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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 July 2016 (28.07.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/118087 A1

(51) International Patent Classification:
G06Q 20/40 (2012.01) *G07F 7/12* (2006.01)
G06Q 30/00 (2012.01) *H04L 9/00* (2006.01)

(21) International Application Number:
PCT/SG2016/050028

(22) International Filing Date:
21 January 2016 (21.01.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
201510029503.6 21 January 2015 (21.01.2015) CN

(71) Applicant: **JING KING TECH HOLDINGS PTE. LTD.** [SG/SG]; 24 Kaki Bukit Crescent, Kaki Bukit Techpark I, Singapore 416255 (SG).

(72) Inventor: **SUN, Guohua**; c/o Jing King Tech Holdings Pte. Ltd., 24 Kaki Bukit Crescent Kaki Bukit Techpark I, Singapore 416255 (SG).

(74) Agent: **RHT I-ASSETS ADVISORY PTE. LTD.**; Six Battery Road #10-01, Singapore 049909 (SG).

(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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 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, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, 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, KM, ML, MR, NE, SN, TD, TG).

Published:

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

WO 2016/118087 A1

(54) Title: SYSTEM AND METHOD FOR SECURE ONLINE PAYMENT USING INTEGRATED CIRCUIT CARD

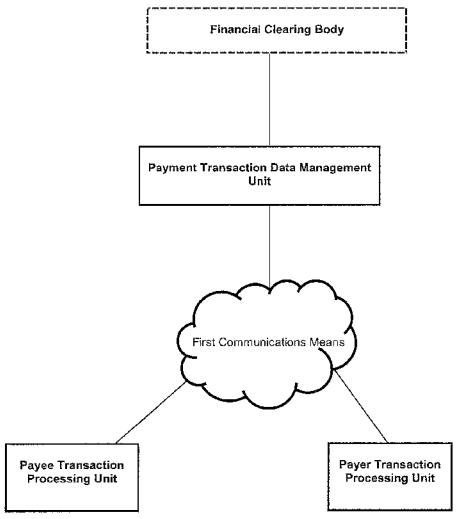

Figure 1

(57) Abstract: The present invention relates to a system and a method for secure online payment using an integrated circuit card. There is disclosed a system for secure online payment comprising a payer transaction processing unit, a payee transaction processing unit, and a payment transaction data management unit, the payment transaction data management unit connectable to a transaction clearing unit, wherein the payer transaction processing unit, the payee transaction processing unit and the payment transaction data management unit interconnect via a first communications means for sending and receiving payment transaction information that is encrypted, and wherein a first portion of the payment transaction information is communicated from the payee transaction processing unit to the payer transaction processing unit and to the payment transaction data management unit through a first communications channel, and a second portion of the payment transaction information and the first portion of the payment transaction information are communicated from the payer transaction processing unit to the payment transaction data management unit through a second communications channel for verification and processing of the transaction payment information enabling secure payment online.

SYSTEM AND METHOD FOR SECURE ONLINE PAYMENT USING INTEGRATED CIRCUIT CARD

FIELD OF THE INVENTION

The present invention relates to a system and a method for secure online payment using an integrated circuit (IC) card, and its applications include various types of payments that can be made online such as third party payment, mobile payment, online shopping payment and e-commerce payment.

BACKGROUND TO THE INVENTION

The following discussion of the background to the invention is intended to facilitate an understanding of the present invention. However, it should be appreciated that the discussion is not an acknowledgment or admission that any of the material referred to was published, known or part of the common general knowledge in any jurisdiction as at the priority date of the application.

The conventional offline credit card payment system is a typical payment platform which relies on a point of sale (POS) machine or a conventional magnetic swipe card reader to complete a user's payment process such as a shopping payment process by swiping a financial or bank card which enables the reading of the bank card information, and submitting the bank card information to a backend transaction system. This payment method which is easy to operate has become a mainstream mode of payment for offline payments.

With the widespread use of the Internet, online businesses have developed rapidly providing numerous online shops where users are able to shop and make payment for their purchases online (online payment). However, in contrast to offline payment where a POS machine or a swipe card reader is used to process payment, such a machine or card reader is not readily available for online payment. As such, online payments are typically made via online banking or Internet banking with the respective banks. However, there are also some limitations associated with online banking or Internet banking; firstly, a user is required to separately

register an online banking account with a bank in order to utilise the various online banking services offered by the bank. Typically, the installation and payment process is relatively complex and the numerous online banking functions associated with an online banking account tend to be attacked by hackers via the online payment process. In order to enhance the security of online banking, a user is currently required to have on hand additional security tools, such as U shield（USB Key）or an access token, etc., in order to utilise online banking services such as making payment via online banking or Internet banking.

However, with the emergence of mobile payment (mobile banking), new issues relating to security of payment made by means of mobile banking are now present. Security tools such as U shield or an access token that are typically used for online banking to enhance security have to be adapted so as to also support the mobile phone environment, which further increases the complexity of application of security tools to mobile banking.

Another issue that arises relates to various banks each having its own online banking system that may be involved in a single online payment transaction. For instance, the bank used by a particular online shop or merchant (the acquiring bank) for an online purchase by a user (payer) may differ from the bank that the user is using to make the online payment (issuing bank). As different banks have their own online banking systems which are not harmonised across all banks, such a payment transaction can only be completed through an authorised body such as Visa™, MasterCard™ or China UnionPay™ (for interbank payment or settlement in China) to achieve interbank payment or settlement. However, due to various reasons such as security related issues, it is difficult for an authorised body to achieve the connection with each of the millions of ordinary online businesses or stores online. Therefore, there is the emergence of third-party payment service providers such as PayPal™ and Alipay™ (platforms) for providing professional services to various online businesses or stores so as to solve the online payment (collection) issues of online stores. Whilst such third-party payment service providers (platform) facilitate and make online payment more convenient for online stores, users or customers, the security of such payments is unfortunately reduced. This issue has been hindering the further development of online payment.

In relation to offline payment, in order to further improve payment security, financial agencies such as banks worldwide have actively replaced traditional magnetic strip cards with IC cards, enabling offline payment to be simple, convenient, secure and reliable. By contrast, existing financial IC card payment systems or platforms for online and/or mobile payment still lack the above-mentioned advantages associated with offline payment systems, especially in relation to the convenience and security of online and/or mobile payment.

Therefore, the present invention attempts to overcome at least in part some of the aforementioned disadvantages.

SUMMARY OF THE INVENTION

Throughout this document, unless otherwise indicated to the contrary, the terms "comprising", "consisting of", and the like, are to be construed as non-exhaustive, or in other words, as meaning "including, but not limited to".

In accordance with a first aspect of the present invention, there is provided a system for secure online payment comprising:

(a) a payer transaction processing unit;

(b) a payee transaction processing unit; and

(c) a payment transaction data management unit, the payment transaction data management unit connectable to a transaction clearing unit,

wherein the payer transaction processing unit, the payee transaction processing unit and the payment transaction data management unit interconnect via a first communications means for sending and receiving payment transaction information that is encrypted, and wherein a first portion of the payment transaction information is communicated from the payee transaction processing unit to the payer transaction processing unit and to the payment transaction data management unit through a first communications channel, and a second portion of the payment transaction information and the first portion of the

payment transaction information are communicated from the payer transaction processing unit to the payment transaction data management unit through a second communications channel for verification and processing of the transaction payment information enabling secure payment online.

Preferably, the first communications channel comprises means for encrypting the first portion of the payment transaction information and sending the encrypted information to the payer transaction processing unit and to the payment transaction data management unit; means for receiving the encrypted information by the payer transaction processing unit and decrypting the encrypted information; and means for receiving the encrypted information by the payment transaction data management unit and decrypting the encrypted information.

