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

(19) World Intellectual Property Organization
International Bureau

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

WIPO | PCT

(10) International Publication Number
WO 2012/140625 A1

(51) International Patent Classification:
G06Q 20/32 (2012.01)

(21) International Application Number:
PCT/IB2012/051849

(22) International Filing Date:
13 April 2012 (13.04.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PP50017-2011 13 April 2011 (13.04.2011) SK

(71) Applicant *(for all designated States except US)*: **Logomotion, s.r.o.** [SK/SK]; Winterova 15, 921 01 Piešťany (SK).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **HUBINÁK, Emil** [SK/SK]; JUDr. Emil Hubinák, Beethovenova 4, 921 01 Piešťany (SK). **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**; Kancelária pre patenty a známky, 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, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

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))*

Published:

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

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(54) **Title**: PAYMENT CARD, CASHLESS PAYMENT METHOD

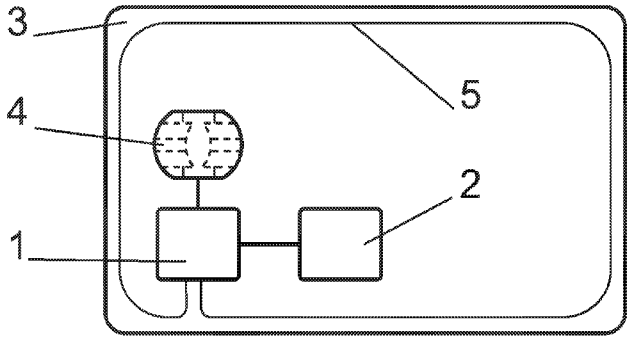

Fig. 2

(57) **Abstract**: The payment card, apart from a chip with the common payment card unit, also contains a second chip with an indifferent POS payment terminal, which becomes a specific POS terminal on behalf of the payments recipient after connection with the reader of the payments recipient. These two chips on the payment card are connected in a contact way. The reader contains the common POS terminals identification data which are sent 10 to the payment card of the customer, where they are moved to the second chip for the configuration of the POS terminal. Then on the payment card, the payment-terminal application is realized as if it were a common POS with the inserted card in a contact way, using the payment account data from the first chip. The payment cryptogram generated in the other chip on the payment card is sent to the reader for payment processing on 15 behalf of the reader-holder (merchant).

WO 2012/140625 A1

Payment card, cashless payment method

Technology

The solution refers to a payment card, on which there can run a POS (Point of Sale) terminal´s payment terminal application. The payment card can be used in common payment processes according to existing configurations and in addition it can also form a POS terminal. The solution also describes the cashless payment method based on this kind of payment card.

Present technology

There are known payment cards which besides the basic function fulfill even additional tasks. For instance, according to patents and publications ES 2 153 324, EP 0387366A1 the card contains two independent chips for usage in different payment systems, e.g. during usage in different countries. The chips in these solutions are not interconnected. There is also known a solution according US 201/0065628 A1 with multifunctional configuration; however this one only accumulates various existing functionalities of different cards of the user.

The solution according EP 0402182 A1 describes a removable element of the payment card which has its independent functionality. This element is not interconnected with the basic chip of the card.

The existing POS terminals, widespread in business premises, are characterized by a stable structure, which, besides other things, encompasses a communication channel connected to a payment processing center, printer, encryption key, display, card reader (sometimes card readers of different forms) and also a keyboard for PIN code entering. This technical configuration requires certain space and it is relatively expensive. The known realizations of POS terminals are intended especially for stable sale locations in physical shops, where the high costs of purchase, installation and operation of POS terminals are compensated by the correspondingly high purchase turnovers.

Some published patents describe divided POS terminals in which there is only its operating part directly at the payment location in the shop; it is connected to the remaining part located at a different location in the shop. The known solutions and published patents do not offer simple instructions how to create a cheap, non-complicated and possibly also even portable POS payment terminal, the essential parts of which are located directly on the payment card and the parts of which can generate payment cryptograms according to existing standards, especially EMV standards.

All existing solutions require relatively complicated installation and encompass many output and input devices, a situation that increases their price. Until now there are not known any solutions that would be characterized by simplicity, high security and that would also be portable and usable even in small shops such as e.g.. newsstands or portable stands, e.g. selling fast food. The solution according to this application enables to do that.

An important requirement is for the new solution to be compatible with the structures of existing payment data on the payment processor level. A configuration which would require a completely new hierarchy or new authorization procedures in general obviously would not be implementable in reality.

Subject matter of the invention

The deficiencies mentioned are to a great extent eliminated by a payment card which includes two chips according to this solution. One chip, which contains a Secure Element with the payment card application, is connected with the common contact field on the payment card and/or with a contactless communications channel,and possibly even with an antenna on the payment card. A second chip, which contains a Secure Element with a POS terminal application, is connected to the first chip by means of a contact connection on the payment card. The subject matter of this solution thus lies in the fact that the payment card has two chips with Secure Element and a chip with a payment card unit is connected to a chip with a payment terminal unit in a contact way.

The core feature of the solution presented is that the POS payment terminal chip can be located on the payment card; this chip is connected basically

permanently in a contact way to the chip with the payment card unit. The configuration presented unites a payment card and a virtual POS terminal´s kernel into one carrier. The mutual interconnection of chips with Secure Elements can be done directly or through a circuit and/or computing module. Even a contactless communication channel antenna or a contact field can be connected to this circuit and/or computing module. The second Secure Element contains a payment terminal has all software applications and possibly even configuration data necessary for the run of the payment terminal stored within it. The payment card with the second Secure element will not have the outer appearance of the POS terminal as this one is perceived by a paying customer in a physical shop. In most cases, the run of the POS payment terminal in the payment card Secure Element will first run in the form of generic and temporarily not configured payment terminal and only subsequently the configuration data will be loaded in the interaction with the reader or another counter device. The Secure Element will contain POS payment terminal in such a way that it encompasses an independent unit with payment-terminal application and in preferable configuration even there will be minimally a memory controller unit and download management unit.

