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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 October 2010 (28.10.2010)

PCT

(10) International Publication Number
WO 2010/122520 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/IB2010/051779

(22) International Filing Date:
23 April 2010 (23.04.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PP 50024-2009 24 April 2009 (24.04.2009) SK

(71) Applicant *(for all designated States except US)*: **LOGO-MOTION, S.R.O.** [SK/SK]; Winterova 15, 921 01 Piešťany (SK).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **FLOREK, Miroslav** [SK/SK]; Ing. Miroslav Florek, Sedmokráskova 4, 821 01 Bratislava (SK). **MASARYK, Michal** [SK/SK]; Ing. Michal Masaryk, PhD., Medzilaborecká 7, 821 01 Bratislava (SK).

(74) Agent: **PORUBČAN, Róbert**; Puškinova 19, 900 28 Ivanka pri Dunaji (SK).

(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, RO, RS, RU, 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, 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, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *of inventorship (Rule 4.17(iv))*

[Continued on next page]

(54) Title: METHOD AND SYSTEM OF ELECTRONIC PAYMENT TRANSACTION, IN PARTICULAR BY USING CONTACTLESS PAYMENT MEANS

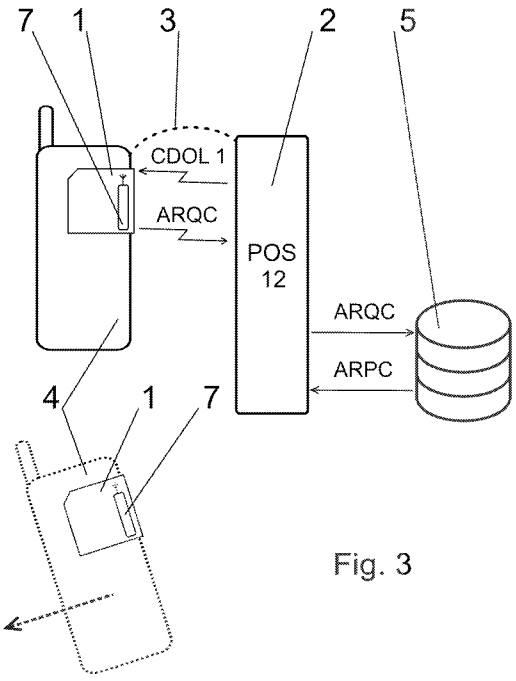

Fig. 3

(57) Abstract: A method of electronic payment transaction is characterized by the fact that during processing of one payment transaction, a communication link (3) between the card (1) and the terminal (2) is interrupted and the ARPC answering file is received to the card (1) after the original communication link (5) is interrupted. Two phases are separated by a reset of the card (1) where in the second phase initial payment data (ARQC) are used. Electronically signed ARQC payment file is stored in the card's (1) memory for at least until the corresponding time ARPC answering file is of received and processed. The solution enables to place the mobile phone with a payment card (1) near to the terminal's (2) reader twice. The first time, a request for on-line authorization is generated and during the second touch the information from the payment processor (5) is recorded into the payment application.

WO 2010/122520 A2

Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

METHOD AND SYSTEM OF ELECTRONIC PAYMENT TRANSACTION, IN PARTICULAR BY USING CONTACTLESS PAYMENT MEANS

FIELD OF INVENTION

The invention relates to a procedure and a system of an electronic payment application with the use of payment means in a form of a payment card. It deals with a method of a direct debit payment transaction by using contactless payment means that is adjusted so it can be inserted into a mobile communication device.

PRESENT TECHNOLOGY STATUS

POS (point of sale) terminals are commonly used to process electronic payment transactions using different chip payment cards. These terminals are connected to a remote payment processor in the form of a clearing centre belonging to a payment card issuer or a bank. At the beginning of a payment process, the chip of the payment card is reset into its initial position. After reset, the information about the card and terminal type will be exchanged between the card and terminal. This basic identification brings the connection between the card and the terminal into a position allowing mutual communication as well as communication towards the payment processor server.

The POS terminal sends data about the required payment into the card, the data structure includes for example amount, currency, date and similar. The terminal also requests the card to give a statement. The card, according to its settings generates an answer and signs it with its electronic signature. The card´s response in the form of "TC" (Transaction Certificate) means an acceptance of off-line payment where the authorization by a payment processor is not needed. The response in the form of "AAC" (Application Authentication Cryptogram) means that the payment will not be accepted by the card under any conditions. The subject matter of this invention is a method, a procedure of a payment process during generation of the response in the ARQC (Authorization Request Cryptogram) form. Such answer means that the card requires authentication and co-operation with a payment processor server.

After an answer is generated in the form of a payment file, mainly of ARQC type, the card sends this encrypted payment file to the processor and waits until the processor's answer is received. While waiting, the payment card must remain in touch with the terminal to create

a continuous communication channel between the card and the payment processor. The interruption of this channel will cause termination of the payment process. If the payment processor sends back a ARPC response file (Authorization Response Cryptogram) into the card, then this file is sent via terminal into the payment card and the payment card decodes the instructions for further procedure (in particular as ARPC) from the response file and reports the result to the terminal in the form of TC eventually AAC.

The essential feature of the communication method between the payment card and the terminal/payment processor that is known up till now is a constant connection, a continuous, uninterrupted channel of the given cashless payment hardware elements during bidirectional communication. This communication lasts approximately some seconds, eventually tenths of seconds. The interruption of the connection between the card and the terminal would cause a new restart of the card application, which will be recorded for example via incrementation of its counter. Change of counter data would elicit a change of newly generated payment file ARQC and after an interruption it would not be possible to finish the payment process successfully using the data that were originally generated before the connection was interrupted. When using standard payment cards connected through a contact there is no problem to keep a reliable communication link since this link is interrupted only in the case when the card is taken early from the slot of the appropriate reader.

With the increasing usage of contactless payment means there appears the problem with the stability of the communication channel. It is not suitable to require from the payer to hold his contactless payment means uninterruptedly and with concentration within the reach of a contactless reader during the whole time of payment process. The contactless reader usually has area limited reach in order to prevent any interference with other devices, to lower energetic demands for creation of contactless field and to reduce safety risks. A solution which can phase a payment communication process into some interrupted phases is required. However, until now no procedures and methods meeting this demand are known.

