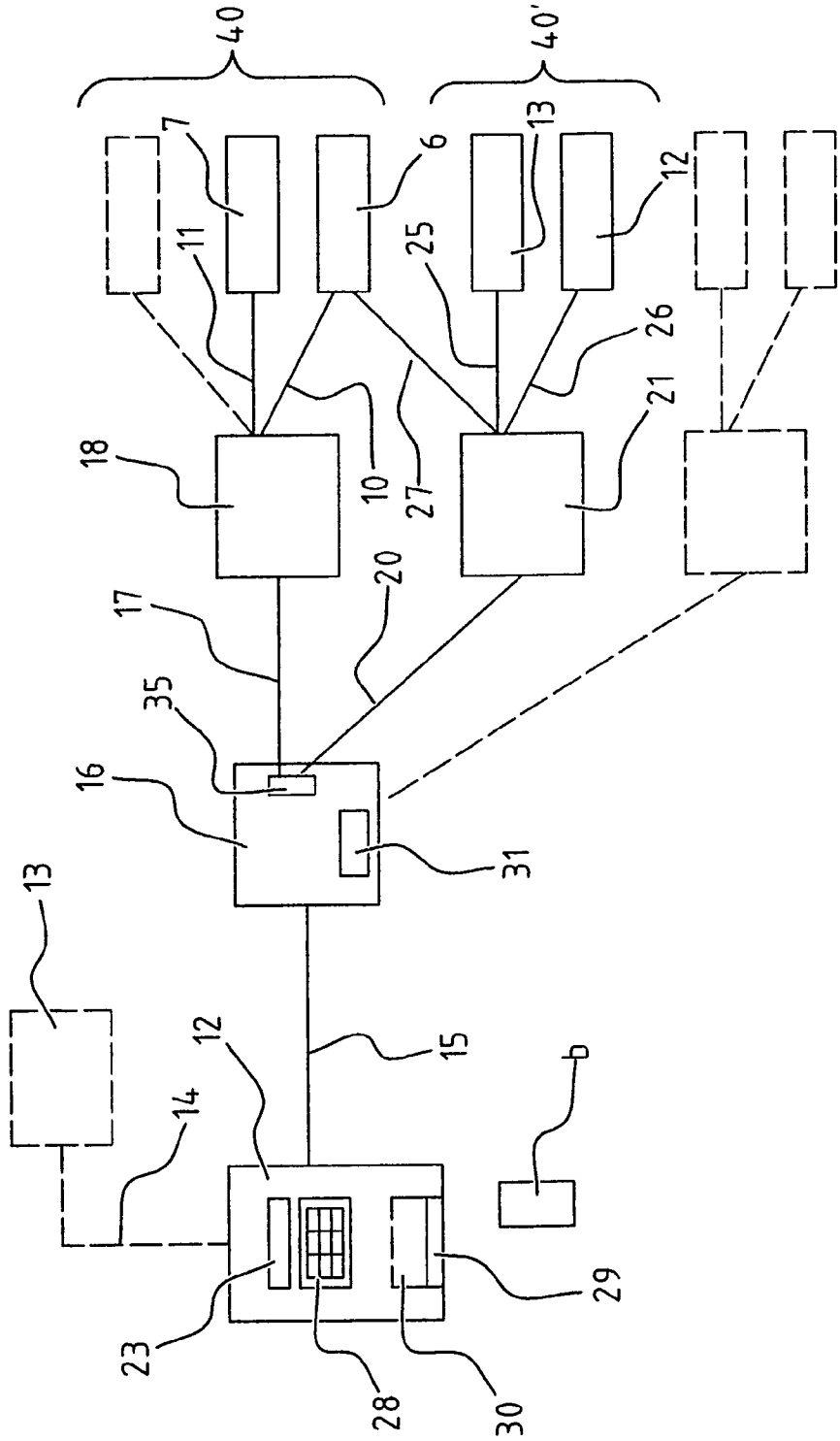

40
40'
7
6
13
12
11
25
26
10
27
21
18
20
17
35
16
31
13
12
15
14
b
29
23
28
30

FIG. 3

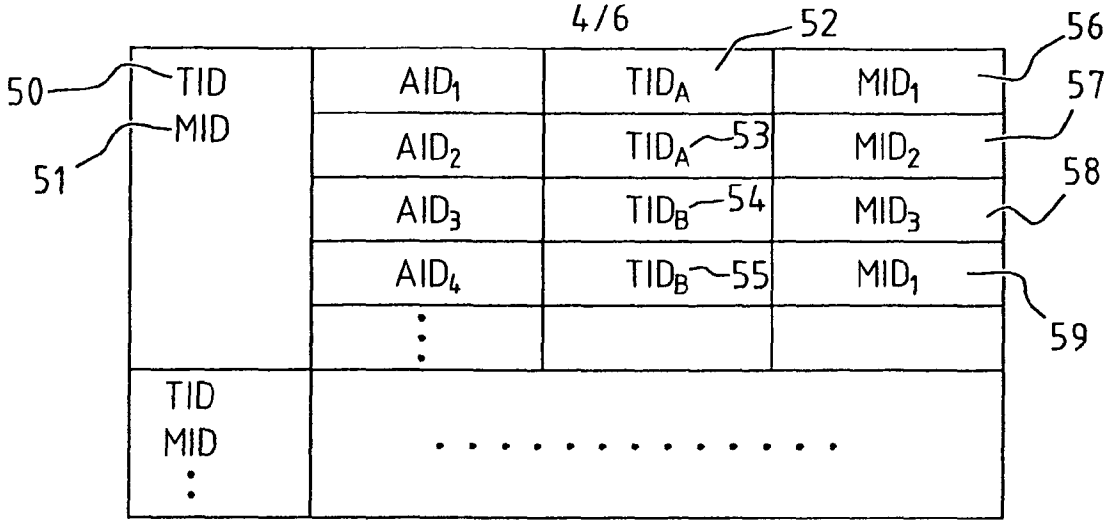

50
TID
MID
51
AID1
AID2
AID3
AID4
TIDA
TIDA
TIDB
TIDB
MID1
MID2
MID3
MID1
52
53
54
55
56
57
58
59
TID
MID

FIG. 4