Preferably, the second communications channel comprises means for encrypting the second portion of the payment transaction information and encrypting the first portion of the payment transaction information, and sending the encrypted first and second portions of the payment transaction information to the payment transaction data management unit; and means for receiving the encrypted information by the payment transaction data management unit and decrypting the encrypted information.

Preferably, the payee transaction processing unit comprises a processor having a payee transaction processing module which is connectable to the payment transaction data management unit.

Preferably, the payer transaction processing unit comprises a communications device having a payer transaction processing module which is connectable to the payment transaction data management unit via the communication means and is connectable to an integrated circuit (IC) card via a second communications means.

Preferably, the second communications means is a wireless communication means.

Preferably, the wireless communications means is in the form of near field communication (NFC).

Preferably, the payment transaction data management unit comprises a data management module, an information database module, a payer interface module for connecting to the payer transaction processing unit, a payee interface module for connecting to the payee transaction processing unit, and a transaction clearing interface module for connecting to the transaction clearing unit, wherein the data management module is in communication with the information database module, the payee and payer interface modules and the transaction clearing interface module.

Preferably, the data management module generates at least one secret key for encryption and decryption.

Preferably, the information database module is operable to record information relating to a payee, a payer and a financial clearing body.

Preferably, the information relating to the payee comprises business registration information, bank information and account information.

Preferably, the information relating to the payer comprises name of the payer, identification number of the payer, telephone number of the payer and e-mail address of the payer.

Preferably, the information relating to the financial clearing body comprises registration number of the body, name of the body and the predetermined security certification information of the financial clearing body.

Preferably, each of the payer interface module, the payee interface module and the transaction clearing interface module is an application programme interface (API).

Preferably, the means for encrypting the first portion of the payment transaction information and sending the encrypted information to the payer transaction processing unit and to the payment transaction data management unit is the payee transaction processing module.

Preferably, the means for receiving the encrypted first portion of the payment transaction information by the payer transaction processing unit and decrypting the encrypted information

is the payer transaction processing module.

Preferably, the means for receiving the encrypted first portion of the payment transaction information by the payment transaction data management unit and decrypting the encrypted information is the data management module.

Preferably, the means for encrypting the second portion of the payment transaction information and encrypting the first portion of the payment transaction information, and sending the encrypted first and second portions of the payment transaction information to the payment transaction data management unit is the payer transaction processing module.

Preferably, the means for receiving the encrypted first and second portions of the payment transaction information by the payment transaction data management unit and decrypting the encrypted information is the data management module.

Preferably, the payment transaction information is encrypted and is decrypted based on a symmetric or an asymmetric algorithm.

Preferably, payment transaction information comprises transaction certification information, payee information and information on the payment amount.

Preferably, the transaction certification information comprises at least one of an identification number, an electronic signature and a dynamic code.

Preferably, the first communication means is one of the Internet, an intranet, a dedicated network and any network suitable for interconnecting the payer transaction processing unit, the payee transaction processing unit and the payment transaction data management unit.

In accordance with a second aspect of the invention, there is disclosed a payment transaction data management unit for use in a system for secure online payment wherein upon receiving a first encrypted information comprising a first portion of a payment transaction information from a payee transaction processing module of a payee transaction processing unit, the encrypted information is decrypted at a data management module; the data management

module further receives a second encrypted information comprising a second portion of the payment transaction information from a payer transaction processing module of a payer transaction processing unit where the second encrypted information is decrypted; the first and second portions of the payment transaction information is verified and encrypted at the data management module for sending to a transaction clearing interface of a transaction clearing unit in a prescribed format; receiving a transaction result to the data management module from the transaction clearing interface, converting the transaction result into a prescribed format and sending the converted transaction result to the payer transaction processing module and the payee transaction processing module.

Preferably, the payment transaction information is encrypted and is decrypted based on a symmetric or an asymmetric algorithm.

Preferably, the first portion of the payment transaction information comprises information on payment amount and payee information.

Preferably, the payee information comprises business registration information, bank information and account information.

Preferably, the payment transaction information comprises transaction certification information, payee information and information on the payment amount.

Preferably, the transaction certification information comprises at least one of an identification number, an electronic signature and a dynamic code.

In accordance with a third aspect of the invention, there is provided a method for secure online payment comprising:

(a) generating a first portion of the payment transaction information by a payee transaction processing module of a payee transaction processing unit, encrypting the first portion of the payment transaction information, and sending the encrypted information to a data management module of a payment transaction data management unit and to a payer transaction processing module of a payer

transaction processing unit;

(b) receiving and decrypting the first portion of the payment transaction information by the payer transaction processing module and the data management module;

(c) obtaining a second portion of the payment transaction information by placing an integrated circuit (IC) card adjacent to or at a predetermined distance to a communications device of the payer transaction processing unit and inputting a password into the communications device;

(d) encrypting the second portion of the payment transaction information and the first portion of the payment transaction information by the payer transaction processing module and sending the encrypted first and second portions of the payment transaction information to a data management module of a payment transaction data management unit;

(e) receiving and decrypting the first and second portions of the payment transaction information by the data management module;

(f) verifying the first and second portions of the payment transaction information and by the data management module; and

(g) converting the first and second portions of the payment transaction information by the data management module into a standard format for sending to a financial clearing unit.

Preferably, wherein in the step (d), the method further comprises inputting a password or signing for verification of the first portion of the payment transaction information prior to encrypting the first portion of the payment transaction information and sending the encrypted first portion of the payment transaction information to the data management module.

Preferably, encryption and decryption of the payment transaction information is based on a symmetric or an asymmetric algorithm.

Preferably, the method further comprises generating at least one secret key for encryption and decryption by the data management module.

Preferably, wherein prior to the step (a), the method further comprises initialising the payee and the payer transaction processing modules by the data management module.

Preferably, the first portion of the transaction information comprises information on payment amount and payee information.

Preferably, the payee information comprises business registration information, bank information and account information.

Preferably, the payment transaction information comprises transaction certification information, payee information and information on the payment amount.

Preferably, the transaction certification information comprises at least one of an identification number, an electronic signature and a dynamic code.

In accordance with a fourth aspect of the invention, there is disclosed a system for secure online payment substantially as described herein with references to the accompanying drawings.

In accordance with a fifth aspect of the invention, there is disclosed a payment transaction data management unit substantially as described herein with references to the accompanying drawings.

In accordance with a sixth aspect of the invention, there is disclosed a method for secure online payment substantially as described herein with references to the accompanying drawings.

Other aspects and advantages of the invention will become apparent to those skilled in the art from a review of the ensuing description, which proceeds with reference to the following illustrative drawings of various embodiments of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will now be described, by way of illustrative example only, with reference to the accompanying drawings, of which:

Figure 1 is a schematic diagram of a system for secure online payment in accordance with an embodiment of the present invention; and

Figure 2 is a schematic diagram of a payment transaction data management unit, a payee transaction processing unit and a payer transaction processing unit of the system of Figure 1.

DETAILED DESCRIPTION OF THE INVENTION

Particular embodiments of the present invention will now be described with reference to the accompanying drawings. The terminology used herein is for the purpose of describing particular embodiments only and is not intended to limit the scope of the present invention. Additionally, unless defined otherwise, all technical and scientific terms used herein have the same meanings as commonly understood by one of ordinary skill in the art to which this invention belongs.