A solution in which a contactless payment card is adapted also for a contact connection with the terminal is used. In such a configuration most of the payments are realized via contactless link between a payment card and a terminal during which the payment card does not wait for a response from the payment processor. To achieve bidirectional communication between the card and the payment processor server it is necessary for the card to be in contact connection with the terminal regularly, for instance in every tenth payment. Then the card receives instructions from the payment processor and executes them. This configuration lowers the user´s comfort and above all it demands contact interface of the payment card so it

is not applicable for payments that use payment cards within a mobile communication device. It is not possible to require for the different mobile communication devices, e.g. mobile phones to be connected with the POS terminal in a contact way.

BACKGROUND TO INVENTION

The disadvantages mentioned above are eliminated significantly by a method of a contactless payment transaction, in particular with the use of contactless payment means which includes a method by which after the reset of the card, the card receives payment data from the payment terminal. Based on these data a payment file is created and electronically signed, mainly in the form of ARQC. This payment file is sent via a link between the card and the payment terminal to the payment processor, subsequently the card receives back a response file from a processor, mainly in the form of ARPC, which includes even data about the original payment file in an encoded form. The card will process and decode the response file and consequently decides, defines and sends back an affirmative or negative statement towards the payment, mainly in the TC or AAC form according to this invention to the terminal . The subject matter of this invention is in the fact that during procession of one payment transaction, the communication link between the card and the terminal is interrupted. This interruption may arise basically immediately after the payment file is sent from the card into the terminal. The initial reception of data from the terminal, generation of a payment file in the form of ARQC and its sending into the terminal lasts approximately some milliseconds and it is realizable during a comfortable placement of the card near to the terminal´s reader. The response file from the payment processor is received by the card after the original communication link between the card and the terminal is interrupted. The two phases of the payment transaction processing and communication mentioned are divided by the card´s reset, while in the second phase the data created on the card before the interruption of the communication link between the card and the terminal are used. The new reset of the card during one payment transaction is induced by the reestablishment of the communication link.

The above mentioned communication mechanism can be realized in a safe way and at the same time with little interventions into common EMV (**E**uropay, **M**asterCard, **V**ISA) procedures in such a way that an electronically signed payment file, in particular in the form of ARQC is stored into the memory of the card whereas the payment file is stored in a memory for at least until the time of receiving and proceeding a particular answering file from a

payment processor, mainly as ARPC. Storage of a payment file, in particular as ARQC is an essential feature of the submitted solution since it allows to divide the process of payment transaction into phases in the way that interruption and procedure leading to the second phase do not elicit cancellation and closing of the in progress payment transaction.

Card decodes the received answering file, gains information about a payment file which was used by a payment processor during creation of the answering file. ARQC payment file is encoded in an answering file where other instructions and scripts for the card can be stored. The card compares the originally created and stored payment file to a payment file included in answering file, subsequently the card creates declined or accepted statement to the payment. Accepting statement to the payment is on the card conditioned by equality of originally created and on the card stored payment file with a payment file generated from decoded answering file. It means that a card, in the second processing phase besides other operations also compares the stored ARQC file with the ARQC file, which served as a base of created ARPC at a payment processor.

After receiving an answering file, terminal requires a reconnection of a communication link of the card and the terminal. After reestablishment of a communication link of the card and the terminal, card requires from the terminal to send again payment data in a form of CDOL (Card Risk Management Data Object List) which are, compared to original CDOL supplemented with an answer from a payment processor.

It is advantageous if a payment card is included in a mobile communication device, such as a mobile phone. From the point of view of possible expansion of such payment means it is suitable if the payment card is located in a memory card of the micro SD or mini SD or SD type since mobile phones commonly have slots to enter broadening memory cards.

In existing one-phase communication system during payment transaction the backward communication from the payment processor towards the card was always realized through the same communication channel as was used when sending the payment file to the payment processor. The new method presented with two phases enables to divide these phases not only from the time but also from the hardware point of view. A different communication path can be used for transfer of answering file than was used for transfer of payment file. It can be a connection via a mobile communication network to which mobile communication device encompassing the card is logged. The mobile communication network is used for sending of the answering file and the answering file enters the card through the mobile phone, which receives it in the SMS format. This can happen after the terminal received the answering file, but when the communication link between the terminal and the card was not reestablished in

the preset time limit. Then the terminal sends information on this status to the payment processor and the one organizes sending of the answering file into the card in a different way.

It is suitable that in case the same communication path via the POS terminal is used, this terminal logs to the card after receiving the answering file from the payment processor as a terminal with an identification that is different from the payment terminal identification in the phase when the payment file was sent to the payment processor. Basically it means that the terminal with different identification prefix gives the card a signal that it tries to connect as a postprocess terminal in order to finish the already started payment transaction. In this kind of configuration the terminal keeps the answering file as a preparation for reestablishment of the communication link with the card.

The disadvantages mentioned in the present technology status are eliminated significantly also by a method of contactless payment transaction, especially with the usage of contactless payment device encompassing a payment card, a terminal, a connection between the terminal and the payment processor according to this invention. The subject matter of this invention is also in the fact that the payment card is equipped with a memory for storage of the payment file, favorably a payment file in a form of ARQC, where the payment file is stored in the memory even after the card is reset when the communication link between the card and the terminal is ended. The terminal is equipped with a memory for temporary storage of answering file, mainly in the form of ARPC and is adjusted to the change of its identification data after the answering file is received. From the point of reaching required security view it is necessary that the card´s memory for the storage of payment file is in the form of a secure element.

In advantageous configuration, the system can be set in such a way that the payment card is within the mobile communication device, preferably on a memory card of the micro SD or mini SD or SD form and in which the memory card encompasses a communication element for the connection with the terminal. By doing this an update of the mobile phone is reached and not only for the function of the payment card carrier, or carrier of various payment cards respectively, but also for the creation of the communication channel between the mobile phone and the terminal. This communication will run mainly in accordance with the NFC standard.

DESCRIPTION OF DRAWINGS

The invention is described in more details on the figures 1 to 5 where figure 1 shows an algorithm of existing method and connection for electronic payment transactions. The figure 2

shows an algorithm with two separable phases of processing an electronic payment application.

