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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 January 2009 (29.01.2009)

PCT

(10) International Publication Number
WO 2009/014502 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/SI2008/000043

(22) International Filing Date: 21 July 2008 (21.07.2008)

(25) Filing Language: Slovenian

(26) Publication Language: English

(30) Priority Data:
P-200700188 23 July 2007 (23.07.2007) SI

(71) Applicant *(for all designated States except US)*: **Halcom d.d.** [SI/SI]; Trzaska 118, 1000 Ljubljana (SI).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **KOMELJ, Andrej** [SI/SI]; Na Gulc 13, Vnanje Gorice, 1351 Brezovica Pri Ljubljani (SI). **CADEZ, Matjaz** [SI/SI]; Kosovelje 34, 6221 Dutovlje (SI). **KUHAR, Peter** [SI/SI]; Oresje nad Sevnico, 8290 Sevnica (SI). **SEGA, Marko** [SI/SI]; Trubarjeva 45, 1000 Ljubljana (SI).

(74) Agent: **PIPAN, Marjan**; Kotnikova 5, 1000 Ljubljana (SI).

(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, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

(54) **Title:** METHOD AND SYSTEM FOR SAFETY AND SIMPLE PAYING WITH MOBILE TERMINAL

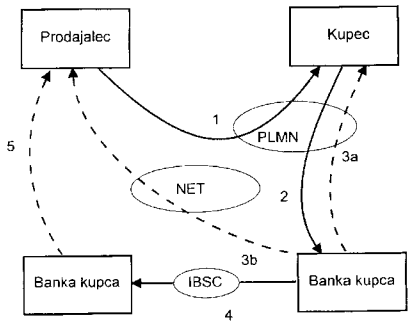

FIG. 1

(57) **Abstract:** The subject of the invention is a system for safe and simple payment with a mobile terminal that enables the user (of even completely ordinary) mobile phone or similar mobile terminal that can receive and send standardized messages (SMS, MMS, USSD and similar) to authorize and carry out a credit payment to the provider of goods or services The subject of the invention enables simple payment with a mobile terminal, whose realisation enables the carry out of the process, where the salesman sends (step 1) to the buyer (payer) an extract of the original bill (m-bill), which includes at least the bill of approval and the total amount of payment, or also some other data, like the date of the currency and the purpose so that the buyer recognizes the payment easily, on his mobile phone The buyer then digitally signs the pertaining payment warrant with his private key that is stored on the smart SIM card and sends the signed payment warrant (m-payment) to the offer of the payment services where his account is open This account is stated in the payment warrant (step 2) After the implementation of the payment the offer of the payment services (usually it's the bank) sends a certificate to the buyer (step 3a) and to the salesman (step 3b), it sends a certificate that the transaction has been carried out.

WO 2009/014502 A2

METHOD AND SYSTEM FOR SAFE AND SIMPLE PAYMENT WITH MOBILE TERMINAL

The subject of the invention is a method and system for safe and simple payment with mobile terminal enabling a mobile terminal user (usually mobile phone user), who can receive and send standardized messages (such as SMS, MMS, USSD and similar), which will hereinafter be referred to as short messages, to authorize credit payment to a goods or services provider via the mobile terminal. The invention falls within the G 06 F 17/60 Class of international patent classification. Systems for safe and simple remote payment, which in order to keep confidentiality, integrity and authenticity of a payment order for money transfer from the payer's account opened at a payment service provider (usually a bank), which will hereinafter be referred to as bank account, to the recipient's bank account, uses the Public Key Infrastructure (PKI), where the buyer (payer) has his private key stored without a possibility of alienation on the SIM (Subscriber Identification Module) smart card of his mobile terminal, and communication between the buyer and the payment system is performed via the Public Land Mobile Network (PLMN) by means of exchanging short messages.

Technical problem satisfactorily solved by the presented method and system for safe and simple payment with mobile terminal under this invention is represented by the installation and realization of such

payment system for the implementation of payments with mobile terminal which enables a buyer to realize simple and safe payment for goods and services directly from his bank account without using other payment instruments (such as payment cards).

There exist relatively many solutions for payment with mobile terminal. Most solutions use the mobile terminal only as a channel for authorization of payments with payment cards, such as for example under the patent document US2003069792A1 and under the patent document US2003171993A1 and are thus intended primarily to conduct payments for online purchases. Such solutions do not enable (remote) payment directly from the buyer's account opened at a payment service provider, and require (at least an indirect) use of other means of payment (e.g. payment cards) and/or the use of the Internet to realize a payment. A version of the solution for payments of purchases via the Internet without using a payment card is described in the patent document WO2006128215A1. The solution is limited only to online shopping, and its disadvantage is also a quite complicated use of technology, which is not supported by all mobile terminals (java technology).

Another group of solutions for payment with mobile terminal is focused on payments for loading a prepaid account which subsequently serves for payment of mobile phoning services. Such payment mode can be used to a limited extent (for the so-called micro-payments) also to pay goods and services of other sellers or providers apart from the mobile operator,

particularly due to limited funds on a user's prepaid account and relatively low safety standards for the realization of payment. Such is, for example, the "paybox TopUp Mobiliser" solution of the Company paybox.net AG.

Furthermore, there are also solutions (such as the M-Pay solution or the solution under the patent document EP 1 777 972 A1) where a buyer approves payment to a provider of goods or services via the mobile terminal, and the sum is credited by the mobile operator until the user has paid the subscriber's invoice to the mobile operator for the services of mobile phoning. Since the operator takes the risk of non-payment in the case of such solutions, this group of mobile payments is intended solely for payments of small sums of money.

There is also a solution under the patent document WO03107288A1, which anticipates payment to be settled directly from a user's account opened at a payment service provider and which is not intended solely for payment of online purchases. The described solution is deficient, as a user must enter a range of data himself. Besides, identification and authorization can be abused, as they are based on call number (CLIP) and the entry of PIN number only.

The subject of the invention is a system for safe and simple payment with mobile terminal, the realization of which enables an implementation of a procedure in which a seller sends to a buyer's (payer's) mobile phone an extract of the original invoice (m-invoice), containing at least a number of authorization account and total sum for payment, but it can also contain

some other data, such as debit account, date of payment, and purpose in order for the buyer to recognize the payment more easily. The buyer then digitally signs the payment order with his private key stored on the SIM smart card and sends it to the payment service provider (usually a bank). After the payment has been made, the payment service provider sends the buyer and the sender a confirmation on a completed transaction.

The invention will be explained in detail on the basis of the implementation procedure and Images, which present the following:

Fig 1 data exchange process among the participants in the proposed procedure for safe and simple payment with mobile terminal under the invention;

Fig 2 presentation of the system for the implementation of the procedure for safe and simple payment with mobile terminal under the invention with individual units and connections among them;

Fig 3 presentation of the system for the implementation of the procedure for safe and simple payment with mobile terminal under the invention with a uniform unit for reception and distribution of both the m-invoices as well as the m-payments.