The present invention discloses a system and a method for secure online payment using an integrated circuit (IC) card. The IC card can be in the form of a financial IC card issued by a financial body such a bank. The system (or payment platform) and the method advantageously enhance the convenience and security of online payment, which include various types of payments that can be made online such as third party payment, mobile payment, online shopping payment and e-commerce payment.

The ultimate purpose of a payment platform is to acquire the account numbers of payee and payer, as well as the transaction amount in order to effect the transfer of funds from the payer's bank account to the payee's bank account to complete the transaction. Certainly, an indispensable aspect of a payment platform is ensuring the security of this transaction at all stages and making the whole transaction process as simple and convenient as possible. It is based on this principle that this invention provides a system (or payment platform) and a

method for secure online payment.

With reference to Figures 1 and 2, there is described hereinafter a system for secure online payment comprising a payer transaction processing unit, a payee transaction processing unit and a payment transaction data management unit in which the payment transaction data management unit is connectable to a transaction clearing unit. The system can be in the form of a payment platform.

The payer transaction processing unit, the payee transaction processing unit and the payment transaction data management unit interconnect via a first communications means for sending and receiving payment transaction information that is encrypted. A first portion of the payment transaction information is communicated from the payee transaction processing unit to the payer transaction processing unit and to the payment transaction data management unit through a first communications channel, and a second portion of the payment transaction information and the first portion of the payment transaction information are communicated from the payer transaction processing unit to the payment transaction data management unit through a second communications channel for verification and processing of the transaction payment information enabling secure payment online.

The payment transaction information comprises transaction certification information, payee information and information on the payment amount. The transaction certification information can be one or more of the following: an identification number, an electronic signature and a dynamic code.

The first communications means is in the form of the Internet, an intranet, a dedicated network or any network suitable for interconnecting the payer transaction processing unit, the payee transaction processing unit and the payment transaction data management unit.

The payment transaction data management unit comprises of a computer system hardware, and its software comprises a data management module, an information database module, a payer interface module for connecting to the payer transaction processing unit, a payee interface module for connecting to the payee transaction processing unit, and a transaction

clearing interface module for connecting to the transaction clearing unit, wherein the data management module is in communication with the information database module, the payee and payer interface modules and the transaction clearing interface module.

The payment transaction information is encrypted and is decrypted based on a symmetric or an asymmetric algorithm, and the data management module generates at least one secret key for encryption and decryption.

The information database module is used to record information relating to a payee, a payer and a financial clearing body. The information relating to the payee comprises business registration information, bank information and account information. The information relating to the payer comprises name of the payer, identification number of the payer, telephone number of the payer and e-mail address of the payer. The information relating to the financial clearing body comprises registration number of the body, name of the body and the predetermined security certification information of the financial clearing body.

In addition, each of the payer interface module, the payee interface module and the transaction clearing interface module is an application programme interface (API).

The payee transaction processing unit comprises a processor having a payee transaction processing module which is connectable to the payment transaction data management unit.

The payer transaction processing unit comprises a communications device having a payer transaction processing module which is connectable to the payment transaction data management unit via the communication means and is connectable to an integrated circuit (IC) card via a second communications means. The second communication means is in the form of a wireless communication means, such as near field communication (NFC) and the like.

The first communications channel comprises means for encrypting the first portion of the payment transaction information and sending the encrypted information to the payer transaction processing unit and to the payment transaction data management unit. The first communications channel also comprises means for receiving the encrypted information by the

payer transaction processing unit and decrypting the encrypted information. The first communications channel further comprises means for receiving the encrypted information by the payment transaction data management unit and decrypting the encrypted information.

The second communications channel comprises means for encrypting the second portion of the payment transaction information and encrypting the first portion of the payment transaction information, and sending the encrypted first and second portions of the payment transaction information to the payment transaction data management unit. The second communications channel also comprises means for receiving the encrypted information by the payment transaction data management unit and decrypting the encrypted information.

Further to the first communications channel, the means for encrypting the first portion of the payment transaction information and sending the encrypted information to the payer transaction processing unit and to the payment transaction data management unit can be in the form of the payee transaction processing module. The means for receiving the encrypted first portion of the payment transaction information by the payer transaction processing unit and decrypting the encrypted information can be in the form of the payer transaction processing module. The means for receiving the encrypted first portion of the payment transaction information by the payment transaction data management unit and decrypting the encrypted information can be in the form of the data management module.

Further to the second communications channel, the means for encrypting the second portion of the payment transaction information and encrypting the first portion of the payment transaction information, and sending the encrypted first and second portions of the payment transaction information to the payment transaction data management unit can be in the form of the payer transaction processing module. The means for receiving the encrypted first and second portions of the payment transaction information by the payment transaction data management unit and decrypting the encrypted information can be in the form of the data management module.

The data management module has a plurality of functions which comprises: (a) a installing a

module in the payee's computer system or managed server that is part of the payee transaction processing unit in the payee transaction processing module; (b) installing a module in the payer's communication device such as a mobile phone that is part of the payer transaction processing unit in the payer transaction processing module; (c) co-processing the initialization and data integration of the payee transaction processing module and the payer transaction processing module.

The payee transaction processing module can be downloaded by the payee through communications means such as the Internet where the module installs automatically and is set by the payer through registration. Alternatively, the module is installed manually by a technician administrating the system (payment platform) to achieve connection with a payee application system and initialization is conducted by the data management module. The payer transaction processing module can be downloaded by the payer through communications means such as the Internet where the module installs automatically and is set by the payer through registration, and initialized by the data management module. The data management module resides in the payment transaction data management unit (or backend system) where in addition to conducting the initialization of the payee and payer module, it also conducts the data exchange, certifies the exchange information provided by the payee and payer, and organizes the certified transaction information of payee and payer into a standard format, conducting the data exchange with the financial clearing agency (or body) through the interface. The function of the data management module also includes receiving the transaction processing results from the financial body or agency, converting the results into a unified standard format matching with the payee interface module and payer interface module, and sending them to the payee and payer respectively.

The payee interface module, payer interface module and the transaction clearing interface module for connecting to the transaction clearing unit are in an application programme interface (API) format, which provides internal processing for the payee transaction processing unit, and provides external processing for the third party collection body or agency, payee and financial clearing agency. The payee transaction processing unit comprises the payee transaction processing module installed in the payee's computer or entrust managed

server. This software module shares the digital exchange interface with the online store software of the payee. Alternatively, the module can be embedded directly into the payee's online store software for receiving payment transaction information provided by the online store software. This information will be encrypted or signed, and given a transaction code, which will then be sent to the data management module of the system. In addition, the payee transaction processing module converts the transaction code into the 2-dimensional code or other encoding mode, and then sends the code back to the online store software module for pushing the encoding mode of this transaction code to the payer terminal or the payer transaction processing unit. Meanwhile, it also receives the processed transaction information from the backend system, and resubmits it back to the online store software after decrypting or certifying.

The encryption and decryption of the information adopts the standard symmetric or asymmetric algorithm, or the symmetric or asymmetric algorithm issued by the authorities. The at least one secret key of encryption and decryption is generated in the initialization of the payee transaction processing module by the data management module in the backend system. The stated collection transaction information includes: transaction certification information, payee information and the collected amount, among which, the transaction certification information is the information of a particular or certain transaction. The transaction certification information certifies the transaction information of the same transaction provided by the payer in the backend system, to determine the identity of the transaction information from the payee and payer. This transaction certification information includes the number, or the electronic signature or dynamic code. This payee information is the payee information recorded in the information database of payee, payer and financial clearing agency in the backend system of the payment platform.