In this configuration the POS terminal will communicate with the payment card unit in a way as if this one was inserted in the contact reader of the payment card, however in reality this connection is stable due to contact connection on the payment card. The first Secure Element will contain a payment card in the way used until now by having a payment data unit, which however do not have to be exclusively in the EMV standard form. The payment card can be in a form, size of a standard card, e.g. ID-1 in accordance with ISO/IEC 7810 (85.60 x 53.98 mm) with electric connection according ISO 7816.

The payment card according to this solution will cooperate even with a common POS terminal reader; in this case only the common functionality of the payment card is used. The cooperation with a reader according to this solution, during which the reader will ensure that the POS payment terminal on the payment card is configured with current data. The reader can belong to the merchant or it can be only held by the merchant; it contains a secure memory with identification data, which above all encompasses data that are necessary for configuration and allocation of the POS payment terminal to the corresponding merchant´s bank

account. The payment card will encompass generic payment terminal, which will become a specific payment terminal with unique identity only after it is connected to the reader. The reader will provide the temporarily created connection with a unique identification of the user for the benefit of whom the payment should be made.

The really functional POS terminal will come into existence from a temporary connection between a reader owned or held by a merchant and a payment card according to this solution. The second SE on the payment card according to this solution is configured to correspond with the merchant by a temporary connection between the payment card and the reader. The connection is called temporary because after the payment process is ended, the parts can be separated, the communication channel is interrupted and new connections between the reader and a different payment card can be created repeatedly. Naturally, the repeated connection between the beforehand used payment card and the reader is not excluded. It is necessary to understand the temporality of the connection as a time interval in principle limited to one specific payment process (for example, a consumer making one check-out at the merchant´s). This connection interval refers to a connection that takes place between the start and the end of the payment process. The possibility to always pair a new element on the side of the merchant and a new element on the side of the paying user presents a solution, in which a POS terminal on the paying user´s payment card can always be created, with the POS terminal having the identity of the corresponding merchant – recipient of the payment.

According to outside appearances, from the merchant´s point of view the reader in this case behaves as a POS payment terminal and the merchant will commonly call it a POS terminal; however from the structure and course of applications´ point of view, the reader is only a necessary but not a sufficient part of the entire POS payment terminal functionality. Therefore, the term reader must be understood generally as a part of the terminal, which is basically associated with a merchant, or with a particular point of sales and this part of a terminal ensures correct routing of cashless payments made by users. The device described here as a reader has an important configuration task and it contains corresponding hardware and software elements to fulfill this task. The reader is therefore necessary to understand any device, which cooperates with a credit card as described above.

In the overall configuration, the reader can have two basic functions - carrying the identity of a POS terminal and a means for entering the value of the payment. In principle, even a narrower hardware version is possible, during which the value of the payment is entered over the keyboard on the payment card, however, this kind of version may not be comfortable for the merchant, because he would have to control the paying customer´s payment card or he would have to trust that the customer entered the correct payment amount into the payment terminal application. The inserted value could be displayed even on a display on the payment card or on the reader´s display so it could be checked by the merchant. However, it will be more comfortable, if the amount to be paid is entered over the elements on the merchant´s side. The version described in this paragraph including entering of the amount to be paid over a keyboard on the payment card would not have to fulfill some standards (e.g. EMV) on behavior and operation of the merchant when realizing cashless payment. However in principle it is technically realizable using the principle of the presented solution. Therefore, in suitable configuration the payment card can encompass even a display and a keyboard.

Even in the case the keyboard and display are absent, the payment card can include a payment button, which will be used for the confirmation of the payment by the paying customer.

According to this solution, the reader itself is not capable of realizing payment terminal application with a common payment card and it does not even have to have communication channels for the creation of the connection with the payment processor center (e.g. bank, clearing house etc.) because especially its usage in off-line payments will be important. This enables considerable simplification of the hardware of the device on the side of merchant and by that to increase the number of locations where it will be possible to pay in a cashless form. Only by connecting the reader and the payment card according to this solution will the complete hardware set capable of fulfilling all basic functions of a common POS payment terminal be created.

The important element of the presented solution is the fact that besides the normally included chip with payment card data, the payment card contains also hardware and software elements, so that the set, together with the reader, will be able to run and realize payment terminal application directly on the payment card´s

carrier for specific payments. The payment terminal application forms the core of the cashless payment operation in a process way.

The communication channel for the connection of the payment card with the reader can be a contact one using a contact field on the payment card or it can be contactless e.g. NFC field with an antenna in the payment card´s body.

Thanks to the configuration described it will be possible for the payment recipient to buy only a very simple reader, which will carry the information such as the identity and the terminal´s number, and to this information the account number of the corresponding recipient can be assigned in the payment processor center. This kind of reader will be very small and simple. It can be in the form of a small box with display and keyboard over which the payment recipient will enter the required amount to be paid. The identification data can be stored directly in the corresponding element on the printed circuit of the reader or they can be stored on ICC (integrated circuit card) card or on other carriers like e.g. until now known SAM (Security Authentication Module) cards with cryptographic key.

The customer will connect his payment card to the reader. This can be done in a contact way – by inserting it into the reader´s slot or in case of contactless payment cards, it can be done by taping the payment card to the reader. By tapping it, the NFC communication channel will be created and the reader sends the information on the identity of this temporarily created POS payment terminal to the payment card. In so doing, the identification data can be encrypted using Master Key, which is stored in the Secure Element of the reader. Under the term Secure Element we can understand especially, however not exclusively, a secure memory with necessary interface, which can be in the form of independent chip with a corresponding computing capacity. The Secure Element can be configured in such a way that the data stored on it are not accessible from the outside; however these data can be used as input parameters on the realization of computing operation within Secure Element and only the results of these computing operations, e.g. in the form of cryptograms, are getting out.

After the input data from the reader are read on the payment card, they become the basis for the payment terminal application´s operation. From a general, generic, indifferent terminal a specific POS terminal is created in this way, and this

specific POS terminal is assigned to the corresponding payment recipient in the payment system. This phase is something like preparation for the start of a new one-time POS terminal. Subsequently, during the connection, the payment terminal application e.g. of the EMV type can run in a similar way as it runs in standard POS terminals today. The payment within the payment terminal application runs in such a way as if there was a payment card, the chip of which is in reality firmly connected to the POS terminal´s chip, inserted in the POS terminal in a contact way.