The purpose of the proposed invention is to introduce a new mobile payment approach, in which we eliminate or at least minimize exposure/risks with a simultaneous, significantly simpler and more

accessible payment method. Risk exposure and/or complexity and accessibility of use, especially as regards the buyer, are very much identifiable in the existing systems and approaches, of which some are indicated in the present application.

The proposed invention is specific in that it provides a new procedure and a suitable implementation system for linking together several duly adjusted units into a payment system which introduces a new approach to mobile payment. This approach and mobile payment related to it have all characteristics of safe credit payment, where an account holder provides a signed order for payment chargeable to his account at a payment service provider (e.g. a bank), where he has his account opened.

The payment procedure and relations among subjects in the payment transactions are shown in Fig. 1, which presents the data exchange process among the participants in the proposed procedure for safe and simple payment with mobile terminal under the invention:

- a seller initiates a payment by sending (directly or indirectly) elements of payment to the buyer's mobile terminal (Step 1). These elements of payment are a part or an extract of the original invoice and are hereinafter referred to as "m-invoice";
- the buyer confirms on the mobile terminal that he/she wants to pay the invoice, specifies an account from which he/she wants to settle the payment, and by entering the password for the access to his private key he/she initiates a process which digitally signs the

payment order on the SIM card. Such digitally signed payment order is hereinafter referred to as "m-payment";

- after signing is completed, the m-payment is sent to a payment service provider (e.g. a bank), where the buyer has his/her debit account opened (Step 2). When the payment is realized at the provider, the payment service provider sends a notice on the completed payment to the buyer's mobile terminal (Step 3a), and to the seller's system in which the payment was initiated (Step 3b). Subsequently, payment between the buyer's and seller's payment service providers is settled in line with the applicable rules of settlement in financial area (e.g. inter bank clearing systems) (Step 4), which results in the seller receiving a paper/electronic notice on an inflow (Step 5) from his bank.

In the proposed invention we include also mobile payments for certain anticipated transactions (e.g. loading of a prepaid account for telephone services users), for which the elements of payment (m-invoice) are sent to/configured on buyers' mobile terminals by sellers in advance. In such a case, the buyer only selects the corresponding service (m-invoice), which he needs/wants, and then continues following the above described procedure.

The described procedure is applicable also for the loading of the NFC (Near Field Communication) account. With the mobile terminal, a user can safely confirm the transfer of funds from his account at a payment service

provider (e.g. from his/her bank account) to his/her NFC account from which he/she then withdraws funds at payment by using the mentioned technology.

The proposed mobile payment is equal to cash payment at a cash register, credit payment at a bank counter, or safe, i.e. digitally signed online payment; its advantage is, of course, that the buyer can sign the payment anytime and anyplace where the mobile network service for an exchange of (short) messages is enabled. In this case, the buyer is independent of the seller's location and the location of his/her payment service provider, and does not require access to any kind of additional devices (such as computer with Internet access, POS devices and other).

The proposed payment system is based on the method of safe mobile payment with the use of suitable computer, communication and software equipment and ordinary and mobile land network presented in Fig. 2 and 3. As presented in the Fig. 2 and 3, the proposed payment system is composed of units for issuing m-invoices (Ia and/or Ib), the unit for reception and distribution of m-invoices (II), unit for preparation and signing of m-payments (III), unit for reception and distribution of m-payments (IV), and the unit for realization and settlement of m-payments (V). It is understandable that the units and equipment related to the content are taken care of by their holders (seller for units Ia and Ib, buyer for units III, and banks for units V). Specialized infrastructural units can be established at the indicated subjects (units II at the seller, units IV at the

buyer's bank), although it is more rational and efficient to establish them as infrastructure at trustworthy business subjects, similar to the practice of the certificate agencies for the issue of digital certificates.

Units for issuing m-invoices (Ia and Ib) are an upgrade of the sales systems enabling a selection of goods and/or services, issue of original invoices, payment realization, and in certain cases also the delivery of goods. Each unit for issuing m-invoices (Ia and Ib) contains a module for creation of an invoice extract, module for definition of the number of the buyer's mobile terminal whom the m-invoice is intended to, and module for digital signing of an m-invoice (if a statutory regulative or the practice is such or if this is a method of seller's identification in a unit for reception and distribution of m-invoices (II)). The unit for issuing m-invoices (Ia and Ib) is connected with the unit for reception and distribution of m-invoices (II) through the module for the delivery of an m-invoice and the module for the reception of feedback on the payment status linked to a certain m-invoice.

In compliance with the proposed invention, the extract of the original invoice contains at least an authorization account, which is an account on which the seller wishes to receive funds and the total sum of payment.

Optionally, the extract includes a short purpose of payment, which enables a buyer to recognize the payment on the mobile terminal more easily. Other optional data are also possible, among which also the debit account, i.e. an account from which a buyer wants to pay, and the date of

payment, which is a date when the payment should be settled. Date of payment is usually used only in automatic units for issuing m-invoices (description is given in continuation).

The proposed invention includes two different modes of connecting units for issuing m-invoices (Ia and Ib) with the units for reception and distribution of m-invoices (II).

Fixed units for issuing invoices (Ia) are connected with units for reception and distribution of m-invoices (II) via the land line telecommunication network (e.g. local network, VPN, the Internet) and are further divided in the so-called automatic and interactive systems.

Automatic fixed units for the issue of invoices (Ia) contain units where m-invoices are issued at sellers in suitable applications, the foundation of which is a register of buyers containing connection between the buyer's number and the number of his mobile terminal, and in certain versions also the number of the buyer's bank account. Such automatic units are usually used by sellers who have a large number of regular customers, which is why they are appropriate also for the payment of regular liabilities (e.g. utility services, electricity). Automatic units most frequently operate in the so-called batch mode in the phase of m-invoice sending and in the phase of the reception of payment statuses linked to the issued m-invoices.

Interactive fixed units for issuing m-invoices (Ia) are those units where the data for the issue and direction of an m-invoice are entered

interactively into a corresponding application. A feature of interactive units is also that after the entry has been confirmed to be correct, an m-invoice is immediately issued, namely by sending the m-invoice immediately to the unit for reception and distribution of m-invoices (II), and that they wait in the same session for information on the payment realization. Interactive units can be direct, meaning the data are entered by the seller, or indirect, meaning they are integrated into the seller's web store which enables a buyer to enter the data. Such interactive systems are usually implemented on the seller's websites.