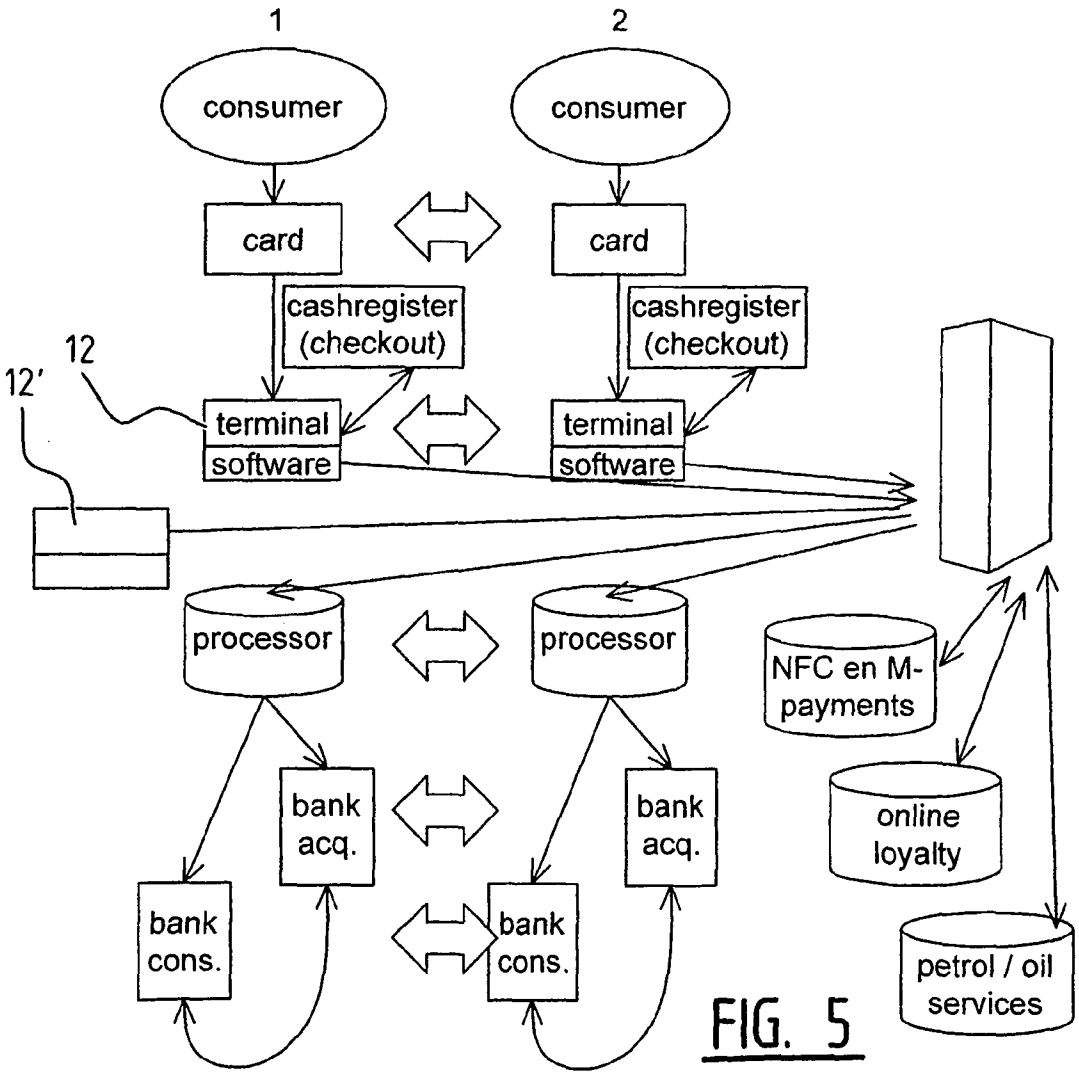

1
2
consumer
consumer
card
card
cashregister (checkout)
cashregister (checkout)
12
12'
terminal software
terminal software
processor
processor
bank acq.
bank acq.
bank cons.
bank cons.
NFC en M-payments
online loyalty
petrol / oil services