The payer transaction processing unit comprises the payer transaction processing module which is installed in a communications device such as a payer's phone, tablet, laptop, computer and any communications device of the like. The financial IC card conducts data interchange with this payer transaction processing module by near field communication (NFC). The payer transaction processing module, as an independent application, can be

started manually by the payer (or buyer) or can be triggered by other applications. When the payer transaction processing module is in operation, firstly, it shall acquire the payment transaction information from the payer by scanning the code or through other wireless transmission methods; if the payment transaction information is only in the form of a transaction code, then, the payment transaction processing module may first send this transaction code to the data management module in the backend system of the payment platform, and acquire the complete content of the payment transaction information, which can be also referred to as the collection transaction information, from the backend system; after the payer transaction processing module acquires the complete content of the payment transaction information, the screen of the payer's phone may display the relevant payment information, including: the name and collection amount of the payee, etc., and prompt the payer to attach the bank card or financial IC card to the back of the phone, and input the transfer password; the payer transaction processing module will conduct the data processing on the payment transaction information and the bank card transfer password of the payer via NFC and the bank card attached to the back of the phone according to the standards and specifications prescribed by the financial clearing agency, and then send them to the data management module in the payment transaction data management unit. Thereafter, the module awaits and receives the result transaction processing information.

The encryption and decryption of the information between the payer transaction processing module and the data management module in the backend system adopts the standard symmetric or asymmetric algorithms or the symmetric or asymmetric algorithm issued by authorities, and the at least one secret key of encryption and decryption is generated in the initialization of payee transaction processing module by the data management module in the backend system.

Advantageously, the effect of this invention includes the following: A user (payer) can complete the transaction payment by scanning (or directly), acquire the merchant's (payee) collection information via the user's phone, and then complete the payment by inputting password and swiping card (the internet banking or phone banking is omitted in this operation); the payment transaction information can be conducted with dual-channel

information certification in the backend system via the dual-channel of the merchant and the user's phone; the secret key system between the backend system and the merchant, and the backend system and the user's phone are different, and the data transmission between the merchant and the user can only be operated in the form of code without any transaction information. All these increase the difficulty in a hacker's attack, and therefore, improve significantly the security and convenience of a transaction made online.

With reference to Figures 1 and 2, the implementing process of an embodiment of the invention is described hereinafter.

Referring to Figure 1, the system for secure online payment includes three parts: a payment transaction data management unit (backend system), a payee (merchant) transaction processing unit; and a payer (buyer) transaction processing unit. These three units or parts interconnect via a first communications means for sending and receiving payment transaction information that is encrypted. The first communications mean can be one of the Internet, an intranet, a dedicated network and any network suitable for interconnecting the payer transaction processing unit, the payee transaction processing unit and the payment transaction data management unit. The payment transaction data management unit (backend system) can also connect with the financial clearing agency (such as China Union-pay or any bank) with transaction clearing function through a transaction clearing unit.

Referring to Figure 2, in accordance with an embodiment of the invention, the payment transaction data management unit, the payer transaction processing unit and the payee transaction processing unit are described in detail as follows:-

1. The payment transaction data management unit (backend system): as the core part of the system or payment platform, the hardware comprises a computer system, and its software includes: a data management module, an information database module, a payer interface module for connecting to the payer transaction processing unit, a payee interface module for connecting to the payee transaction processing unit, and a transaction clearing interface module for connecting to the transaction clearing unit (such as Union-pay or any bank),

wherein the data management module is in communication with the information database module, the payee and payer interface modules and the transaction clearing interface module.

The payee, payer and financial clearing agency records the payee (merchant) information, the payer (buyer) registration information, and the information of financial clearing agency, including business registration information (the number, title and contact information of the merchant), as well as the information about the opening bank and account of payee (merchant); the registration information of payer (buyer) includes name, ID number, phone number and E-mail; the information of the financial clearing agency includes number, name and the agreed security certification information of the financial clearing agency.

The payee interface module, payer interface module and the transaction clearing interface module which connects to the financial clearing agency are all in API format, which internally, can provide the program invocation for the payee (merchant) transaction processing unit and payer (buyer) transaction processing unit, and externally, the applications invocation for the third party collection agency (merchant), payee (buyer) and financial clearing agency.

The data management module includes: the module installed in the payee's (merchant's) computer system (or managed server) belongs to the payee (buyer) transaction processing unit in the payee (buyer) transaction processing module; the module installed in the payer's mobile phone belongs to the payer transaction processing section in the part of payer transaction processing module; the data management module used for co-processing the initialization and data integration of payee transaction process module and payer transaction process module.

The payee transaction processing module can be downloaded by the payee (merchant) through the Internet, the module installs automatically and can also be set by the payee through registration. Alternatively, the module is installed manually by the technician administrating the financial IC card payment platform, to achieve the connection with the payee (merchant) application system, and the initialization is conducted by the data management module (download and install the secret key to ensure safe communication); the payer transaction processing module is downloaded by the payer (buyer) through the Internet,

the module installs automatically and is set by the payer through registration, and initialized by the data management module (download and install the secret key to ensure safe communication); the data management module resides in the backend system. In addition to conducting the initialization of the payee and payer modules, it also conducts the data exchange, certifies the exchange information provided by the payee and payer, organizes the certified transaction information of payee and payer into a standard format (the format required by the financial clearing agency), and conducts the data exchange with the financial clearing agency through the interface. The function of the data management module also includes receiving the transaction processing results provided by the financial agency, converting the results into the standard format matching with the payee interface module and payer interface module, where these are then sent to the payee and payer respectively.

The payment transaction data management unit for use in a system for secure online payment wherein upon receiving a first encrypted information comprising a first portion of a payment transaction information from a payee transaction processing module of a payee transaction processing unit, the encrypted information is decrypted at a data management module; the data management module further receives a second encrypted information comprising a second portion of the payment transaction information from a payer transaction processing module of a payer transaction processing unit where the second encrypted information is decrypted; the first and second portions of the payment transaction information is verified and encrypted at the data management module for sending to a transaction clearing interface of a transaction clearing unit in a prescribed format; receiving a transaction result to the data management module from the transaction clearing interface, converting the transaction result into a prescribed format and sending the converted transaction result to the payer transaction processing module and the payee transaction processing module.

The payment transaction information is encrypted and is decrypted based on a symmetric or an asymmetric algorithm. The first portion of the payment transaction information comprises information on payment amount and payee information. The payee information comprises business registration information, bank information and account information. The payment

transaction information comprises transaction certification information, payee information and information on the payment amount, in which the transaction certification information comprises at least one of an identification number, an electronic signature and a dynamic code. The above-mentioned different types of information that make up the payment transaction information are exemplary embodiments and are not restricted or limited as such. It would be appreciated that the payment transaction information can also include other types of information.

2. The payee (merchant) transaction-processing unit is the payee (merchant) transaction-processing module of the system or payment platform installed in the payee's computer (or entrust managed server). This software module shares the digital exchange interface with the online store software (used for selling commodities or services) of the payee (merchant). It can also be embedded directly to the payee's (merchant's) online store software for receiving the collection transaction information provided by the online store software. Meanwhile, this information will be encrypted or signed (conduct MAC computing on transaction information), and given a transaction code (this code can be generated randomly or by certain mathematical logic), then send to the data management module of payee and payer in the payment platform system. In addition, the payee transaction processing module converts the transaction code into the 2-dimensional code or other encoding mode, and then send the code back to the online store software module for pushing the encoding mode of this transaction code to the payer (buyer) terminal (computer or phone). Meanwhile, it also receives the processed transaction information (such as the transaction is completed or there is some mistake in the transaction) from the backend system, and resubmit it back to the online store software after decrypting or certifying. Among which, the information encryption and decryption adopts the standard symmetric or asymmetric algorithm (or the symmetric or asymmetric algorithm issued by the authorities), the at least one secret key of encryption and decryption which is generated in the initialization of payee transaction processing module by the data management module in the backend system. The collection or payment transaction information includes: transaction certification information, payee information and the collected amount, among which, the "transaction certification information" is the information

of a particular transaction, certify the transaction information of the same transaction provided by the payer in the background system to determine the identity of the transaction information from the payee and payer. Therefore this "transaction certification information" includes the number (serial number or code), or the electronic signature or dynamic code; this "payee information" is the payee (merchant) information recorded in the information database of payee, payer and financial clearing agency in the backend system of the payment platform.