Mobile units for issuing m-invoices (Ib) are connected with the unit for reception and distribution of m-invoices (II) through the public land mobile network (PLMN). These are basically interactive units enabling the entry of elements of an m-invoice and the entry of the buyer's mobile terminal's number, a review of the entered data, issue of an m-invoice (also digital signature if needed), and sending of an m-invoice to the unit for reception and distribution of m-invoices (II) through the public land mobile network. The status of payment linked to the issued m-invoice returns through the public land mobile network to the number which forwarded the m-invoice immediately after the realization of the payment.

The unit for reception and distribution of m-invoices (II) is an intermediary unit between the unit for issuing m-invoices (Ia and Ib) and the unit for preparation and signing of m-payments (III). The unit for reception and distribution of m-invoices (II) contains a module for

reception of m-invoices, module for m-invoice sender's identification, module for m-invoice integrity verification (usually through the issuer's digital signature), module for sending m-invoice to the buyer's mobile terminal, and a module for reception and forwarding of the status of payments linked to the sent m-invoices. The unit for reception and distribution of m-invoices (II) contains a register of sellers and their identification elements (usually, these are digital certificates the validity of which must in such case be verified), and a database of issued m-invoices and the payment statuses linked to the issued m-invoices. The unit also has access to local or external registers of valid or revoked digital certificates.

The unit for reception and distribution of m-invoices (II) usually contains an integrated additional module enabling, in connection with the unit for preparation and signing of m-payments (III), the payment of those m-invoices which are still valid (their date of payment has not expired yet), and which were not paid immediately when the buyer received a notice at his mobile terminal.

The unit for preparation and signing of m-payments (III) is connected with the unit for reception and distribution of m-invoices (II) and the unit for reception and distribution of m-payments (IV) through the public land mobile network. The unit for preparation and signing of m-payments (III) contains a module for reception of m-invoices, module for selection of a debit account if more accounts are possible, a module for preparation and

digital signing of a payment order, module for sending of m-payments, and a module for reception of the payment realization status. The unit for reception and distribution of m-payments (IV) contains a register of possible debit accounts if the implementation is such that the debit account is not a part of an m-invoice.

The unit for preparation and signing of m-payments (III) usually contains an integrated additional module enabling this unit to subsequently pay those m-invoices which were not paid immediately when the buyer received a notice at his mobile terminal.

The unit containing the module for payment of services prepared in advance is considered a special version of the unit for preparation and signing of m-payments (III). This module is closely connected with the register of services prepared in advance, such as the loading of a prepaid account for mobile phoning. Another service prepared in advance is also the so-called loading of an account used by a buyer for payment with the NFC technology. Besides the module for loading of an NFC account, the proposed system in the unit for the preparation and signature of m-payments (III) in such a case contains also two modules for actual refreshing of balance of funds on the NFC account in the database and the mobile terminal when the datum on the sum of the available resources is also kept there.

The unit for preparation and signing of m-payments (III) can also contain infrastructural modules (a module for reception and extension of a

digital certificate, module for maintenance of the register of possible debit accounts and a module for maintenance and adding of services prepared in advance), which enable remote maintenance of this unit.

The unit for reception and distribution of m-payments (IV) is connected through mobile network with the unit for preparation and signing of m-payments (III), and through land line telecommunication network with the unit for realization and settlement of payments (V). The unit for reception and distribution of m-payments (IV) contains a module for reception of m-payments, module for m-payments authenticity verification (of the buyer), module for m-payment integrity verification (on the basis of the digital certificate verification), module for sending of m-payments to the unit for realization and settlement of payments, module for reception and forwarding of payment realization status. The unit for reception and distribution of m-invoices (II) contains a register of payment service providers (including their communication specifics) and a database of receipted m-payments and their relevant payment realization statuses. The unit also has access to local or external registers of valid and revoked digital certificates.

Each unit for realization and settlement of m-payments (V) connects the unit for reception and distribution of m-payments (IV) with the existing complex systems for the reception, realization and settlement of payment orders at payment service providers (e.g. banks). It contains at least the module for reception of m-payments, module for verification of the

signatory's authorizations on a defined debit account, and a payment realization module which checks if there are enough funds on an account, realizes the payment and returns the status of the payment realization to the unit for reception and distribution of m-payments. The unit for realization and settlement of payments (V) at a payment service provider contains at least a register of clients (buyers), their digital certificates and their authorizations.

An advantage of the proposed invention is primarily the fact that all data of the payment order are joined when they arrive at the buyer's mobile terminal, and that they are also digitally signed there in the way which enables an unambiguous authentication of the signatory and integrity and non-repudiation of the payment order in the continuation of the payment process. In other words this means that a digitally signed payment order can only be issued with duly adjusted mobile terminal, which is owned by the buyer and is one of the system units used in the described procedure. If the buyer does not sign the payment order with his mobile terminal, this procedure disables the payment order from being issued in any other way, thus making a falsification or a break into the system practically impossible.

No risk exists also in the case of a loss/disposal of mobile terminal, as access to the private key on the SIM card is actively protected. If somebody enters an incorrect password (at the recommendations, for example a 6 or more-digit PIN code or other alphanumerical password) for

the access to his private key a few times in a row (e.g. three times), the signing function in the mobile terminal blocks and it cannot be used anymore.

An additional advantage of the proposed invention is also its simplicity of use, which is important especially for the buyer or payer who is included in the payment chain via the mobile terminal. Technical features of mobile terminals (this applies predominantly to a small screen and small characters on the screen and keypad) are not comparable with other interactive computer devices, which is why the proposed solution, which requires from the buyer only to review the m-invoice and in the basic version to make one single entry, i.e. entry of the password for access to personal private key, presents the simplest possible solution.

And last but not least, the proposed mobile payment method can be realized on each mobile terminal which supports the technology of the exchange of short messages (for example SMS), thus making this payment method nowadays accessible practically to all owners of mobile phones, pocket PCs or other mobile terminals operated by means of a wireless communication network.

Digital signature of an m-invoice or m-payment ensures integrity and non-repudiation of a document during its transport, and long-term archiving ensures integrity and non-repudiation in the statutory determined period of the keeping of such documents. Long-term archiving can be established at an individual business entity (record of m-invoices at

sellers, and record of m-payments at the payment service providers). The most rational and efficient way is to establish long-term archiving as an infrastructure at trustworthy business subjects, as in such a case the same records can be used by all subjects in the mobile payment chain: the seller, buyer and payment service providers.

On the presumption that the holders of digital certificates, the private key of which is stored on the mobile terminal's SIM card and is actively protected, act with due diligence and care and in compliance with the policy of a digital certificate issuer, the proposed payment system is very safe, as it disables a third party to access the data which could enable him to issue a payment order without having authorization.

Information confidentiality during the transport of documents is guaranteed with the use if adequate encryption methods (e.g. 3DES/AES symmetrical encryption systems and PKI technology).