FIG. 5

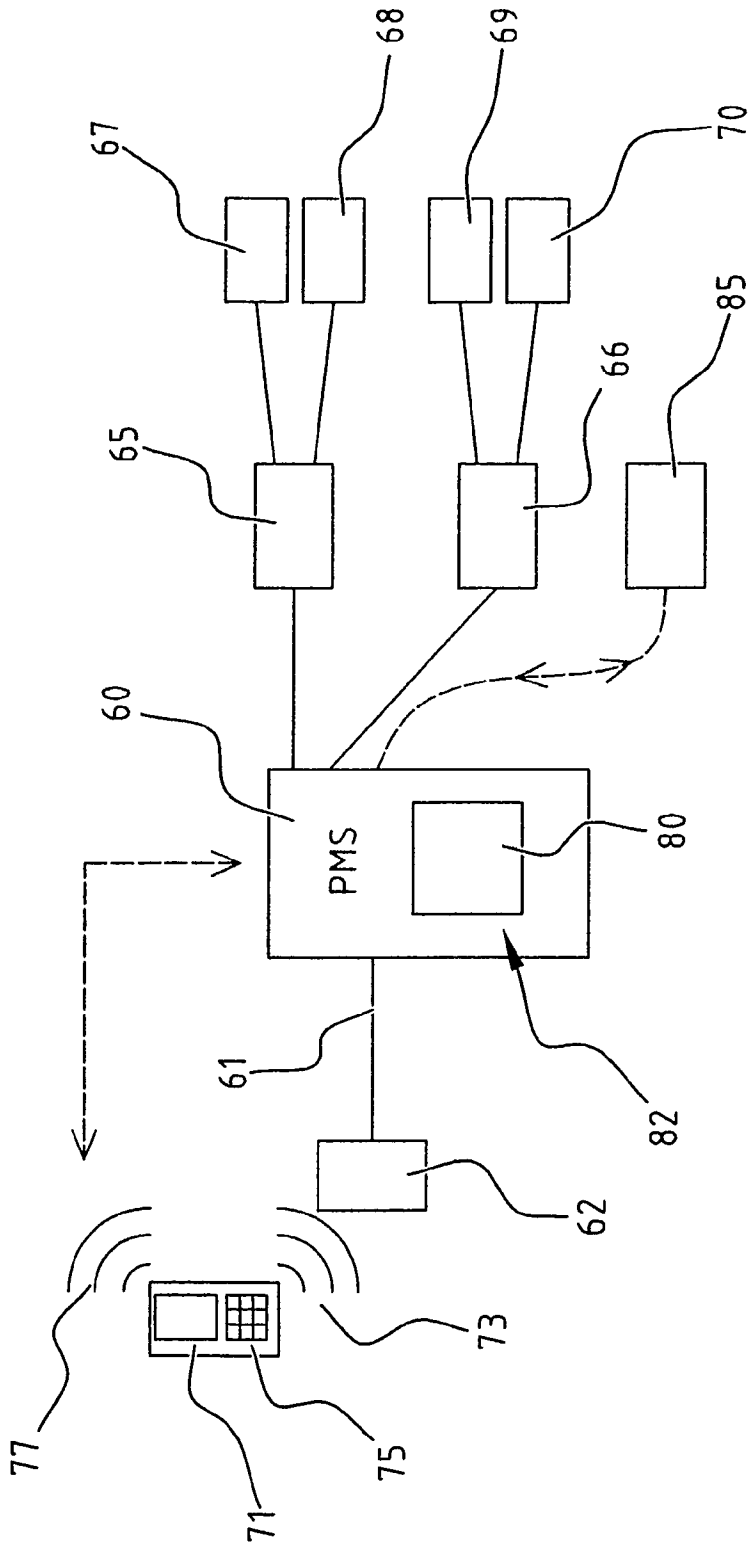


FIG. 6

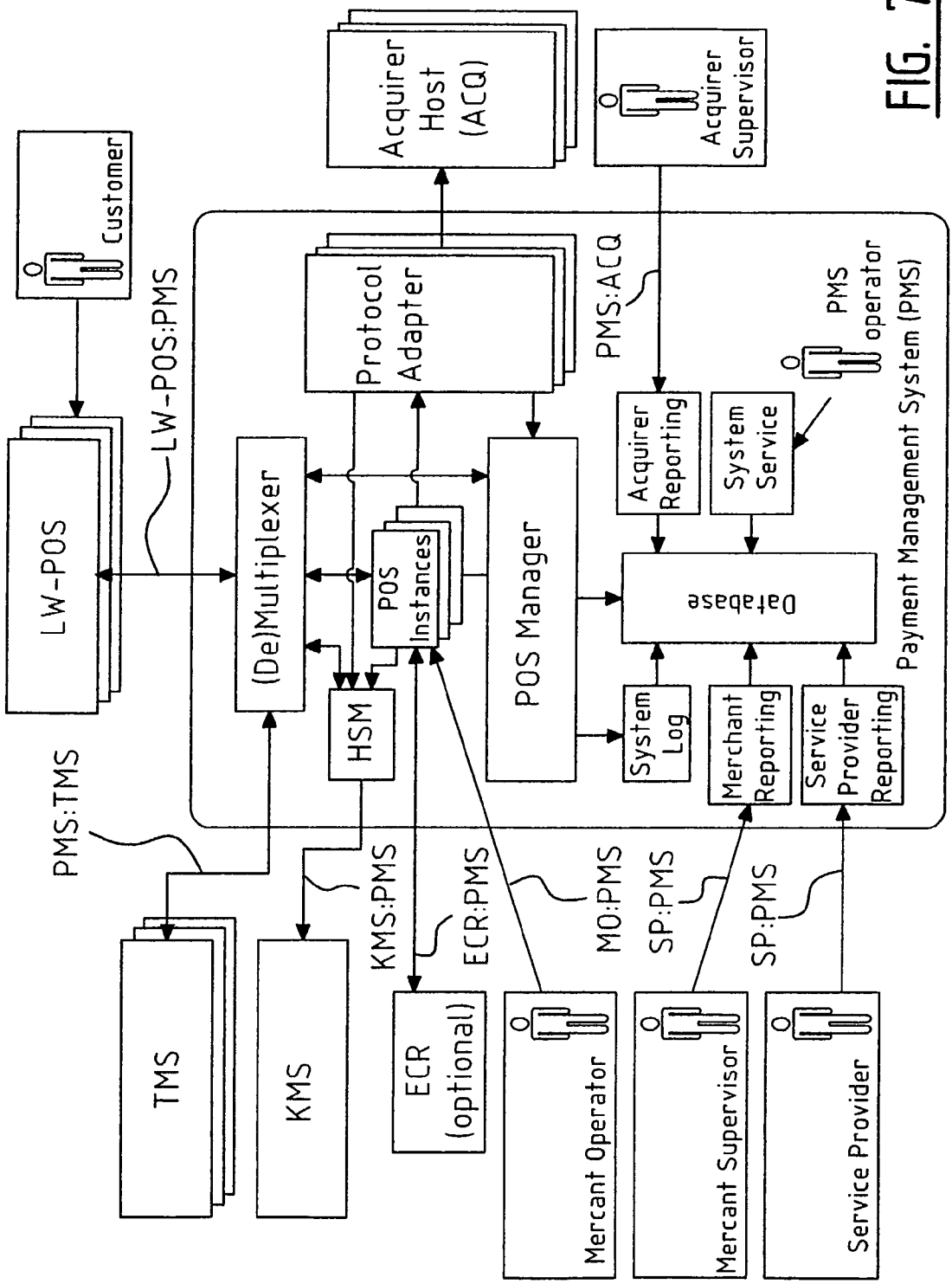

Customer
LW-POS
LW-POS:PMS
Acquirer Host (ACQ)
Acquirer Supervisor
Protocol Adapter
PMS:ACQ
PMS operator
Payment Management System (PMS)
(De)Multiplexer
POS Instances
POS Manager
Acquirer Reporting
System Service
Database
HSM
System Log
Merchant Reporting
Service Provider Reporting
PMS:TMS
KMS:PMS
ECR:PMS
M0:PMS
SP:PMS
SP:PMS
TMS
KMS
ECR (optional)
Mercant Operator
Mercant Supervisor
Service Provider

FIG. 7

INTERNATIONAL SEARCH REPORT

International application No
PCT/NL2012/050248

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q30/00 G06Q20/00 G06Q20/16
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)
G06Q