The figure 3 represents a system connection scheme for a contactless, direct debit transaction over a mobile phone equipped with a payment card on an inserted memory card having an antenna in the first phase, so in pre-processing. The course of orders and a flow of files is shown in from the top downward order.

In the figure 4 there is a connection scheme relating to a scheme according to the figure 3 where shown is the second phase post-processing with the transfer on the card via a terminal. The course of orders and a flow of files is shown in from the top downward order.

In the figure 5 there is a connection scheme related to the scheme shown on figure 3, however here is shown the second phase, the post-processing in the version of ARPC transfer over SMS message. The course of orders and a flow of files is shown in from the top downward order.

EXAMPLES OF APPLICATION

Example 1

In this example the system contains a mobile communication device 4, a terminal 2 with NFC reader, a payment processor server 5, a connection between the terminal 2 and the payment processor 5 server. The mobile communication device 4 is represented by the e.g. NOKIA 6131 mobile phone. The removable card 1 with a memory of micro SD format is inserted into the slot of the mobile communication device 4. A payment card 1 and also an NFC communication element 7 is located on a removable card 1 with a memory having common standardized dimensions. The card 1 is equipped with a memory for storage of the payment file, with the memory being in the form of a secure element, respectively in a shape of actual domain of the secure element. The ARQC payment file is stored her even after the card 1 is reset. The card´s 1 reset is elicited by re-connection of the card 1 to the terminal 2 after interrupting a communication link 3 between the card 1 and terminal 2 in the first phase of the transaction. The terminal 2 is equipped with a memory for temporary storage of the answering file, in particular in the form of ARPC. The terminal 2 has a variable identification prefix; terminal 2 is adjusted to change its identification data after an answering file is received. In the first phase, the terminal 2 registers as a terminal 2 of the 12 type (POS terminal 2 attended by a salesperson) and in the second phase as a terminal 2 of the 12tc2 type or possibly of the 27 type (Post_Process_Terminal). The change of the terminal´s type serves

for correct matching of communicated messages, in principle it can be a new type number of the terminal, e.g. 27. In other case, when it will be problematic to introduce new type number of the terminal into existing processing systems, the same type number 12 and different terminal capability can be used, here it is expressed as 12tc2 = 12 with different tc – terminal capability. Terminal 2 has a memory to store an answering file ARPC as a preparation for realization of the reconnection of the communication link 3 with a card 1.

Data about a required payment which include an amount, currency and a date are prepared in the terminal 2. These are included in CDOL1 data (Card Risk Management Data Object List). The user applies his mobile phone to the terminal 2 reader. After the communication link 3 is created, the terminal 2 asks the card 1 for a statement. On the basis of the received data, the card 1 will create a payment file in the form of the ARQC cryptogram. This file is encoded by electronic signature of the card 1. During the originally created communication link 3 a payment file ARQC is transferred into a terminal 2. After its creation, the ARQC payment file is stored in the secure element on the card 1. After transfer of the ARQC payment file into the terminal 2, basically it does not matter if the mobile phone is moved away from the terminal´s 2 reader or not. It is supposed that the phone will be moved away since the mobile phone will be held by the user's hand during the whole payment transaction. The mobile phone will be placed near to the terminal´s 2 reader at the request of the terminal 2, or actually at the request of an attendant who monitores the whole course of the payment transaction. After the first placement, the user waits for another request for placement. The communication link 3 between the card 1 and the terminal 2 is disconnected when one payment transaction is in progress.

Meanwhile, the ARQC payment file is sent from the terminal 2 to the payment processor 5. The payment processor processes it, evaluates it and together with possible other instructions encodes the ARQC payment file into an answering file in the form of the ARPC cryptogram. This file encompasses encoded data about the ARQC payment file. The ARPC answering file is received by the card 1 from a payment processor 5 after the original communication link 3 between the card 1 and terminal 2 is interrupted. This interruption contains a time element for the moment which separates the first and the second phase of the payment transaction processing. From the card´s 1 point of view these two are phases separated by the card 1 being reset, while the data created on the card during the first phase are used in the second phase.

The ARQC payment file is stored in the card´s 1 memory at least until the moment when the particular ARPC answering file from the payment processor 5 is received and

processed. The card 1 decodes the received ARPC answering file, gains information about ARQC payment file which was used by a payment processor 5 when creating ARPC answering file. Next, the card 1 compares the originally created and stored ARQC payment file with ARQC payment file which is included in the ARPC answering file. After this comparison the card 1 can make decision on its statement concerning the payment in process. Subsequently, the card 1 creates a statement of acceptance or rejection of the payment in TC or AAC form. Statement of acceptance is created on the card 1 under necessary condition when the originally created and on the card 1 stored ARQC payment file is identical to ARQC payment file included in the ARPC answering file.

The connection as described in this example also offers more possibilities of the way how the ARPC answering file is transferred to the card 1. If the terminal 2 reports to the payment processor 5 that the user did not place his mobile phone near to the terminal´s 2 reader for the second time, the payment processor 5 will try to send ARPC as SMS data to the phone number assigned to this particular payment card 1. In the mobile phone, the received SMS is analyzed as data relevant to the inserted micro SD card and initializes launch of its own generic, basically virtual POS terminal 2. The SMS message contains information about terminal 2 belonging to the payment processor 5 with prefix 17 (PostProcessingTerminal 2 belonging to the payment processor 5).

Example 2

The process of an on-line payment transaction is realized in two steps – preprocessing and postprocessing. A contactless application fulfilling e.g. PAYPASS and PAYWAVE specification can be used as a payment application. There are two separate applications on the card 1 – PAYPASS/PAYWAVE and PAYPASS/PAYWAVE_POSTPROCESS. Applications are located in one Secure Domain and are EMV compatible while they share at least three common variables (Data Element): Off-line Counter, Application Transaction Counter (ATC), Last Online Application Transaction Counter (LATC). The application PAYPASS/PAYWAVE temporary stores the ARQC value, which it provides later in POSTPROCESS to PAYPASS/PAYWAVE_POSTPROCESS application so this one did not have to count it once again, by which time is saved. According to this invention a new type of terminal 2 is introduced: Terminal_Type=27 (POST PROCESS TERMINAL 2).