The proposed invention is understandingly linked to the proposed units and their connection, and defines also a method of how these units work and are interlinked.

In compliance with the invention, an extract of the original invoice containing at least an authorization account and the sum, and usually also the purpose and optionally also the date of payment and other data, is prepared in the unit for issuing m-invoices (Ia and Ib) on the basis of the original invoice. If necessary, this invoice extract is signed (depending on legislation or practice or agreement) with a relevant digital certificate and

equipment (HSM or smart card; and server certificate on disc only if access to the server is duly protected) and is sent via the local or land network together with the buyer's mobile terminal number to the unit for reception and distribution of m-invoices.

The unit for reception and distribution of m-invoices (II) receives and verifies the m-invoice and the identity of its issuer. If the issuer is included in the proposed payment system and if everything is OK with the m-invoice, it sends the m-invoice via the public land mobile network to the unit for preparation and signing of m-payments (III).

The unit for preparation and signing of m-payments (III) is implemented in the mobile terminal, which contains a relevant smart card, such as SIM (Subscriber Identity Module). When this unit (III) receives an m-payment, it offers the buyer an option to pay it. When the buyer confirms his will to pay the invoice, the account from which he wants to settle the payment is determined by the program. If the debit account is already defined in the m-payment, this is a default debit account. Otherwise, the account is determined on the basis of configured accounts in the mobile terminal. If more debit accounts are configured, the buyer must choose the one from which he wants to realize the payment. Otherwise, the buyer does not enter anything, as the only configured account is considered a default debit account. The client then enters a password (for example PIN – Personal Identification Number) for access to his private key, which

activates a process that creates a payment order in the smart card, such as SIM card, and digitally signs it.

The password for the access to personal private key is different from the PIN code for telephone protection and consequent access to ordinary mobile services. The signing procedure pursuant to the PKI (Public Key Infrastructure) technology is based on a digital certificate and a private key, which is located on the card and is actively protected. Private key is actually the only truly secret datum and is not known to anyone (not even the owner).

After the signing is completed, the m-payment containing a digitally signed payment order is sent via the public land mobile network to the unit for reception and distribution of m-payments (IV). The unit verifies the m-payment and the buyer's identity. If the buyer has a valid digital certificate and if everything is OK with the m-payment, it sends the m-payment to the unit for realization and settlement of m-payments (V), which is an entrance channel for mobile payments at the payment service provider where the buyer has his account opened and which is indicated as the debit account in the m-payment.

On the basis of a digital certificate of the buyer who has signed the m-payment, the unit for realization and settlement of m-payments (V) first verifies if this person is actually authorized for realization of payments on the indicated debit account. If so, the unit sends the payment for realization. The unit for realization and settlement of m-payments (V) at a

certain payment service provider is usually common to all channels (bank counter, electronic bank) and realizes the payment if there are enough funds on the account, otherwise it rejects the payment.

If payment is realized at the payment service provider, it is later settled between the seller's and the buyer's payment service providers in compliance with the applicable settlement rules in the financial area (e.g. inter bank clearing systems), which results in the seller receiving a paper/electronic notice on inflow from his payment service provider.

The payment service provider informs the unit for realization and settlement of m-payments (V) about the payment realization status, which in connection with other units in the mobile payment chain can provide for the feedback on the payment realization status linked to a certain m-invoice to be transferred to the buyer's mobile terminal, and to the system of the seller in which he initiated the payment.

The versions of the proposed payment system where the system for preparation and signing of m-invoices (III), i.e. on the buyer's mobile terminal, contains established anticipated transactions (e.g. loading of prepaid account for the users of telephone services or the NFC account) and for which the sellers have sent/configured the payment elements (m-invoice) in advance, the buyer simply chooses a desired transaction and consequently naturally also the m-invoice from the menu, selects the debit account if necessary and enters the password for the access to his private

key, which activates the preparation of the payment, digital signing and sending of the m-payment.

One of the payments prepared in advance is also the loading of the NFC account, which apart from the procedures indicated in the ordinary m-payments requires also the updating of the information on the balance on the NFC account in the database of the NFC services provider, and information on the balance on the mobile terminal when the information is kept also there. The information on the amount of available funds on the NFC account is refreshed in the database through the network connection immediately after the payment is realized or funds are transferred, and on the mobile terminal through feedback received by the software on the terminal through the mobile network or through the NFC channel, when the mobile terminal is leaned against a relevant NFC reader/transmitter.

In the proposed invention, the issue and maintenance of the digital certificate base can be implemented at individual subjects involved in the payment (the seller and the buyer's payment service provider), at trustworthy business subjects where, for example, the unit for reception and distribution of m-invoices (II) and/or the unit for reception and distribution of m-payments (IV) is implemented, or at the existing certification agencies (CA). If certification agencies are outside the described systems, adequate interfaces must be implemented to the units which require data on issued/revoked digital certificates.

In the proposed invention, similar applies for long-term archiving, which can be implemented at individual subjects involved in the payments (the seller and the buyer's payment service provider), at trustworthy business subjects where, for example, the unit for reception and distribution of m-invoices (II) and/or the unit for reception and distribution of m-payments (IV) is implemented, or at the existing agencies for archiving. If agencies for archiving are outside the described systems, adequate interfaces for the transfer of documents which must be archived in a long-term period, must be implemented.

In comparison with other systems and methods, the proposed invention brings a range of advantages in mobile payment. No sensitive information (such as credit card number; the only really secret information, i.e. the private key, is not known and not available even to its holder) is transferred through public networks. The highest possible and commercially available level of mobile payment security is ensured, as the integrity and non-repudiation of mobile payment and also mobile invoice if necessary, are provided in the time of the payment and within the statutory period of time if these mobile documents are duly long-term archived. During the transfer through public networks, the data are encrypted, meaning the confidentiality of data is also provided for. Payment in line with the described procedure is completely simple, as an entry of one single datum is required in the basic version, i.e. the password for the access to the personal private key. And the use of the

short message sending technology, which is nowadays supported practically by all mobile terminals, enables payment with the proposed systems and methods accessible practically to anyone.

The proposed payment system with the units included in it, features of these units and connections among them are described into detail and accompanied with relevant schemes in Images 2 and 3 in the continuation of the present document. The schemes are, of course, merely illustrative and given to enable easier understanding. The schemes do not set the limits of the invention, which is defined with the statements.

Each m-invoice intended to a user's mobile terminal is created in the unit for issuing m-invoices (Ia and/or Ib). The invoice extract creation module is in charge for the preparation of the basic data of the m-invoice, such as the sum, purpose and authorization account. At the preparation of the extract, the module uses a relevant electronic invoice form in case of automatic fixed units for issuing m-invoices (Ia), and in other cases the data of the invoice are determined interactively with the entry in a relevant program solution.