The encryption of the POS terminal´s identification data can be realized using Master Key, which in general can be and mostly even will be different from encryption keys, that are used subsequently by the payment terminal application itself for the creation of the payment cryptogram. The Master Key can originate from e.g. the supplier of the reader´s hardware and the encryption keys of the payment terminal application can be issued by the bank or by the payment processor. The difference of the encryption keys in reality will be conditioned by different requests of individual subjects operating in the payment settlement system.

From the point of view of increasing security even the data concerning the amount of the payment can be encrypted during the transmission from the reader into the payment card. This will decrease the risk of the payment value being lowered over a special application even before the kernel of the payment terminal application is run. However, this kind of change manifests itself at the point of final payment confirmation on the merchant side in the form of displaying paid amount, however in case of inattentiveness and routine approach the merchant would not have to notice the change of the amount.

On the payment card there can be stored several units of independent payment cards that are either in physically separate secure elements or in independent domains of one secure element. In this kind of configuration the payment terminal application can run directly on the payment card while the data on the customer´s payment card are neither sent over an external reader, nor to the internet or other communications network, a situation which has a positive influence on the security of the payment operation.

The reader can be of different appearance besides a small one-purpose box with a keyboard, which directly contains Secure Element with identification data. It

can be also created in such a way that it has an external card reader created within, which preferably is in the classic standard ICC (integrated circuit card) card form. In that case, the sensitive data can be loaded into the chip of this kind of ICC card. The card´s chip also contains even some set memory capacity, which can be suitably used for recording data on realized payment transactions. After the end of the day, the merchant can keep the basic part of the reader in the store, e.g. in the newsstand and take only the ICC card with him. In case he takes the ICC card out of the reader, he can take it to the bank for processing or he can back up the data from it over his computer. In case the merchant has several mobile stands there can also exist several readers combined with one ICC card having identification data of one terminal and one bank account and vice versa one reader can be used subsequently with several ICC cards belonging to different merchants in multiple shifts of one store.

It is advantageous, but not necessary, if the reader has its own interface, e.g. of the USB form for the connection with extending accessories, which enables for the payment data to be printed from the reader, or respectively, over this connector it would be possible to ensure connection to the GPRS modem and similar.

Pictures overview

The invention is described in more detail using the figures 1 to 7.

In the figure 1 there is a scheme of how the different components are connected by means of a circuitry and/or computing module.

The figure 2 depicts a possible different interconnection of chips with Secure Elements. Here the antenna is connected to the first chip which contains the Secure Element with a payment card unit.

The figure 3 shows a payment card as in figure 1 which also has a display and payment button.

In the figure 4 there is a contactless connection between the payment card and the reader.

In the figure 5 there is a contact connection between the payment card and the reader.

In the figure 6 there is a diagram showing the course of the payment illustrating task division between the reader and the payment card with two-tap mode.

In the figure 7 there is a diagram showing the course of the payment illustrating task division between the reader and the payment card with the payment card in the reader mode.

The measures, shape nor proportions of the payment card in relation to the reader are not binding and are selected only with regard to better clarity of the figure.

Realization examples

Example 1

In this example, based on figures 1, 4 and 6, on the merchant's side there is a system having a reader 8 in the shape of a single purpose box. This reader 8 has a numerical keyboard 12, a display 11, its own power source in the form of a rechargeable battery and an NFC communications element with an antenna 5 under the surface of the upper cover. The reader 8 has also a guiding symbol marking showing a user where he should tap his payment card 3. A removable SAM card with a Secure Element 2 is inserted into the reader 8. This Secure Element 2 has the identification of the POS payment terminal and also the Master Key for encryption of communications which were previously downloaded. In a different version of the reader 8, these data can be downloaded directly into a Secure Memory on the reader's 8 printed circuit board.

The payment card 3 as shown in figure 1 has a Secure Element 1 with a common payment card unit as found in common plastic payment cards; it also has a Secure Element 2 which contains a POS terminal unit, a contact field 4 according to the ISO 7816 standard, an antenna 5 and a module 6 with circuitry and/or computing capability. In this example, Secure Element 1 contains a payment card unit associated with one specific payment account of the user. This payment card unit can cooperate with a standard contact POS and standard contactless readers by operating as a standard dual interface card. The power required for operation of the payment card 3 when it operates as a standard dual interface card can be provided

by the electro-magnetic field of the reader 8, just like a standard dual interface card. Similarly, the power required for operation of the payment card 3 with the reader 8 can also be powered in this way, or optionally by means of its own power source, preferably chargeable from the electro-magnetic field of the reader 8.

When the user wishes to pay the merchant, the merchant enters the amount he wants for his goods or service to the reader 8 using the keypad 12. If the user is satisfied with the numeric output shown on the display 11 and considers it to be ok, the merchant presses OK or ENTER on the keypad 12. The identification data of the POS payment terminal and the payment amount are encrypted with the help of the Master Key and prepared for transmission by the NFC communications element of the reader 8. The merchant asks the paying customer to tap his payment card 3 to the reader 8.

Once the NFC communications channel 7 is generated, the encrypted data from the reader 8 are sent from the reader 8 to the payment card 3. On the payment card 3, the data are decrypted. A payment transaction is then made according to the normal EMV standard in Secure Element 2 using the POS terminal data, payment amount and payment account data received from Secure Element 1. The result is encrypted in a payment cryptogram.

The paying customer then taps his payment card 3 a second time to the reader 8. During this second tap, the payment cryptogram is sent to the reader 8. The paying customer then presses OK or ENTER on the reader 8, and the payment cryptogram is storing in the removable SAM module of the reader 8. The figure 3 shows a different option of mutual interconnection of elements on the payment card 3 with the same outer functionality.