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 2004/030647 A1 (HANSEN KURT L [US] ET AL) 12 February 2004 (2004-02-12) the whole document	1-32
X	WO 02/079939 A2 (FIRST DATA CORP [US]) 10 October 2002 (2002-10-10) the whole document	1-32
A	WO 2008/117212 A1 (IVERI PAYMENT TECHNOLOGIES PRO [ZA]; COETZEE BAREND BARTHOLOMEUS JOUBE) 2 October 2008 (2008-10-02) abstract figure 1 page 8	1-32

-/--

[X] Further documents are listed in the continuation of Box C.

[X] 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
18 May 2012	01/06/2012

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Kemény, Michael

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/NL2012/050248

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2005/015336 A1 (YEATES ANTHONY JAMES [US] ET AL) 20 January 2005 (2005-01-20) paragraph [0004] paragraph [0049] - paragraph [0050]	9,10,18, 19
Y	WO 02/101512 A2 (PAYTRONIX SYSTEMS INC [US]; D ARBELOFF MATTHEW A [US]; ROBBINS ANDREW) 19 December 2002 (2002-12-19) page 8, line 18 - line 31	9,10,18, 19

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/NL2012/050248

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004030647 A1	12-02-2004	US 2004030647 A1	12-02-2004
		US 2006277146 A1	07-12-2006
WO 02079939 A2	10-10-2002	CA 2443220 A1	10-10-2002
		US 2002169719 A1	14-11-2002
		US 2002178025 A1	28-11-2002
		US 2007022049 A1	25-01-2007
		WO 02079939 A2	10-10-2002
WO 2008117212 A1	02-10-2008	NONE	
US 2005015336 A1	20-01-2005	US 2005015336 A1	20-01-2005
		US 2011078083 A1	31-03-2011
WO 02101512 A2	19-12-2002	AU 2002315133 A1	23-12-2002
		WO 02101512 A2	19-12-2002