The module for definition of the number of the buyer's mobile terminal in the unit for issuing m-invoices (Ia and/or Ib) adds the buyer's mobile terminal's telephone number to the data of the invoice. The module uses the register of PTN user telephone numbers in case of automatic fixed units for issuing m-invoices (Ia), and in other cases the telephone number is entered in the m-invoice during the time of shopping.

The digital signing module takes care that the m-invoice is digitally signed if this is anticipated in a relevant unit for issuing m-invoices (Ia and/or Ib).

An m-invoice can be prepared and digitally signed automatically in the provider's back-office processing (large providers) or the data and m-invoices are prepared interactively and digitally signed during the time of shopping with the use of relevant equipment (e.g. web store, call center for catalogue sale, mobile unit for issuing m-invoices (Ib)).

The units for issuing m-invoices (Ia and Ib) forward prepared m-invoices to the unit for reception and distribution of m-invoices (II) (Step 1). Information is exchanged through the NET public land line telecommunication network (Ia unit) or PLMN public land mobile network (Ib unit) through the module for issuing m-invoices in the units for issuing m-invoices (Ia and Ib) and a module for reception of m-invoices in the unit for reception and distribution of m-invoices (II).

When the module for reception of m-invoices in the unit for reception and distribution of m-invoices (II) successfully receives a new m-invoice, it delivers it to the module for identification of the sender or issuer of m-invoice. The module for sender's identification uses the database of MTP registered issuers of m-invoices, in which it finds a corresponding record on the basis of identification data of the unit for issuing m-invoices (Ia and Ib) and checks if the unit is authorized for the forwarding of m-invoices. Verification of the issuer's identity is usually performed on the basis of a

digital certificate used by the unit for issuing m-invoices to connect with the unit for reception and distribution of m-invoices (II). When the legislation or the environment requires the issued m-invoices to be digitally signed, identification is verified also on the basis of a digital certificate used to sign the m-invoice.

The authenticity of the used digital certificates in the unit for reception and distribution of m-invoices (II) is verified previously also in the CDR directory of valid digital certificates. Besides the presence of the certificate, time validity of the certificate and the status of the certificate in the list of the revoked digital certificates issued by the digital certificate issuer in the system or an independent external digital certification authority (CA) are also verified.

Verification of the identity of the issuer who uses a mobile unit for issuing m-invoices which does not support the use of the PKI functionality, is implemented on the basis of the terminal's identification (SIM card serial number and telephone number), shared confidentiality between the terminal and the unit for reception and distribution of m-invoices (II), and MAC (Message Authentication Code) codes.

All indicated mechanisms (digital certificates and digital signatures, CDR directory of digital certificates, validity of certificates, MAC codes) make sure that the unit for reception and distribution of m-invoices (II) can credibly verify the identity of the issuer of each m-invoice delivered into the

system, and thus provide for the authenticity of the m-invoice and consequently of the data in payment.

Besides the issuer's authenticity, the unit for reception and distribution of m-invoices (II) in the module for the m-invoice integrity verification credibly verifies also the integrity of the receipted m-invoice with the digital signature or MAC code, which together with authenticity means that each invoice was created in an authorized unit for issuing m-invoices (Ia and Ib), that the data were entered into the m-invoice by an authorized issuer and that nobody has changed them during their transport.

After the m-invoices are verified for authenticity and integrity, they are stored in the MBA m-invoice database. If necessary (regulator requirement or legal requirement), such m-invoices can be also archived in a long-term way. In such a case, authenticity and integrity of the recorded m-invoices are provided for by the technology of digital signatures, time stamping, long-term archiving and a control of the access to the records.

After the issuer's identity and m-invoice's integrity are verified and the m-invoice is stored in the database, the unit for reception and distribution of m-invoices (II) sends an m-invoice through the PLMN public land mobile network via the m-invoice sending module to the buyer's mobile terminal, i.e. the unit for preparation and signing of m-payments (III), where it is receipted by the m-invoice reception module (Step 1a).

Initially, the m-invoice reception module in the unit for preparation and signing of m-payments (III) verifies with the use of cryptographic algorithms that the m-invoice was delivered by an authorized unit for reception and distribution of m-invoices (II). Subsequently, all relevant data of the m-invoice are combined into a payment order, which contains specified also the debit account (e.g. the user's bank account), in the unit for preparation and signing of m-payments (III). When a datum about the debit account is not a part of an m-invoice, the account is read in the module for the selection of a debit account from the DAC register of the debit accounts if there is only one debit account in the register. If there are more accounts in the DAC register, the module for the selection of a debit account displays a menu on the screen of the terminal enabling the user to select the corresponding account.

When the payment order is entirely prepared, it contains at least the sum, authorization account and debit account, and optionally also the purpose of payment and the date of payment in the case of a payment with the date of payment in the future time. The module for preparation and digital signing of a payment order displays the extract of the order to the user and offers him an option of payment confirmation or cancellation. If the payment is confirmed, the user can enter a password (for example PIN) to open the private key on the SIM card, which enables the payment to be digitally signed in the card's security module. The operation of digital signing is carried out in the security module, thus making sure the user's

private key never leaves the protected space on the SIM card and remains secret during the entire procedure.

The unit for preparation and signing of m-payments (III) has space on the mobile terminal and the SIM card intended for the storing of m-invoices fixed in advance (e.g. topping of the prepaid account at a mobile operator, topping of NFC account) in the register of the CPY services prepared in advance. M-invoices stored in advance from the CPY register behave similar to the m-invoices sent to the mobile terminal by the unit for reception and distribution of m-invoices (II), with the exception that they are processed by the module for payment of services prepared in advance instead of the module for reception of m-invoices. In such a case, the m-invoice also contains all data required for the preparation of the m-payment and can be dealt with as an ordinary m-invoice in all subsequent modules. The debit account is this way read/selected from the DAC register in the module for the selection of the debit account, while the display, confirmation and signature of the payment are made in the module for the preparation and digital signing of the payment order under the already described procedure.

When the module for preparation and digital signing of the payment order in the unit for preparation and signing of m-payments (III) prepares an m-payment, it delivers it to the module for sending of m-payments, which transfers it through the PLMN public land mobile network to the

module for reception of m-payments in the unit for reception and distribution of m-payments (IV) (Step 2).

After a successful reception, the module for reception of m-payment in the unit for reception and distribution of m-payments (IV) delivers the m-payment to the module for verification of m-payment's authenticity.

On the basis of the sender's identification data on the m-invoice, i.e. the SIM card's serial number or mobile terminal's telephone number, the module for verification of the m-payment's authenticity finds a corresponding digital certificate of an individual unit for preparation and signing of m-payments (III) in the CDR directory of digital certificates and verifies its authenticity, which also verifies the certificate's time validity and status in the CRL list of revoked certificates issued by the digital certificate issuer in the system or an independent external certificate authority (CA).