Example 2

The solution according to this example is shown on the figures 3, 5 and 7 and it contains a reader 8, which has contacts for the connection with the payment card 3. The payment card 3 has two chips with the first and the second Secure Element 1, 2; on the first Secure Element 1 there are several independent domains with payment cards´ units of various issuers. The second Secure Element 2 is intended for the

operation of the POS applications. At first the POS is an indifferent POS terminal without specific acquirer´s configuration data.

In this example, the payment card 3 is also equipped with a display 10 used to show the amount being paid and also to show simple icons, which inform about the course of payment. The payment card 3 in this example also contains a payment button 9, by which one can express explicitly authorization of the running payment. Since it can be problematic to fulfill the energy requirements of these elements on the payment card 3 only from the reader´s 8 electromagnetic field, the payment card 3 in this example can also have its own source of energy in the form of a flat battery, which will be recharged over the payment card´s 3 contact field 4 during each connection with the reader 8.

The reader 8 has a slot for insertion of an ICC card, which carries the payment acquirer´s POS configuration data. Then the reader 8 itself does not have to be personalized and all payment acquirer´s personalization data will be located on the ICC card, to which they will be transferred by means of existing standard equipment or common equipment with small adjustments. The reader 8 has a common contact interface for the connection with the payment card´s 3 contact field 4. This will make it possible to realize a payment for a benefit of a specific recipient even in someone else´s reader 8 in case the payment acquirer´s ICC card is inserted into the reader 8 during payment.

The merchant as the payment´s recipient inserts the information on the paid amount into the reader 8. This information is transferred into the payment card 3, where it is displayed on the display 10. After checking the amount on the display 8, the customer presses the confirming button 9. After this, the POS payment terminal´s identification data is encrypted and sent along with the amount being paid to the payment card´s 3 chip. The customer can monitor individual phases of the payment over the pictograms that are being displayed on the payment card´s 3 display 10. The display 10 is located on the payment card 3 in such a way so it is readable even when the payment card 3 is inserted into reader 8. According to the selected risk management of the payment card 3 and with regard to the amount being paid, the customer can be asked to enter password, PIN code e.g. over the reader 8.

The reader 8 is not connected on-line to the payment processing centre so the clearing of the payments, which is based on the transmission of payment cryptograms can be as following. The payment recipient takes out the ICC card from the reader 8. This ICC card carries not only configuration data but also stores payment cryptograms. He takes this ICC card into his bank or he himself enters it into the ATM machine, which will be able to recognize type of the ICC card and process the payments stored for the benefit of the recipient's account.

Example 3

In this example, the reader 8 is the same as in Example 1. The payment card 3 of figure 3 also has a display 10 and a button 9.

When the user wishes to pay the merchant, the merchant enters the amount that he wants for his goods or service using the keypad 12 on the reader 8. If the user, by viewing the display 10, is certain that the number put-in is correct, the merchant presses OK or ENTER on the keypad 12. The identification data of the POS payment terminal and the payment amount are encrypted with the help of the Master Key and they are prepared for transmission by the NFC communications element of the reader 8. The merchant asks the paying customer to tap his payment card 3 to the reader 8.

Once the NFC communications channel 7 is generated, the data encrypted in the reader 8 are sent from the reader 8 to the payment card 3. On the payment card 3, the data are decrypted. The amount is displayed on the payment card's 3 display 10. The paying customer confirms his payment by pressing the button 9 on the card 3. A payment transaction is then made according to the normal EMV standard in Secure Element 2 using the POS terminal data, payment amount and payment account data received from Secure Element 1. The result is encrypted in a payment cryptogram.

The paying customer then taps his payment card 3 a second time to the reader 8. During this second tap, the payment cryptogram is sent to the reader 8. The payment cryptogram is stored in the removable SAM module of the reader 8.

The payment card 3 in this example has its own energy source, which may be chargeable from the electro-magnetic field of the reader 8.

Industrial applicability

The industrial usability is obvious. According to this invention, it is possible to industrially manufacture and use payment cards with POS payment terminal, which is configured to a specific terminal only after it is connected to the reader. The readers will be designed above all for small business premises, for mobile stands and similar. The payment card according to this invention will be operating also as a common dual interface card, and as such it will be possible to use it for payments on common POS terminals.

LIST OF RELATED SYMBOLS:

1- Secure Element (the first, with the payment card unit)

2- Secure Element (the second, with the POS unit)

3- payment card

4-contact field

5-antenna element

6-circuitry and/or computing module

7- contactless communication channel

8- reader

9- button

10- payment card display

11- reader display

12- reader keyboard

POS - Point of Sale

ICC - integrated circuit card

EMV - Europay, MasterCard, VISA

SAM - Security Authentication Module

PATENT CLAIMS

1. A payment card (3) with a chip with a Secure Element (1) in which there is at least one payment card unit, with a contact field (4) and/or with a contactless element with an antenna (5) for the creation of a contactless communication channel (7), where the payment card (3) is adjusted so it can be connected to a reader (8) and also to a common POS terminal is characterised by the fact that the payment card (3) has two mutually interconnected chips with Secure Elements (1,2); on the payment card a Secure Element (1) with a payment card unit is connected to a Secure Element (2) with a payment terminal application of indifferent POS; the indifferent POS is adjusted to be configured according to the data receive from the reader (8) by a payment card (3), the configured POS is connected to the account data on the Secure Element (1); this account data will be used in payment transaction in configured POS in Secure Element (2); at least one Secure Element (1, 2) is connected, directly or using some other circuit element with a contact field (4) and/or a contactless element with an antenna (5) to create a contactless communication channel (7).

2. The payment card as in the claim 1 is characterised by the fact that the Secure Elements (1,2) are mutually interconnected using a circuit and/or calculating module (6), to which also a contact field (4) and/or contactless element with an antenna (5) is connected.

3. The payment card as in the claims 1 or 2 is characterised by the fact that it includes a button (9) for the confirmation of the payment.

4. The payment card as in any of the claims 1 to 3 is characterised by the fact that it is equipped with a display (10) to display the paid amount.