The presented solution enables to place the mobile phone near the terminal 2 twice. The first time, a request for an on-line authorization is generated and after the second touch, the information from the payment processor 5 is entered into the payment application. If the

user does not place his mobile phone for the second time but relevant data or a script are within the answer, the terminal 2 reports to the payment processor 5 that the answer was not delivered and the payment processor 5 will try to deliver it once more into the mobile phone via SMS – in case the SMS RESPONSE service is activated. In case the user has this service, he can place his mobile phone near to the terminal´s 2 reader only once also willingly and regularly. The service is activated during the first installation of GUI when GUI reports to the payment processor 5 via SMS that SMS REPORT was enabled.

The service is disabled automatically in case when the payment processor 5, after he sends SMS RESOPONSE, does not receive a confirmation of its reception in three consecutive on-line payments. The client pays on-line 3 times consecutively and/or GUI was not activated or his mobile phone was changed for a type not supporting such a service. After deactivation the client will receive an SMS saying that he must either re-activate the service over GUI or use the two-touch method of the payment transaction process.

Also in this example the PreProcessing represents a common on-line contactless operation realized at the first placement of the card 1, herein a mobile phone to the terminal´s 2 reader. During preprocessing, the terminal 2 presents itself as e.g. Terminal_type=12 (POS terminal 2 attended by a salesperson). The terminal 2 sends a request for an on-line authorization to the payment processor 5 (authorized server of the bank which issued the payment card 1). The result of the preprocessing is, besides others, a Response_code and a Script from the payment processor.

The user starts the GUI payment application in the mobile phone. The application asks for a password. If the password is applied, then the EMBEDDED POS TERMINAL uses the password to get the PIN code. The PIN code is stored in a separate application in the Secure Element. The EMBEDDED POS TERMINAL verifies the PIN in the PAYPASS/PAYWAVE application and if it is valid, it configures the payment application in such a way that during the transaction no additional verification by PIN over PIN Entry Device (PED) on an external POS terminal 2 is required. A PIN OVER PASSWORD platform technology is defined by this configuration. If the user starts the payment application but does not enter a password and terminal 2 requires a PIN verification, it is necessary to enter PIN over PED or to place FOB (external data carrier) near to the reader and send it for verification to the payment processor 5. If the phone is not equipped with GUI payment application and the terminal 2 requires PIN verification, the verification will be done on-line at the payment processor 5.

The terminal 2 sends Card Risk Management Data Object List (CDOL1) and 1st GENERATE AC command to the card 1. The card 1 calculates the ARQC. If the risk

management of the terminal 2 requires PIN and no password was entered over GUI, the terminal 2 requires PIN to be entered on the Pin Entry Device (PED) and in this step it verifies the PIN on-line. The terminal 2 sends the calculated ARQC cryptogram as a request for on-line authorization to the payment processor 5. The payment processor 5 sends back the answer (ARPC cryptogram) supplemented for a Response_code and a Script.

The postprocessing runs during the second placement of the card near to the terminal 2 when the terminal 2 sends the Response_code and the Script to the card 1 for next processing as follows:

1. After the terminal 2 receives the ARPC cryptogram from the payment processor (end of preprocessing), the terminal asks the user to place the card 1, the mobile phone near to the contactless reader of the terminal again.
2. After placing the card 1, the terminal 2 activates PAYPASS/PAYWAVE_POSTPROCESS and presents itself not as a Terminal_type=12 but as a Terminal_type=27 (PostProcessingTerminal attended by a salesperson), respectively as a Terminal_type=12 tc2
3. The card recognizes this type of the terminal (it is on the two-touch transaction processing), asks the terminal 2 for CDOL2 data to calculate 2nd GENERATE AC.
4. CDOL2 from the terminal 2 must encompass, besides other data, a Response_code from the payment processor.
5. The terminal 2 sends the Script into the card 1.
6. During calculation the ARQC, which was temporary stored during the preprocessing, is used.
7. Card sends the calculated TC/AAC to the terminal 2.

If the user does not place his mobile phone, the mobile communication device 4, to the reader for the second time, the terminal will report to the payment processor 5 that message delivery was unsuccessful. The payment processor will try to send the ARPC as SMS data to the phone number in which the SD card 1 is inserted (the processor 5 gains and remembers this number during activation of SMS Response from the activating SMS from GUI). The push SMS technology records the received SMS and after finding out that it involves relevant data for the SD card, it runs the GENERIC POS TERMINAL. Besides other information, the SMS data must include also information about Terminal_type=17 (PostProcessing Terminal 2 belonging to a financial institution). The GENERIC POS TERMINAL reads configuration data of the default terminal on the secure element (the terminal 2 belonging to the payment processor 5 or to the Payment processor cooperating with the processor 5 of the payment).

Subsequently, the EMBEDDED POS TERMINAL starts PAYPASS/PAYWAVE_POSTPROCESS and presents itself as Terminal_type=17. The card 1 recognizes such type of the terminal (it is on the two-touch transaction processing platform), asks the terminal 2 for CDOL2 data (containing ARPC) to calculate 2nd GENERATE AC. The terminal 2 sends a Script into the card 1. The ARQC, which was temporary stored during preprocessing, is used for calculation later on. The card 1 sends the calculated TC/AAC as an answer into the terminal 2. The terminal 2 encodes the answer and stores it into the memory from where GUI takes it over and sends its as an answer to the HOST of the processor 5 of the payment whereas it recognizes the phone number from the received SMS RESPONSE.

When the card 1 receives the ARPC from the payment processor 5, it sets the LATC, which enables it to realize other "n" (unlimited) off-line payments and it does not matter whether it is over SMS Response or over second touch. If the user refuses the second touch at the two-touch platform and/or SMS Response is not activated, he will not be able to realize off-line payments. However, he can still pay but only with on-line authorization at the payment processor 5. The off-line transactions will be permitted after ARPC (response) is received correctly from the payment processor 5. Then he will be allowed again to pay unlimited number of times, naturally under the condition that there is enough off-line money on his card.

INDUSTRIAL APPLICABILITY

Industrial applicability is obvious. According to this invention, it is possible to create and use systems for electronic payment applications at which a payment transaction is divided into two phases that enables interruption of a communication link between a card and a terminal.