After the indicated security elements are verified and the authenticity of the m-payment is subsequently ensured, the m-payment is received by the module for verification of integrity and non-repudiation of the m-payment. The module verifies the digital signature of the m-payment, which in the final stage guarantees that the m-payment has come from an authentic source, that the data in it could only be entered by the private key owner in the unit for preparation and signature of m-payments (III) and that the m-payment was not changed during its transport.

The m-payment, for which authenticity, integrity and non-repudiation were verified, is stored in the MPA m-payment database in the unit for

reception and distribution of m-payments (IV). If necessary (regulator requirement or legal requirement), such m-payments can be also archived in a long-term mode. In such a case, the authenticity and integrity of the recorded m-invoices are taken care with the technology of digital signatures, time stamping, long-term archiving and a control of the access to the records.

In the unit for reception and distribution of m-payments (IV), a verified m-payment is finally delivered to the module for sending m-payments in the unit for realization and settlement of payments (V). On the basis of the debit account and the PYP register of payment service providers (e.g. banks supporting the mentioned payment method), this module firstly determines the payment service provider where the debit account is opened, and forwards the m-invoice via the NET land line telecommunication network to the unit for realization and settlement of m-payments (V) (Step 2a).

The module for reception of m-payments in the unit for realization and settlement of m-payments (V) receives and verifies the data of the m-payment. The module can again verify the authenticity and integrity of the m-payment itself or trust the unit for reception and distribution of m-payments (IV) when this system is installed at a trustworthy partner or payment service provider. After successful reception, the m-payment is forwarded to the module for verification of the signatory's authorizations.

The module for verification of the signatory's authorizations in the unit for realization and settlement of m-payments (V) verifies if the m-payment's signatory has relevant authorizations for the management of the funds on the debit account indicated in the m-payment. User searching is performed on the basis of the data in the signatory's digital certificate or the certificate itself in the MPC register of clients (buyers) who use the mobile payment system. After the authorizations have been successfully verified, the module delivers the m-payment to the payment realization module.

The payment realization module in the unit for realization and settlement of m-payments (V) verifies the general operating conditions required for the payment realization (such as the balance on the account) and sends the m-payment for actual realization and settlement. When the payment is realized, the funds on the debit account are transferred to the authorization account through established financial channels (e.g. inter bank clearing system), and the payment realization module provides feedback on the status of the relevant m-payment (accepted, rejected, error) to the unit for reception and distribution of m-payments (IV) (Step 3). This feedback is transferred via the NET public land line telecommunication network and contains all required information for the determination of the final status of the relevant m-payment and m-invoice related to it.

The feedback on the m-payment status is received by the module for the reception and forwarding of the payment realization status in the unit for reception and distribution of m-payments (IV). The module marks the status of the relevant m-payment in the MPA m-payment database, and this status can also be archived in a long-term mode, if necessary. This same module can be assigned the task of forwarding the feedback on the payment status to the unit for the preparation of m-payments (III) (Step 3a) and to the unit for reception and distribution of m-payments (II) (Step $3b_1$ in Image 2).

If the transmission of the status is implemented and used for a relevant m-payment, the module for reception of payment realization status verifies the m-payment status authenticity in the m-payment preparation unit (III) and displays feedback on the payment (accepted, rejected, error) to the user on the screen of the mobile terminal. The status is stored on the mobile terminal in the form of a short message to enable the user to keep it for personal record of m-payments.

The m-payment status is information which directly determines also the final status of an individual m-invoice. This is why the module for reception and forwarding of the payment status can also be implemented in the unit for reception and distribution of m-invoices (II). This module can verify the authenticity and integrity of m-payment status, mark the status of the corresponding m-invoice in the MBA m-invoice database (if necessary,

this status can also be archived in a long-term mode) and forward the m-invoice status to the m-invoice issuer (Step 3b).

Interactive m-invoice issuers receive from the unit for reception and distribution of m-invoices (II) the m-invoice status in m-payment related to it as a response to the sent m-invoice. The automatically operating units for issuing m-invoices can receive several m-invoice statuses, which were previously sent to the unit for reception and distribution of m-invoices (II) at the same time. The units for issuing m-invoices (Ib), which are realized with customized mobile terminals, can use the data from the m-payment invoice also to print a receipt, which is handed over to the buyer for record keeping and as a proof of the realized payment.

When an m-payment is not created and sent within a certain period of time in the unit for preparation and signing of m-payments (III) at the reception of an m-payment, the m-invoices are stored in the unit for reception and distribution of m-invoices (II), where they wait on the request made by the unit for preparation and signing of m-payments (III). On the request made by the payer, the unit for preparation and signing of m-payments (III) can send a request for a new sending of the m-invoices in queue to the unit for reception and distribution of m-invoices (II) via the PLMN public land mobile network (Step R). Such m-invoices are then forwarded by the unit for reception and distribution of m-invoices (II) to the unit for preparation and signing of m-payments (III) the same as at the first sending of m-invoices (Step 1a).

PATENT CLAIMS

1. The procedure for safe and simple payment with mobile telephone,

characterized by

that the relations among subjects are performed in the following sequence:

payment is initiated by the seller by sending (directly or indirectly) the elements of payment to the buyer's mobile terminal (Step 1), where these elements of payment are a part or an extract of the original invoice and are hereinafter referred to as "m-invoice";

m-invoice prepared in advance can be issued and consequently payment can be initiated also by the buyer or mobile phone user alone (in this case, Step 1 is carried out in the mobile terminal) when he wants, with a relevant function on the mobile terminal, to transfer funds from his account at the payment service provider (e.g. a bank) to another of his accounts, which is intended either for payment of certain services and/or products (such as a prepaid user account for payment of mobile operator's services) or for a certain payment method (such as payment with the use of NFC – Near Field Communication – technology);

on the mobile terminal, the buyer confirms that he wants to pay the invoice, specifies an account from which he wants to settle the payment, and by entering the password for the access to his private key

he activates the procedure which digitally signs the payment order, i.e. "m-payment", in the SIM card;

after the signing is completed, the m-payment is sent (Step 2) to the payment service provider (e.g. bank), where the buyer has his debit account opened;

when the payment is realized at the provider, the buyer's payment service provider sends a notice on the realized payment to the buyer's mobile terminal (Step 3a), and to the seller's system where the latter initiated the payment (Step 3b);

payment between the buyer's and the seller's payment service provider is settled pursuant to the applicable settlement rules in the financial area (e.g. inter bank clearing systems) (Step 4);

the seller receives a paper/electronic notice on inflow from his bank (Step 5);