5. The payment card as in any of the claims 1 to 4 is characterized by the fact that the chip with the Secure Element (2) with the POS payment terminal unit is powered in a contactless way from the reader´s (8) electromagnetic field, during which direct and/or during the approach accumulated energy of the reader´s (8) electromagnetic field is used.

6. The payment system encompassing a payment card as in any of the claims 1 to 5 is characterised by the fact that it includes a reader (8) adjusted for the connection with the payment card (3); the holder POS terminal´s configuration data of the reader (8) are stored in the secured part of the memory.

7. The payment card reader in the system as in the claim 6, that encompasses contact or contactless interface for the connection with the payment card (3) is characterised by the fact that the secured part of the memory with configuration data of belonging to the holder of the POS terminal reader (8) can be removed from the reader´s (8) body.

8. The cashless payment method using a payment card (3) on the paying side and a reader (8) on the recipient side is characterised by the fact that the payment card (3) with two chips having Secure Elements (1, 2) is connected to the reader (8), which sends the identification data of the payment recipient´s POS terminal along with the amount of the requested payment to the payment card; on the payment card, the identification data are transferred to the second chip with a payment terminal application, where they are used for the configuration of the originally indifferent POS terminal for the benefit of the payment recipient, subsequently, the payment terminal application is run, during which the payment card account data from a Secure Element (1) are the resulting payment cryptogram is sent to the reader (8).

9. The cashless payment method as in the claim 8 is characterised by the fact that the identification data being transferred from the reader (8) to the payment card (3) are encrypted, preferably using a MasterKey that is stored in the secured part of the memory in the reader (8).

10. The cashless payment method as in the claims 8 or 9 is characterised by the fact that the amount being paid is shown on the payment card´s (3) display (10) and that the payment terminal application is run only after pressing the payment button (9) on the payment card (3).

11. The cashless payment method as in the claims 8 to 10 is characterised by the fact that the paid amount is shown on the reader´s (8) display (11).

12. The cashless payment method as in the claims 8 to 11 is characterised by the fact that the created payment cryptogram is sent from the reader (8) to the payment processing centre.

13. The cashless payment method as in the claims 8 to 12 is characterised by the fact that after being taken from the reader (8), the carrier with the records of realized payments is given for processing to the bank or payment processing centre.

14. The cashless payment method as in the claim 13 is characterised by the fact that the recipient takes the carrier with the realized payment record out of the reader (8) and after that inserts it into a device for automatic processing, which in suitable configuration is in an ATM machine or a common POS terminal.

15. The cashless payment method as in the claims 8 to 14 is characterised by the fact that the information about the payment´s value is inserted into the reader (8) manually using a keyboard (12) or using the connection between the reader (8) and a cash register.