LIST OF RELATED SYMBOLS:

1- a card

2- a payment terminal

3- a communication link

4- a mobile communication device

5- a payment processor

6- a communication path

7- a communication element

POS - point of sale

AAC - Application Authentication Cryptogram

ARQC - Authorization Request Cryptogram

ARPC - Authorization Response Cryptogram

CDOL - Card Risk Management Data Object List

TC - Transaction Certificate

POS 12 - point of sale attended by a salesman

POS 12tc2 - point of sale attended by a salesman in post process – with different terminal capability

EMV - Europay, MasterCard, VISA

PATENT CLAIMS

1. A method of electronic payment transaction particularly with the use of a contactless payment means including a procedure during which a payment file, especially in the form of ARQC, is created by the card (1) and electronically signed on the card (1) with the usage of payment data, mainly in the CDOL form, that are received from the payment terminal (2) after the reset of the card (1), the payment file is sent over the card´s (1) link with the payment terminal (2) to the processor (5), and subsequently the card (1) receives back the answering file from the processor (5), which is mainly of the ARPC type and which in encoded form contains data about the payment file, the card (1) processes the answering file and followingly defines and sends to the terminal (2) statement of acceptance or rejection of a payment mainly in the TC or AAC form, is characterised by the fact that during processing of a payment transaction, the communication link (3) between the card (1) and the terminal (2) is interrupted and, after the communication link (3) between the card (1) and the terminal (2) is interrupted, an answering file from the payment processor (5) is received on the card (1); wherein two phases of payment transaction processing are separated by a reset of the payment card, such that in the second phase data created on the card (1) before the interruption of the communication link (3) are used.

2. A method of electronic payment transaction according to the claim 1 is characterised by the fact that the electronically signed payment file, mainly in the form of ARQC, is stored in the card´s (1) memory at least until the corresponding answering file is received from the payment processor (5), mainly in the form of ARPC, the card (1) decodes the received answering file and gains information about the payment file that was used to create the answering file and subsequently the card (1) creates a statement of acceptance or rejection of the payment.

3. A method of electronic payment transaction according to the claim 2 is characterised by the fact that the card (1) compares an originally created payment file that is stored on the card (1) to a payment file that is included in the answering file.

4. A method of electronic payment transaction according to any of the claims 1 to 3 is characterised by the fact that the approving statement towards the payment is created on the card (1) under condition that the originally created and on the

card (1) stored payment file, is identical to the payment file which is within the answering file.

5. A method of electronic payment transaction according to any of the claims 1 to 4 is characterised by the fact that after receiving the answering file, the terminal (2) requires restoration of the communication link (3) between the card (1) and the terminal (2), wherein after the communication link (3) between the card (1) and the terminal (2) is restored, the card (2) asks the terminal (2) to resend payment data supplemented with an answer from the payment processor (5).

6. A method of electronic payment transaction according to any of the claims 1 to 5 is characterised by the fact that the card (1) is included in removable memory card for a mobile communication device (4), favorably the microSD or miniSD or SD type.

7. A method of electronic payment transaction according to any of the claims 1 or 6 is characterised by the fact that a communication path (6) for the transfer of the answering file is different from a communication path (3) used for the payment file transfer between the card (1) and the terminal (2).

8. A method of electronic payment transaction according to any of the claims 1 to 7 is characterised by the fact that after receiving an answering file from the payment processor (5), the terminal (2) in the second phase contacts the card (1) as a terminal (2) with an identification that is different from an identification of the payment terminal (2) in the phase of sending the payment file to the payment processor (5).

9. A method of electronic payment transaction according to the claim 8 is characterised by the fact that the terminal (2) stores the answering file in preparation for restoring the communication link (3) with the card (1).

10. A method of electronic payment transaction according to any of the claims 1 to 9 is characterised by the fact that the mobile communication network is used to send the answering file and the answering file is received by the card (1) over a mobile communication device (4) that receives the message in SMS format.

11. A system of electronic payment transaction particularly with the use of contactless payment means including a payment card (1) in mobile communication device (4), a

terminal (2), a connection between a terminal (2) and a payment processor (5) is characterised by the fact that the payment card (1) includes a memory having a payment file stored therein, wherein the payment file is also stored in the memory after a reset of the card (1) that follows after the interruption of a communication link (3) of the card (1) and the terminal (2), and wherein the terminal (2) includes the memory for temporary storage of the answering file which is mainly in the form ARPC and the terminal (2) is adjusted for the change of its registry identification data after the answering file is received.

12. A contactless payment applications system according to the claim 11 is characterised by the fact that the card´s (1) memory for the storage of the payment file is a secure element.

13. A contactless payment applications system according to the claim 11 or 12 is characterised by the fact that the payment card (1) is included in a removable memory card for a mobile communication device (4), preferably the microSD or miniSD or SD type.

14. A contactless payment applications system according to any of the claims 11 to 13 is characterised by the fact that the payment card (1) includes a contactless communication element (7) for the communication with the terminal (2).