2. The system for safe and simple payment with mobile terminal under the procedure according to the claim 1,

characterized by

that it is composed of the unit for issuing m-invoices (Ia and/or Ib), unit for reception and distribution of m-invoices (II), unit for preparation and signing of m-payments (III), unit for reception and distribution of m-payments (IV) and unit for realization and settlement of m-payments (V), where fixed units for issuing invoices (Ia) connect with the units for

reception and distribution of m-invoices (II) through the land line telecommunication network (e.g. local network, VPN, the Internet), and mobile units for issuing m-invoices (Ib) connect with the unit for reception and distribution of m-invoices (II) through public land mobile network (PLMN), so that the unit for reception and distribution of m-invoices (II) is an intermediary unit between the unit for issuing m-invoices (Ia and/or Ib) and unit for preparation and signing of m-payments (III); that the unit for preparation and signing of m-payments (III) is connected with the unit for reception and distribution of m-invoices (II) and the unit for reception and distribution of m-payments (IV) through the telecommunication network; that the unit for reception and distribution of m-payments (IV) is connected with the unit for preparation and signing of m-payments (III) through mobile network, and with the unit for realization and settlement of payments (V) through land line telecommunication network, where each unit for realization and settlement of m-payments (V) connects the unit for reception and distribution of m-payments (IV) with the existing complex systems of reception, realization and settlement of electronic payment orders at payment service providers (e.g. banks).

3. The system for safe and simple payment with mobile telephone according to the claim 2,

characterized by

that the unit for issuing of m-invoices (Ia and/or Ib) contains a module for invoice extract creation, module for definition of the number of a buyer's mobile terminal, module for digital signing of an m-invoice (if a statutory regulative or the practice is such or if this is a method of seller's identification in the unit for reception and distribution of m-invoices (II)), and two modules (module for m-invoice delivery and module for reception of payment status feedback linked to a certain m-invoice) for exchange of information with the unit for reception and distribution of m-invoices (II); that in certain versions the unit contains a register of buyers.

4. The system for safe and simple payment with mobile telephone according to the claim 2,

characterized by

that the unit for reception and distribution of m-invoices (II) contains a module for reception of m-invoices, module for m-invoice sender's identification, module for m-invoice integrity verification, module for sending m-invoice to the buyer's mobile terminal, module for reception and forwarding of status of payments linked to sent m-invoices, register of sellers and their identification elements, and a database of issued m-invoices and payment statuses linked to issued m-invoices; that the unit has access to local or external registers of valid and revoked digital certificates; that the unit usually contains an additional module which in

connection with the unit for preparation and signing of m-payments (III) enables payment of those m-invoices which are still valid (their date of payment has not expired yet) and which were not paid immediately after the buyer has received a notice at his mobile terminal.

5. The system for safe and simple payment with mobile telephone according to the claim 2,

characterized by

that the unit for preparation and signing of m-payments (III) contains a module for reception of m-invoices, module for selection of debit account if more accounts are possible, module for preparation and digital signing of payment order, module for sending of m-payments and module for reception of the status of payment realization, and the register of possible debit accounts if implementation is such that the debit account is not a part of the m-invoice; that the unit usually contains an additional module which in connection with the unit for reception and distribution of m-invoices (II) enables subsequent payment of those m-invoices which were not paid immediately after the buyer received the notice at his mobile terminal; that special versions of the unit contain also a module for payment of services prepared in advance and the corresponding register of services prepared in advance (e.g. for the loading of a prepaid account for mobile phoning); that if the unit contains an integrated service to top up an account, which is used by the buyer for payment with the NFC

technology, the unit contains, apart from the module for loading of NFC account, also a module for actual refreshing of balance of funds on the NFC account in the mobile terminal when the datum on the sum of available funds is kept also there; that the unit can contain also built-in infrastructural modules (module for reception and extension of digital certificate, module for maintenance of the register of possible debit accounts, and module for maintenance and adding of new services prepared in advance) enabling remote maintenance of this unit.

6. The system for safe and simple payment with mobile telephone according to the claim 2,

characterized by

that the unit for reception and distribution of m-payments (IV) contains a module for reception of m-payments, module for m-payment authenticity verification (of the buyer), module for m-payment integrity verification (on the basis of a digital signature), module for sending of m-payment to the unit for realization and settlement of payments, module for reception and forwarding of the status of payment realization, register of payment service providers, and a database of receipted m-payments and corresponding payment realization statuses; that the unit has access to local or external registers of valid and revoked digital certificates.

7. The system for safe and simple payment with mobile telephone according to the claim 2,

characterized by

that the unit for realization and settlement of m-payments (V) contains at least a module for reception of m-payments, module for verification of signatory's authorizations on a specified debit account, module for realization of payment, a register of clients (buyers), their digital certificates, and their authorizations.

8. The system for safe and simple payment with mobile telephone according to the claim 2,

characterized by

that the unit for reception and distribution of m-invoices (II) described in claim 4, and the unit for reception and distribution of m-payments (IV) described in claim 6, can be functionally and/or organizationally joined into one unit.

9. The system for safe and simple payment with mobile telephone according to the claim 2,

characterized by

that the unit for issuing m-invoices (Ia and/or Ib) described in claim 2, and the unit for reception and distribution of m-invoices (II) described in claim 4, can be functionally and/or organizationally joined into one unit.

10. The system for safe and simple payment with mobile telephone according to the claim 2,

characterized by

that the unit for reception and distribution of m-payments (IV) described in claim 6, and the unit for realization and settlement of m-payments (V) described in claim 7, can be functionally and/or organizationally joined into one unit.

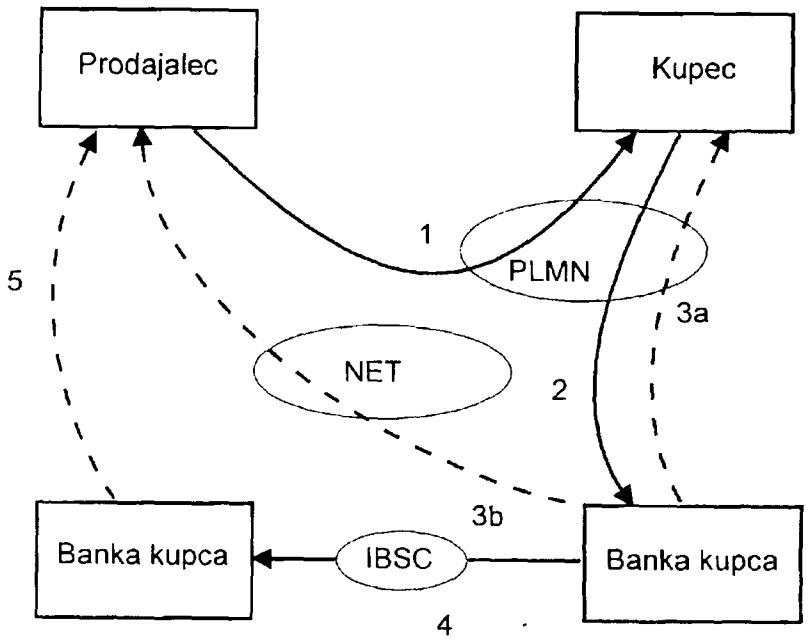
Prodajalec
Kupec
1
PLMN
5
3a
NET
2
3b
Banka kupca
IBSC
Banka kupca
4