3. The payer (buyer) transaction processing unit of the system or payment platform is installed in the payer transaction processing module of the payer's (buyer's) phone, and the financial IC card (the bank card conforming to the standards of China Union-pay in China, or other standards imposed by the financial body in the respective countries) conducting data interchange with this payer transaction processing module by NFC. This software module, as an independent application, can be started manually by the buyer or triggered by other applications; when the payer transaction processing module is in operation, firstly, it acquires the collection transaction information from the payee (for the payee this is known as collection transaction information) by scanning the code (2-dimensional code or bar code, etc.) or other wireless transmission methods (short message, Bluetooth and broadband, etc.), and the specific mode can only be the mentioned transaction code; if the payment transaction information is only in the form of the transaction code, then the payment transaction processing module may first send this transaction code to the data management module in the backend system of the payment platform, and acquire the complete content of the payment transaction information, which is the same as the stated payment transaction information, from the backend system; after the payer transaction processing module has acquired the complete content of the payment transaction information (i.e., the collection transaction information). The screen of payer's phone may display the relevant payment information after payer transaction processing module acquires the complete contents of payment transaction information (i.e. the collection transaction information), including: the name and collection amount of the payee (merchant), etc., and prompts the payer (buyer) to attach the bank card for paying (the bank card conforming to the standards of China Union-pay in China, or other standards imposed by the financial body in the respective countries) to the back of the phone,

and inputs the transfer password. The payer transaction processing module will conduct the data processing on the payment transaction information and the bank card transfer password of payer (buyer) via NFC and the bank card attached to the back of the payer's (buyer's) phone according to the standards and specifications prescribed by the financial clearing agency (such as the PBOC specifications issued by the People's Bank of China or any other specifications issued by a financial body in the respective countries), and then sends them to the data management module in the payment transaction data management unit, and awaits receipt of the transaction processing information. The encryption and decryption of the information between the payer transaction processing module and the data management module in the backend system adopts the standard symmetric or asymmetric algorithms (or the symmetric or asymmetric algorithm issued by the authorities), and the at least one secret key of encryption and decryption is generated in the initialization of payee transaction processing module by the data management module in the backend system.

In accordance with another embodiment of the invention, there is described hereinafter a method for secure online payment. The method comprises the following steps:

(a) generating a first portion of the payment transaction information by a payee transaction processing module of a payee transaction processing unit, encrypting the first portion of the payment transaction information, and sending the encrypted information to a data management module of a payment transaction data management unit and to a payer transaction processing module of a payer transaction processing unit;

(b) receiving and decrypting the first portion of the payment transaction information by the payer transaction processing module and the data management module;

(c) obtaining a second portion of the payment transaction information by placing an integrated circuit (IC) card adjacent to or at a predetermined distance to a communications device of the payer transaction processing unit and inputting a password into the communications device;

(d) encrypting the second portion of the payment transaction information and the first portion of the payment transaction information by the payer transaction

processing module and sending the encrypted first and second portions of the payment transaction information to a data management module of a payment transaction data management unit;

(e) receiving and decrypting the first and second portions of the payment transaction information by the data management module;

(f) verifying the first and second portions of the payment transaction information and by the data management module; and

(g) converting the first and second portions of the payment transaction information by the data management module into a standard format for sending to a financial clearing unit.

The method further comprises inputting a password or signing for verification of the first portion of the payment transaction information prior to encrypting the first portion of the payment transaction information and sending the encrypted first portion of the payment transaction information to the data management module.

The encryption and decryption of the payment transaction information is based on a symmetric or an asymmetric algorithm. The method further comprises generating at least one secret key for encryption and decryption by the data management module.

Prior to the step (a), the method further comprises the step of initialising the payee and the payer transaction processing modules by the data management module. The first portion of the transaction information comprises information on payment amount and payee information. The payee information comprises business registration information, bank information and account information. The payment transaction information comprises transaction certification information, payee information and information on the payment amount, wherein the transaction certification information comprises at least one of an identification number, an electronic signature and a dynamic code.

In accordance with an embodiment of the method for secure online payment, there is described hereinafter the implementing process of an embodiment of the invention:

When a user (payer) selects a commodity and decides to pay for it, the merchant's system may send a 2-dimensional code including the payment amount and merchant's information to the user's computer. The user scans the 2-dimensional code on the computer screen by his or her phone and acquires relevant payment information on their phone. After checking the information and verifying there is no mistake, the user will attach the bank card or financial IC card for paying to the back of the phone, and inputs the transfer password of this card to the phone. The user's mobile software will send the acquired information to the backend system of the payment platform, and all the payment information will be submitted to the financial clearing agency after being verified and integrated by the backend system. The financial clearing agency will send the transaction result information back to the backend system of the payment platform after finishing the transaction. Then the backend system of the payment platform will send the transaction result information to the merchant's system and user's phone respectively, and the transaction is completed.

Based on above described embodiments, there are the following advantages in the payment transaction operated on system or payment platform:

First, as compared with traditional offline payment, a user does not need to swipe card or input code in the POS machine of the merchant, and simply acquires the billing information of the merchant by methods such as QR Code scanning using the user's mobile device, thereafter inputting the user's password and swiping the user's financial IC card on their phone to complete the payment. Therefore, a user will not worry about the risk of their account information and code being stolen, and the security of the online payment transaction is significantly improved.

Second, compared with traditional offline payment, the payment transaction information sent to the backend system (payment transaction data management unit) is no longer from the single device of the merchant (payee), but from the dual-channel of merchant and user's mobile device. The user's mobile device does not receive the payment transaction information directly from the merchant, but from the backend system, meanwhile, the backend system will authenticate the dual-channel information. Therefore, its security is tremendously higher than

the information transmitted via a single channel.

Third, users acquire the billing information of the merchant by scanning the 2-dimensional code (or other encoding codes) with their mobile device. Since there is no linkage or connection between the merchant system and the user's mobile device therefore, hacker attacks such as Trojan horse and virus cannot be realized in the transmission of payment transaction information, which further ensures the security and tamper-resistance of the payment transaction information.

Fourth, the secret key system between merchant's system and the backend system differs from the secret key system between user's system and the backend system, which further increases the difficulty of hacking, while at the same time ensuring it is easier for the management of the backend system. Identity theft is prevented where the merchant cannot pay as a user, and the user cannot pay as a merchant, either.

Fifth, the whole payment process only needs a mobile device and financial IC card, and payment can be completed in a complete shopping process, similar to the process of offline shopping where payment is made via the swiping of a financial IC card. This is different from traditional online shopping, where user needs to register and open the account on the internet bank or mobile bank, register and open a third party's payment account (such as Ali-pay account), and transfer to the internet bank interface from the shopping interface for paying, then return back to the shopping interface after paying, to finally complete the whole payment process. Therefore, on the one hand, this invention can avoid a hacker's attack on the bank transferring by taking advantage of bank payment; on the other hand, it can make the online payment as secure, easy and convenient as the offline payment.