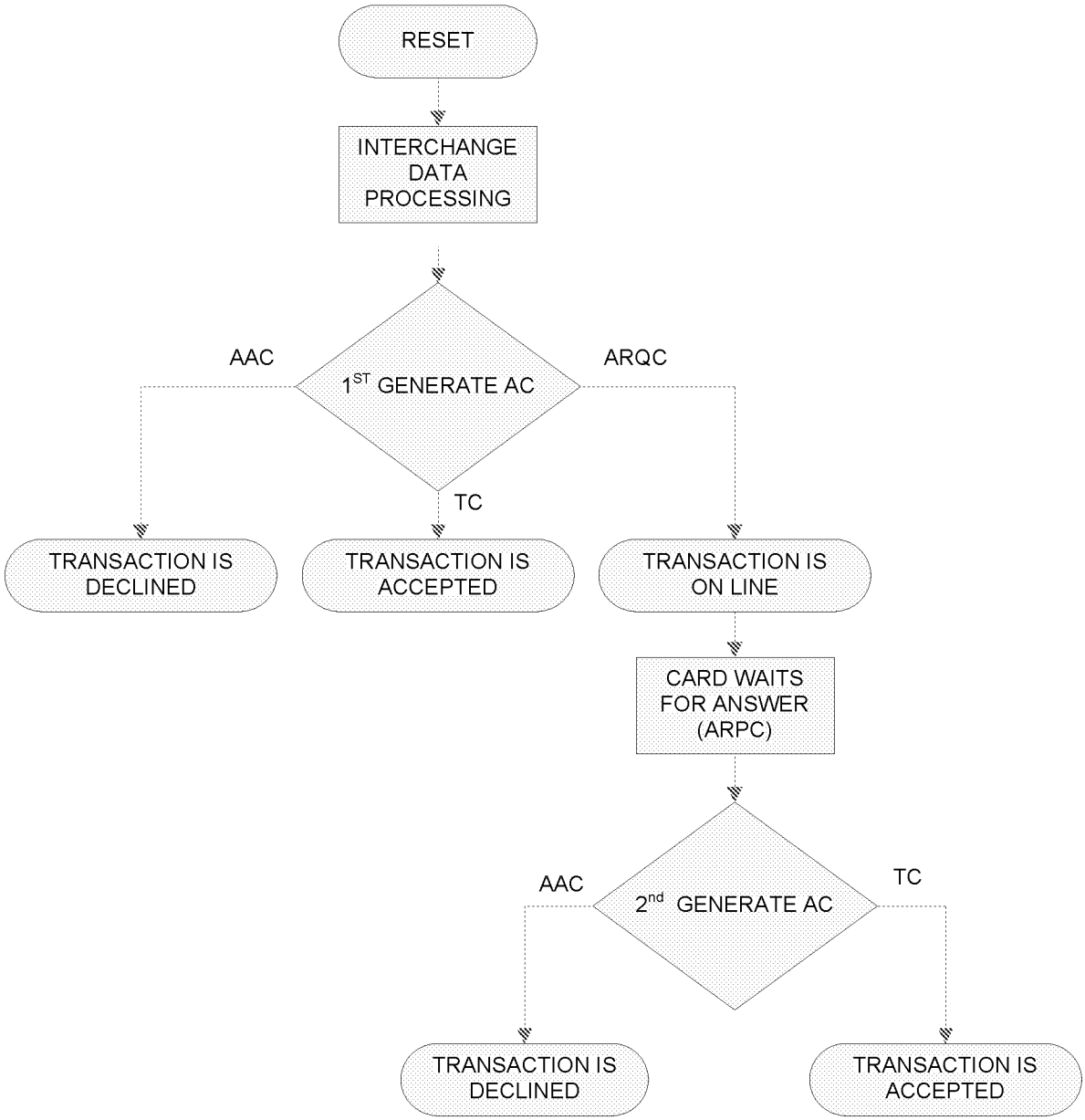
RESET
INTERCHANGE DATA PROCESSING
AAC
1ST GENERATE AC
ARQC
TC
TRANSACTION IS DECLINED
TRANSACTION IS ACCEPTED
TRANSACTION IS ON LINE
CARD WAITS FOR ANSWER (ARPC)
AAC
2nd GENERATE AC
TC
TRANSACTION IS DECLINED
TRANSACTION IS ACCEPTED

Fig. 1

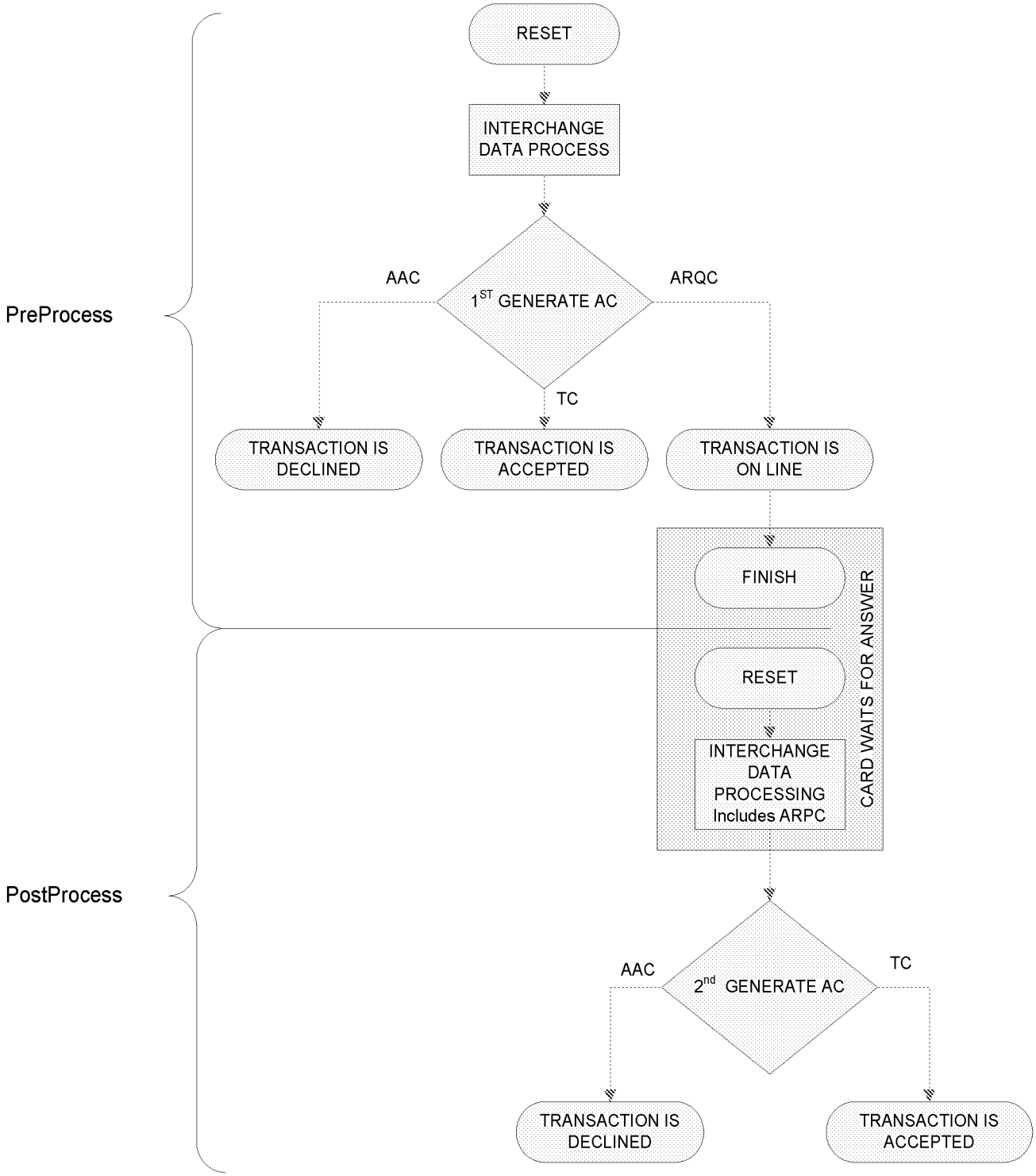
PreProcess
RESET
INTERCHANGE DATA PROCESS
1ST GENERATE AC
AAC
ARQC
TC
TRANSACTION IS DECLINED
TRANSACTION IS ACCEPTED
TRANSACTION IS ON LINE
CARD WAITS FOR ANSWER
FINISH
RESET
INTERCHANGE DATA PROCESSING Includes ARPC
PostProcess
2nd GENERATE AC
AAC
TC
TRANSACTION IS DECLINED
TRANSACTION IS ACCEPTED