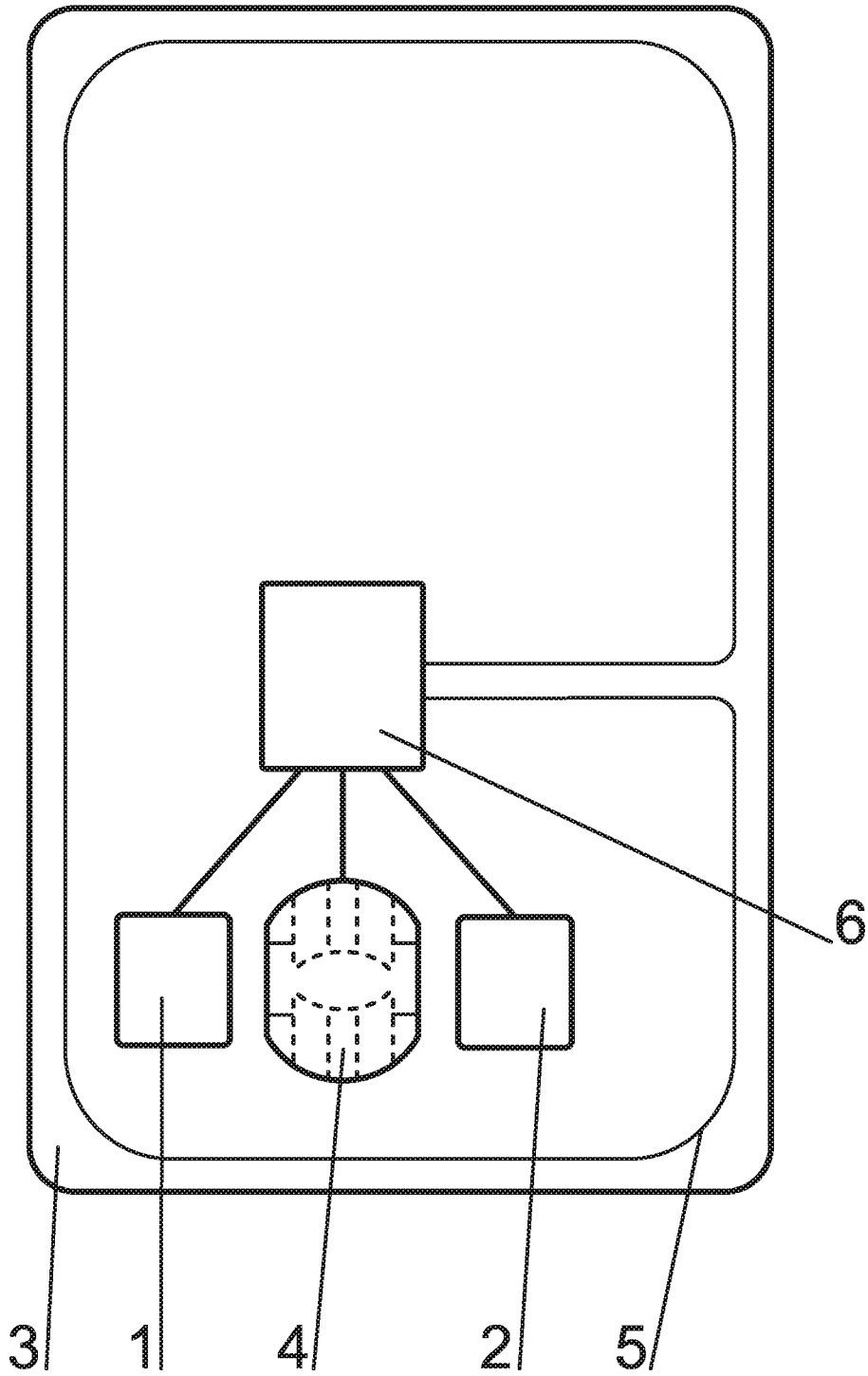

Fig. 1

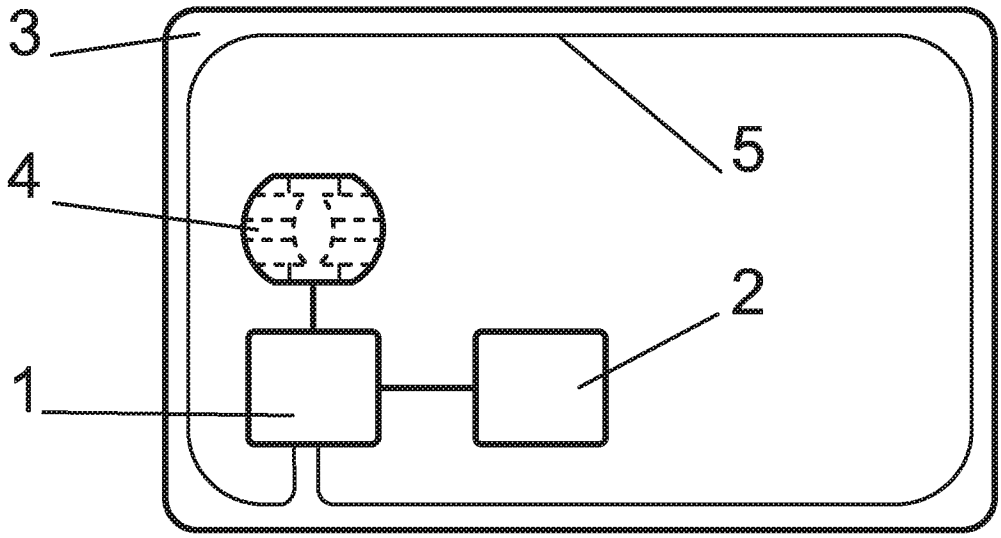

Fig. 2

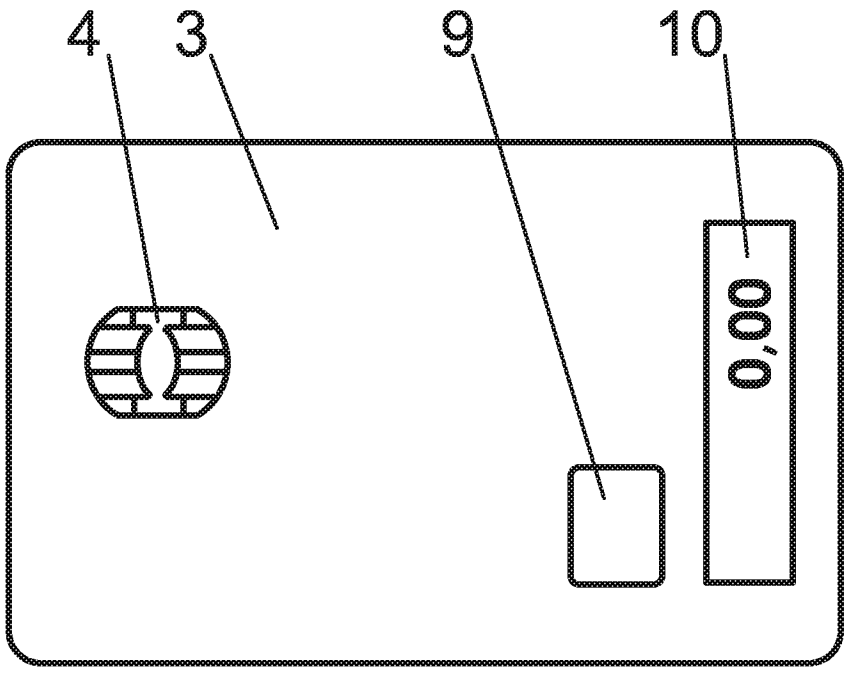

Fig. 3

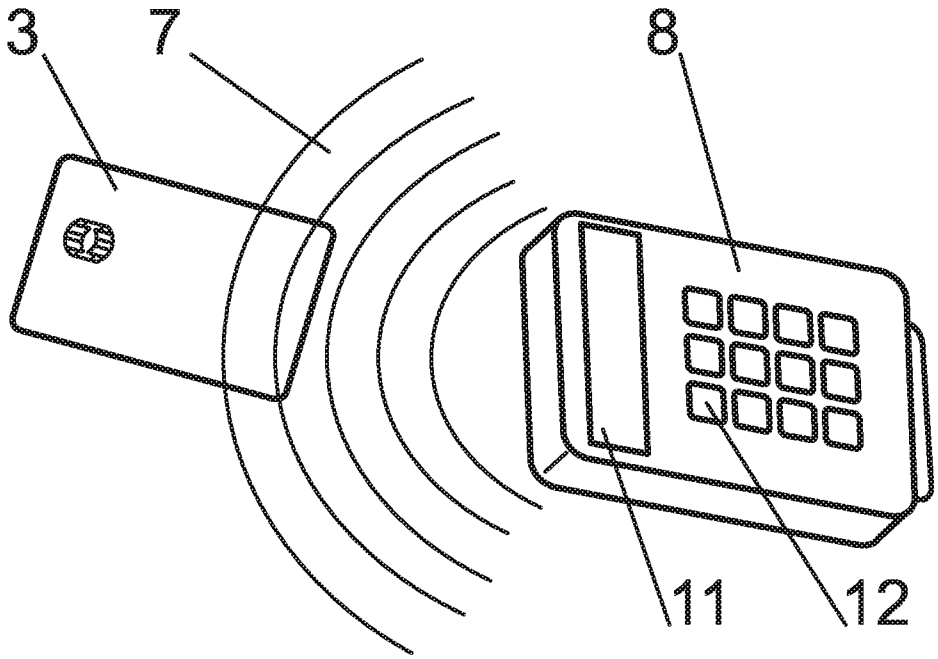

Fig. 4

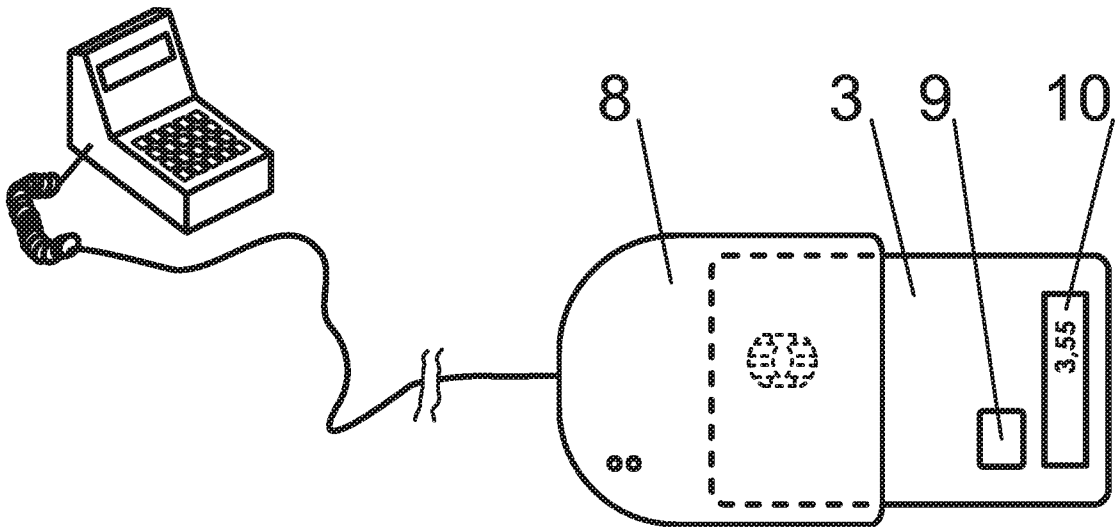

Fig. 5

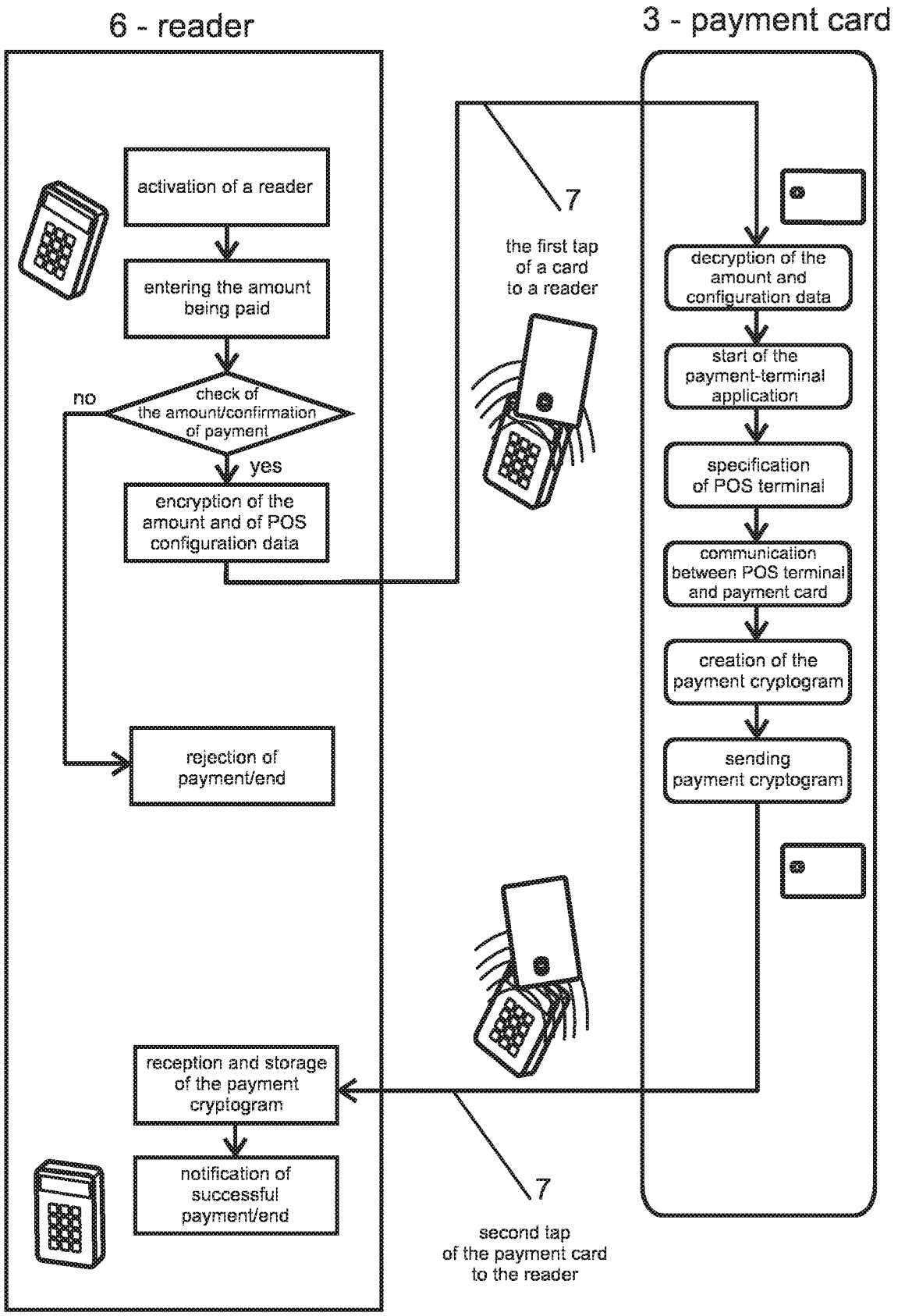
6 - reader
3 - payment card
activation of a reader
entering the amount being paid
check of the amount/confirmation of payment
no
yes
encryption of the amount and of POS configuration data
rejection of payment/end
7
the first tap of a card to a reader
decryption of the amount and configuration data
start of the payment-terminal application
specification of POS terminal
communication between POS terminal and payment card
creation of the payment cryptogram
sending payment cryptogram
reception and storage of the payment cryptogram
notification of successful payment/end
7
second tap of the payment card to the reader