It is to be understood that the above embodiments have been provided only by way of exemplification of this invention, and that further modifications and improvements thereto, as would be apparent to persons skilled in the relevant art, are deemed to fall within the broad scope and ambit of the present invention described herein. It is further to be understood that features from one or more of the described embodiments may be combined to form further

embodiments.

WE CLAIM

1. A system for secure online payment comprising:

   (a) a payer transaction processing unit;

   (b) a payee transaction processing unit; and

   (c) a payment transaction data management unit, the payment transaction data management unit connectable to a transaction clearing unit,

   wherein the payer transaction processing unit, the payee transaction processing unit and the payment transaction data management unit interconnect via a first communications means for sending and receiving payment transaction information that is encrypted, and wherein a first portion of the payment transaction information is communicated from the payee transaction processing unit to the payer transaction processing unit and to the payment transaction data management unit through a first communications channel, and a second portion of the payment transaction information and the first portion of the payment transaction information are communicated from the payer transaction processing unit to the payment transaction data management unit through a second communications channel for verification and processing of the transaction payment information enabling secure payment online.

2. The system according to claim 1, wherein the first communications channel comprises means for encrypting the first portion of the payment transaction information and sending the encrypted information to the payer transaction processing unit and to the payment transaction data management unit; means for receiving the encrypted information by the payer transaction processing unit and decrypting the encrypted information; and means for receiving the encrypted information by the payment transaction data management unit and decrypting the encrypted information.

3. The system according to claim 1 or 2, wherein the second communications channel comprises means for encrypting the second portion of the payment transaction information and encrypting the first portion of the payment transaction information, and sending the encrypted first and second portions of the payment transaction information to

the payment transaction data management unit; and means for receiving the encrypted information by the payment transaction data management unit and decrypting the encrypted information.

4. The system according to any of the preceding claims, wherein the payee transaction processing unit comprises a processor having a payee transaction processing module which is connectable to the payment transaction data management unit.

5. The system according to any of the preceding claims, wherein the payer transaction processing unit comprises a communications device having a payer transaction processing module which is connectable to the payment transaction data management unit via the communication means and is connectable to an integrated circuit (IC) card via a second communications means.

6. The system according to claim 5, wherein the second communications means is a wireless communication means.

7. The system according to claim 6, wherein the wireless communications means is in the form of near field communication (NFC).

8. The system according to any of the preceding claims, wherein the payment transaction data management unit comprises a data management module, an information database module, a payer interface module for connecting to the payer transaction processing unit, a payee interface module for connecting to the payee transaction processing unit, and a transaction clearing interface module for connecting to the transaction clearing unit, wherein the data management module is in communication with the information database module, the payee and payer interface modules and the transaction clearing interface module.

9. The system according to claim 8, wherein the data management module generates at least one secret key for encryption and decryption.

10. The system according to claim 8 or 9, wherein the information database module is operable to record information relating to a payee, a payer and a financial clearing body.

11. The system according to claim 10, wherein the information relating to the payee comprises business registration information, bank information and account information.

12. The system according to claim 10, wherein the information relating to the payer comprises name of the payer, identification number of the payer, telephone number of the payer and e-mail address of the payer.

13. The system according to claim 10, wherein the information relating to the financial clearing body comprises registration number of the body, name of the body and the predetermined security certification information of the financial clearing body.

14. The system according to any of claims 8 to 13, wherein each of the payer interface module, the payee interface module and the transaction clearing interface module is an application programme interface (API).

15. The system according to claims 2 and 5, wherein the means for encrypting the first portion of the payment transaction information and sending the encrypted information to the payer transaction processing unit and to the payment transaction data management unit is the payee transaction processing module.

16. The system according to claims 2 and 4, wherein the means for receiving the encrypted first portion of the payment transaction information by the payer transaction processing unit and decrypting the encrypted information is the payer transaction processing module.

17. The system according to claims 2 and 8, wherein the means for receiving the encrypted first portion of the payment transaction information by the payment transaction data management unit and decrypting the encrypted information is the data management module.

18. The system according to claims 3 and 5, wherein the means for encrypting the second portion of the payment transaction information and encrypting the first portion of the payment transaction information, and sending the encrypted first and second portions of the payment transaction information to the payment transaction data management unit is the payer transaction processing module.

19. The system according to claims 3 and 8, wherein the means for receiving the encrypted first and second portions of the payment transaction information by the payment transaction data management unit and decrypting the encrypted information is the data management module.

20. The system according to any preceding claim, wherein the payment transaction information is encrypted and is decrypted based on a symmetric or an asymmetric algorithm.

21. The system according to any of the preceding claims, wherein the payment transaction information comprises transaction certification information, payee information and information on the payment amount.

22. The system according to claim 21, wherein the transaction certification information comprises at least one of an identification number, an electronic signature and a dynamic code.

23. The system according to any of the preceding claims, wherein the first communication means is one of the Internet, an intranet, a dedicated network and any network suitable for interconnecting the payer transaction processing unit, the payee transaction processing unit and the payment transaction data management unit.

24. A payment transaction data management unit for use in a system for secure online payment wherein upon receiving a first encrypted information comprising a first portion

of a payment transaction information from a payee transaction processing module of a payee transaction processing unit, the encrypted information is decrypted at a data management module; the data management module further receives a second encrypted information comprising a second portion of the payment transaction information from a payer transaction processing module of a payer transaction processing unit where the second encrypted information is decrypted; the first and second portions of the payment transaction information is verified and encrypted at the data management module for sending to a transaction clearing interface of a transaction clearing unit in a prescribed format; receiving a transaction result to the data management module from the transaction clearing interface, converting the transaction result into a prescribed format and sending the converted transaction result to the payer transaction processing module and the payee transaction processing module.

25. The payment transaction data management unit according to claim 24, wherein the payment transaction information is encrypted and is decrypted based on a symmetric or an asymmetric algorithm.

26. The payment transaction data management unit according to claim 24 or 25, wherein the first portion of the payment transaction information comprises information on payment amount and payee information.

27. The payment transaction data management unit according to claim 26, wherein the payee information comprises business registration information, bank information and account information.

28. The payment transaction data management unit according to any of claims 24 to 27, wherein the payment transaction information comprises transaction certification information, payee information and information on the payment amount.

29. The payment transaction data management unit according to claim 28, wherein the

transaction certification information comprises at least one of an identification number, an electronic signature and a dynamic code.

30. A method for secure online payment comprising:

(a) generating a first portion of the payment transaction information by a payee transaction processing module of a payee transaction processing unit, encrypting the first portion of the payment transaction information, and sending the encrypted information to a data management module of a payment transaction data management unit and to a payer transaction processing module of a payer transaction processing unit;

(b) receiving and decrypting the first portion of the payment transaction information by the payer transaction processing module and by the data management module;

(c) obtaining a second portion of the payment transaction information by placing an integrated circuit (IC) card adjacent to or at a predetermined distance to a communications device of the payer transaction processing unit and inputting a password into the communications device;

(d) encrypting the second portion of the payment transaction information and the first portion of the payment transaction information by the payer transaction processing module and sending the encrypted first and second portions of the payment transaction information to a data management module of a payment transaction data management unit;

(e) receiving and decrypting the first and second portions of the payment transaction information by the data management module;

(f) verifying the first and second portions of the payment transaction information and by the data management module; and

(g) converting the first and second portions of the payment transaction information by the data management module into a standard format for sending to a financial clearing unit.