FIG. 1

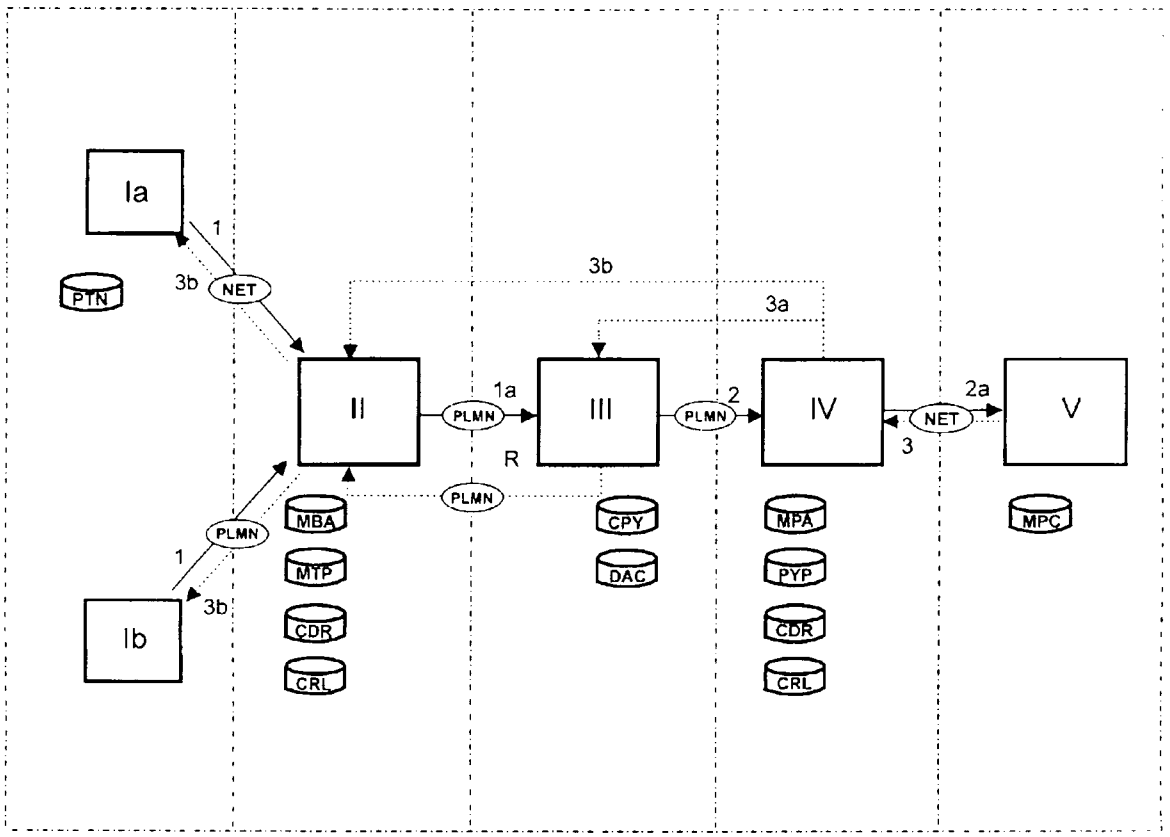
Ia
1
3b
NET
PTN
3b
3a
II
1a
PLMN
III
2
PLMN
IV
NET
2a
V
3
R
PLMN
MBA
MTP
CDR
CRL
CPY
DAC
MPA
PYP
CDR
CRL
MPC
PLMN
1
3b
Ib

FIG. 2

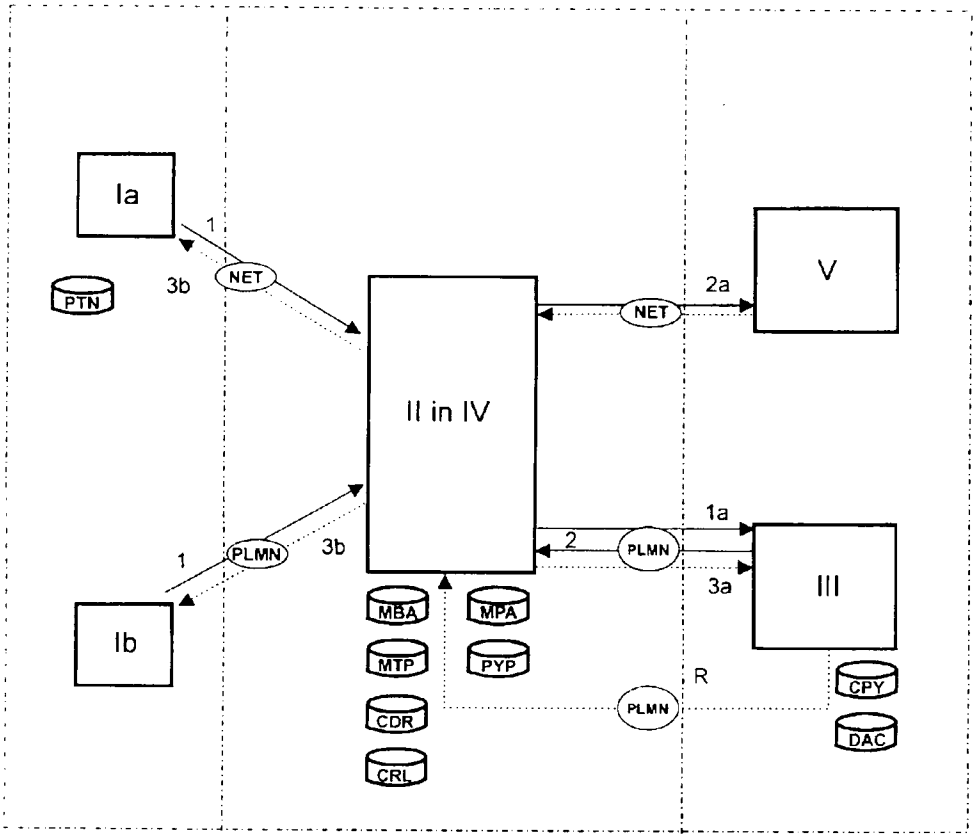
Ia
1
3b
NET
PTN
II in IV
NET
2a
V
1a
2
PLMN
3a
III
1
PLMN
3b
Ib
MBA
MPA
MTP
PYP
CDR
CRL
R
PLMN
CPY
DAC

FIG. 3