Fig. 2

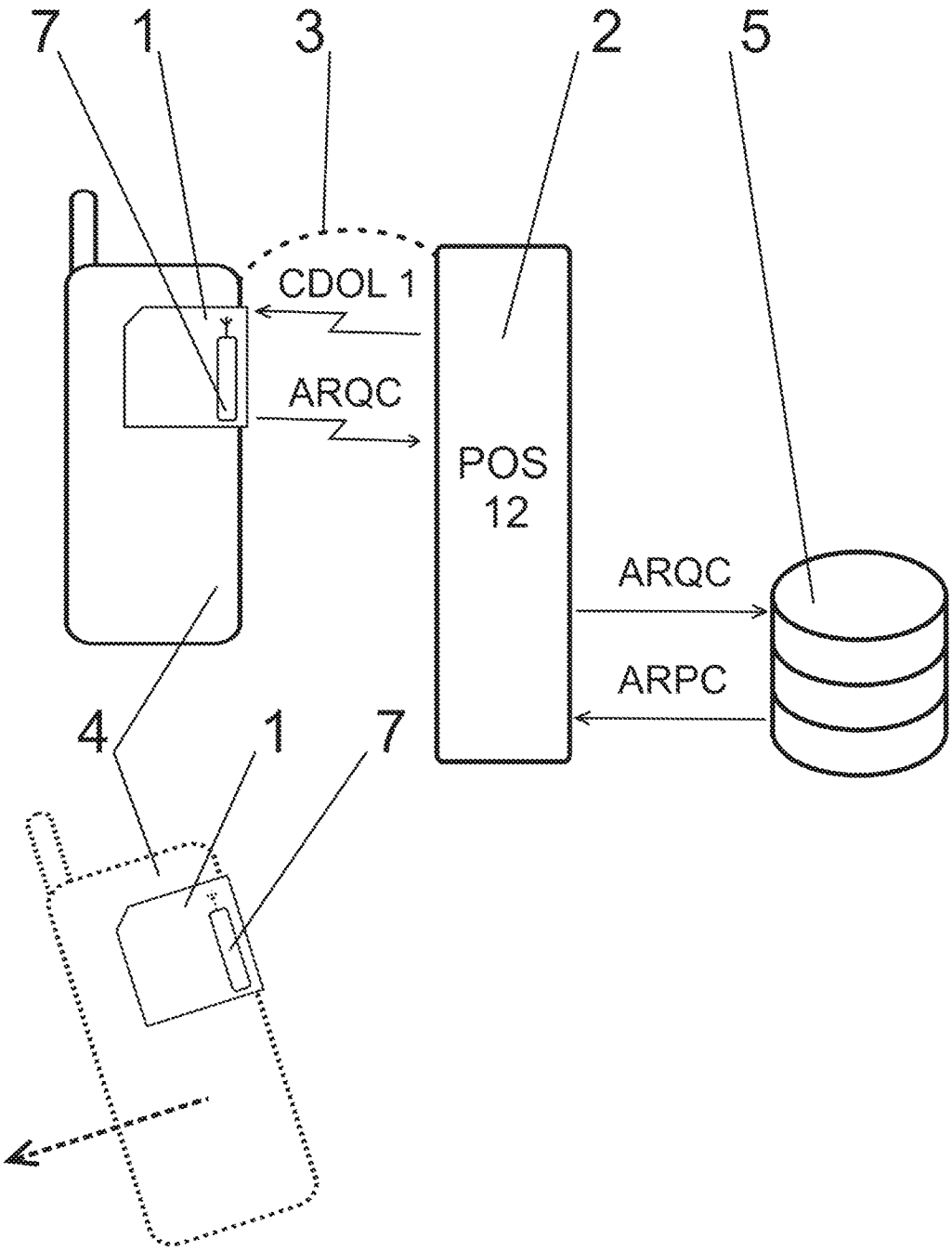

Fig. 3