31. The method according to claim 30, wherein in the step (d), the method further comprises

inputting a password or signing for verification of the first portion of the payment transaction information prior to encrypting the first portion of the payment transaction information and sending the encrypted first portion of the payment transaction information to the data management module.

32. The method according to claim 30 or 31, wherein encryption and decryption of the payment transaction information is based on a symmetric or an asymmetric algorithm.

33. The method according to any of claims 30 to 32, wherein the method further comprises generating at least one secret key for encryption and decryption by the data management module.

34. The method according to any of claims 30 to 33, wherein prior to the step (a), the method further comprises initialising the payee and the payer transaction processing modules by the data management module.

35. The method according to any of claims 31 to 34, wherein the first portion of the transaction information comprises information on payment amount and payee information.

36. The method according to claim 35, wherein the payee information comprises business registration information, bank information and account information.

37. The method according to any of claims 31 to 36, wherein the payment transaction information comprises transaction certification information, payee information and information on the payment amount.

38. The method according to claim 37, wherein the transaction certification information comprises at least one of an identification number, an electronic signature and a dynamic code.

39. A system for secure online payment substantially as described herein with references to the accompanying drawings.

40. A payment transaction data management unit substantially as described herein with references to the accompanying drawings.

41. A method for secure online payment substantially as described herein with references to the accompanying drawings.

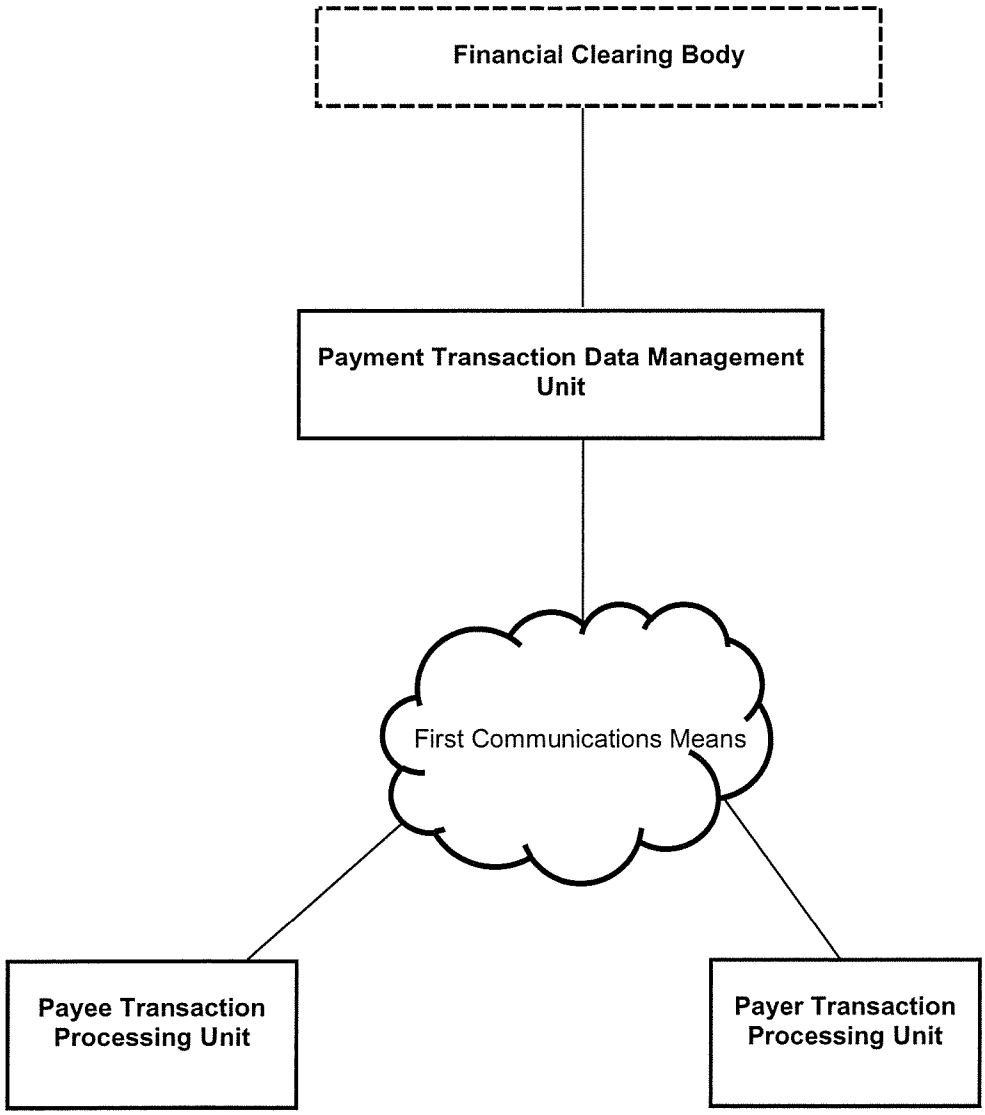
Financial Clearing Body
Payment Transaction Data Management Unit
First Communications Means
Payee Transaction Processing Unit
Payer Transaction Processing Unit

Figure 1

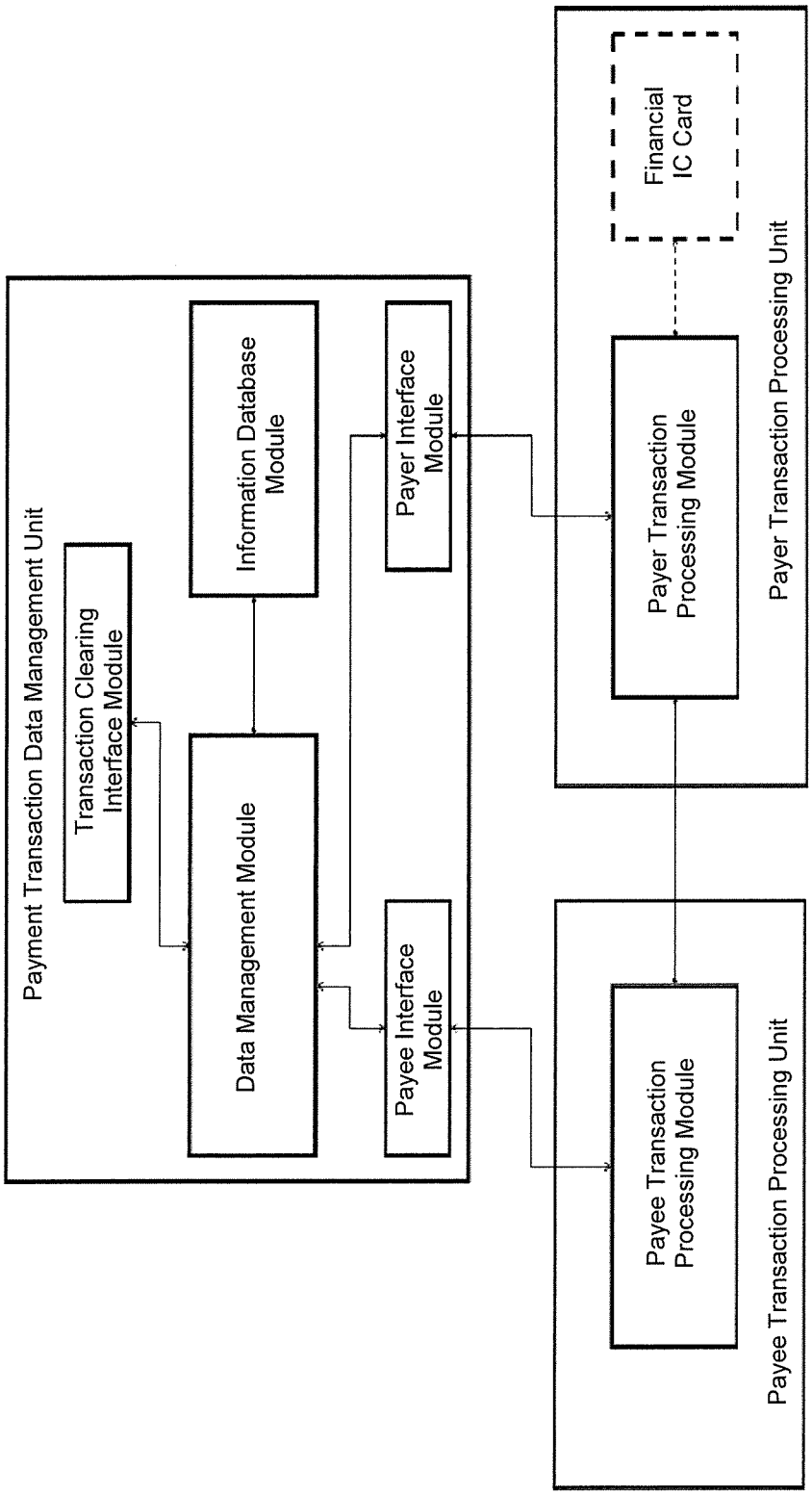
Payment Transaction Data Management Unit
Transaction Clearing Interface Module
Information Database Module
Payer Interface Module
Data Management Module
Payee Interface Module
Payer Transaction Processing Module
Financial IC Card
Payer Transaction Processing Unit
Payee Transaction Processing Module
Payee Transaction Processing Unit