Fig. 6

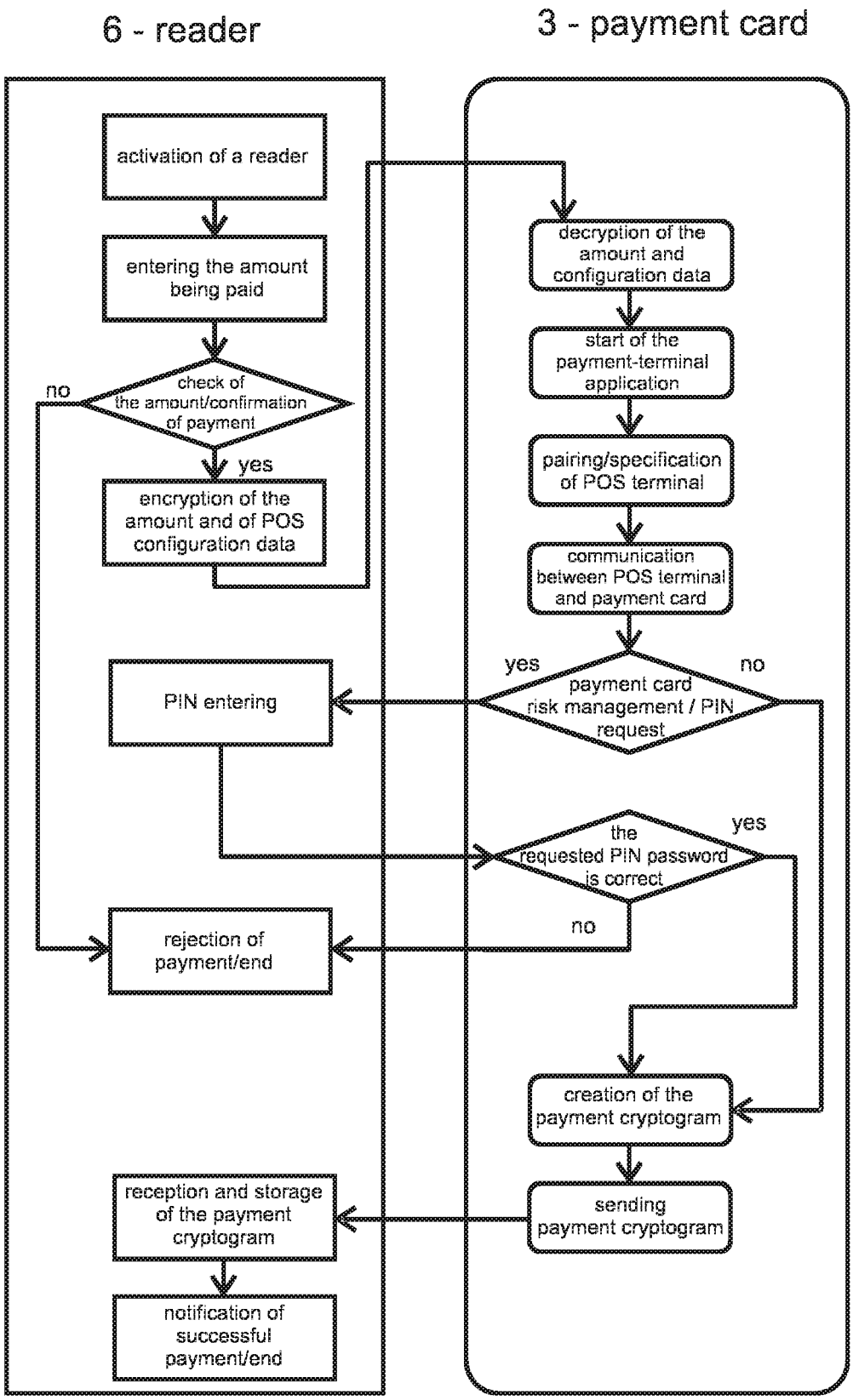
6 - reader
3 - payment card
activation of a reader
entering the amount being paid
check of the amount/confirmation of payment
no
yes
encryption of the amount and of POS configuration data
decryption of the amount and configuration data
start of the payment-terminal application
pairing/specification of POS terminal
communication between POS terminal and payment card
yes
payment card risk management / PIN request
no
PIN entering
the requested PIN password is correct
yes
no
rejection of payment/end
creation of the payment cryptogram
sending payment cryptogram
reception and storage of the payment cryptogram
notification of successful payment/end

Fig. 7

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2012/051849

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q20/32
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 798 867 A2 (INNOVISION RES & TECH PLC [GB]) 20 June 2007 (2007-06-20) abstract; figures 4,14 paragraphs [0007], [0011], [0016], [0032], [0108], [0129], [0131]	1-15
X	US 2010/217707 A1 (PHILLIPS SIMON [GB]) 26 August 2010 (2010-08-26) paragraphs [0002] - [0006], [0017]	1-15
X	WO 2009/083679 A2 (FRANCE TELECOM [FR]; ASSADI HOUSSEM [FR]; PICQUENOT DAVID [FR]) 9 July 2009 (2009-07-09) the whole document	1-15

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 September 2012	04/10/2012

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

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2012/051849

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1798867 A2	20-06-2007	EP 1798867 A2	20-06-2007
		GB 2433386 A	20-06-2007
		GB 2438756 A	05-12-2007
		GB 2464632 A	28-04-2010
		US 2012196529 A1	02-08-2012
US 2010217707 A1	26-08-2010	NONE	
WO 2009083679 A2	09-07-2009	EP 2243106 A2	27-10-2010
		WO 2009083679 A2	09-07-2009