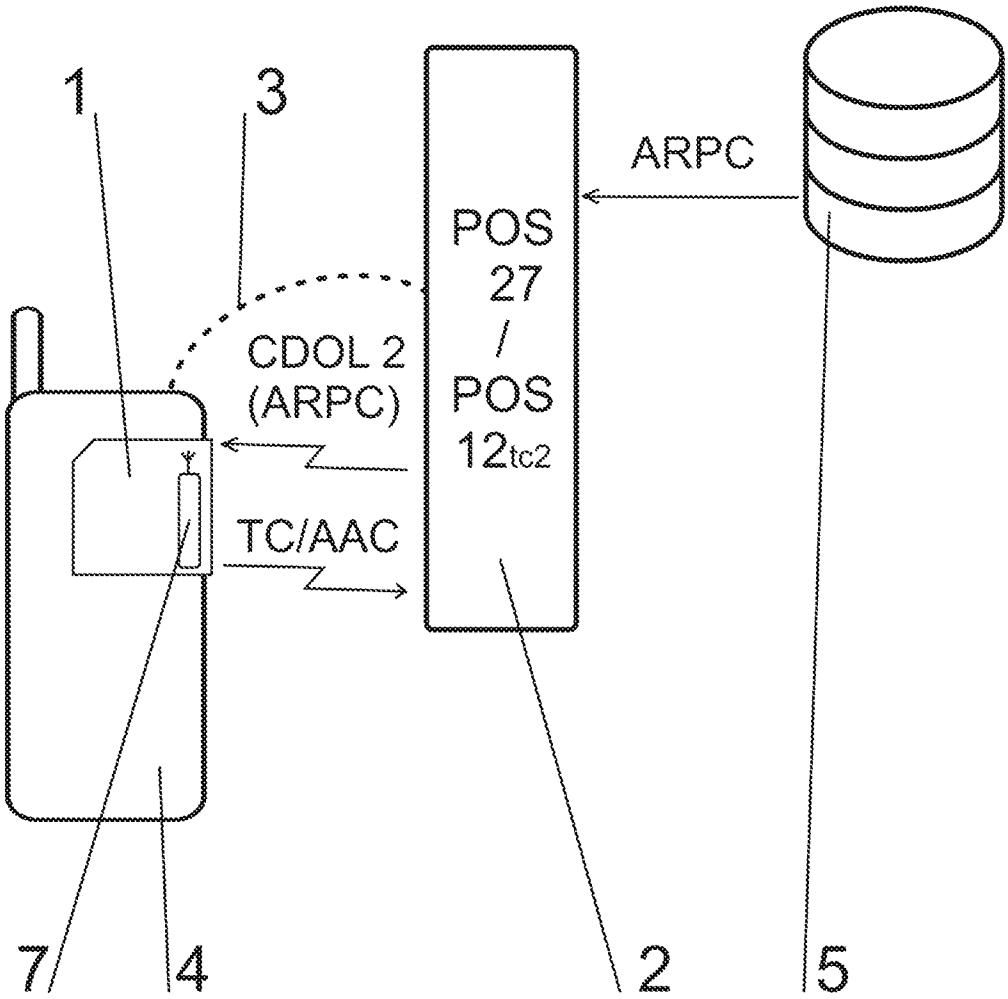

Fig. 4

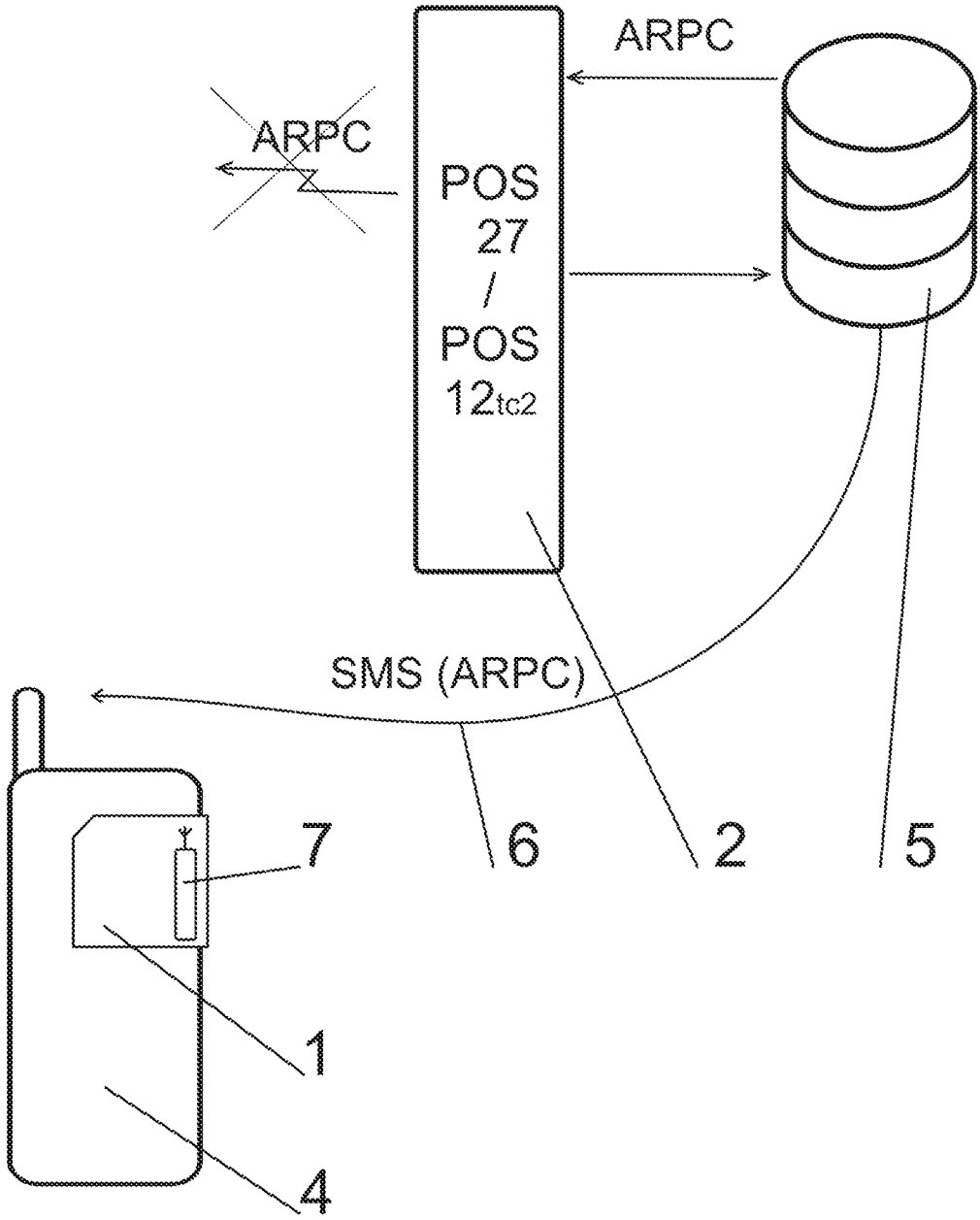

Fig. 5