Figure 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG2016/050028

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/40 (2012.01) G06Q 30/00 (2012.01) G07F 7/12 (2006.01) H04L 9/00 (2006.01)

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)

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)

Databases: WPIAP, EPODOC, as well as $PATEN (all English language full-text databases): IPC/CPC's: G06Q20/00, G06Q30/00, H04M11/00, H04L9/00, G07F7/00, G06Q20/382; Keywords include: cell phone, certificate, credit card, dual communication channel, encryption, ic card, merchant, mobile phone, nfc, password, payment platform, pin, pos device, signature, smart card, smart phone, swipe, without mobile banking, and like terms.

Espacenet, Google, Google Patents, Google Scholar: Keywords include: card, channel, device, dual, encryption, financial, IC card, internet, merchant, mobile, nfc, payee, payer, payment, phone, platform, separate, system, transaction data management, transmission, and like terms, and applicant/inventor names. Also searched internal IP Australia databases, The Lens and AusPat for applicant/inventor names.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	Documents are listed in the continuation of Box C	

[X] Further documents are listed in the continuation of Box C [X] See patent family annex

* Special categories of cited documents:

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 March 2016	23 March 2016

Name and mailing address of the ISA/AU	**Authorised officer**
AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA Email address: pct@ipaustralia.gov.au	Robert Foster AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No. 0262223617

INTERNATIONAL SEARCH REPORT C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		International application No. **PCT/SG2016/050028**
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	US 2014/0143155 A1 (NAGRAVISION S.A.) 22 May 2014	
X	Entire document, especially: Abstract, FIG. 2, [0030], [0039]-[0040], [0043], [0045], [0046], [0050]-[0056], [0058]-[0059], [0061], [0064]-[0065], [0068]-[0070], [0073], [0076], [0079], [0088], [0089]-[0092], [0098]-[0099]	1-38
Y	Entire document, especially: FIG. 2, [0039]-[0040], [0079]	5-7, 13, 21-22, 26-29, 35-38
	US 2013/0246203 A1 (PAYDIANT, INC.) 19 September 2013	
X	Entire document, especially: Abstract, FIG.'s 1, 2 & 9, [0033], [0036]-[0037], [0041]-[0042], [0044], [0046], [0052], [0059]-[0060], [0062], [0064], [0080]-[0081], [0119], [0133], [0164]	1-4, 8-12, 14-20, 23-25, 30-34
Y	Entire document, especially: FIG. 9, [0036], [0080], [0067]-[0068]	5-7, 13, 21-22, 26-29, 35-38
	US 2010/0320266 A1 (WHITE) 23 December 2010	
A	Entire document.	1-38

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG2016/050028

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:

because they relate to subject matter not required to be searched by this Authority, namely:

the subject matter listed in Rule 39 on which, under Article 17(2)(a)(i), an international search is not required to be carried out, including

2. ☒ Claims Nos.: **39-41**

because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

See Supplemental Box

3. ☐ Claims Nos:

because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a)

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

Supplemental Box

Continuation of **Box II**

The claims do not comply with Rule 6.2(a) because they rely on references to the description and/or drawings.

INTERNATIONAL SEARCH REPORT Information on patent family members	International application No. **PCT/SG2016/050028**

This Annex lists known patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document/s Cited in Search Report		**Patent Family Member/s**	
Publication Number	**Publication Date**	**Publication Number**	**Publication Date**
US 2014/0143155 A1	22 May 2014	US 2014143155 A1	22 May 2014
		EP 2733654 A1	21 May 2014
		EP 2733655 A1	21 May 2014
		US 2014143150 A1	22 May 2014
US 2013/0246203 A1	19 September 2013	US 2013246203 A1	19 Sep 2013
		AU 2011237387 A1	15 Nov 2012
		AU 2011237387 B2	07 Aug 2014
		AU 2011348061 A1	13 Jun 2013
		AU 2011348061 B2	10 Dec 2015
		AU 2014219386 A1	30 Jul 2015
		CA 2795766 A1	13 Oct 2011
		CA 2819696 A1	28 Jun 2012
		CA 2898205 A1	28 Aug 2014
		CN 102934132 A	13 Feb 2013
		CN 103282929 A	04 Sep 2013
		CN 104641388 A	20 May 2015
		CN 105164708 A	16 Dec 2015
		EP 2556477 A2	13 Feb 2013
		EP 2656292 A2	30 Oct 2013
		EP 2850572 A1	25 Mar 2015
		EP 2951762 A1	09 Dec 2015
		JP 2013529326 A	18 Jul 2013
		JP 2014508338 A	03 Apr 2014
		JP 2015092387 A	14 May 2015
		JP 2015525383 A	03 Sep 2015
		KR 20150132098 A	25 Nov 2015
		US 2011251892 A1	13 Oct 2011
		US 8380177 B2	19 Feb 2013
		US 2012160912 A1	28 Jun 2012
		US 8632000 B2	21 Jan 2014
		US 2014149293 A1	29 May 2014
		US 9208482 B2	08 Dec 2015
		US 2013238455 A1	12 Sep 2013
		US 2013311313 A1	21 Nov 2013
		US 2014191028 A1	10 Jul 2014

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

INTERNATIONAL SEARCH REPORT Information on patent family members	International application No. **PCT/SG2016/050028**

This Annex lists known patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document/s Cited in Search Report		**Patent Family Member/s**	
Publication Number	**Publication Date**	**Publication Number**	**Publication Date**
		US 2015178732 A1	25 Jun 2015
		US 2015186871 A1	02 Jul 2015
		US 2016048830 A1	18 Feb 2016
		WO 2011127354 A2	13 Oct 2011
		WO 2012088512 A2	28 Jun 2012
		WO 2013173339 A1	21 Nov 2013
		WO 2014130222 A1	28 Aug 2014
		WO 2015130967 A1	03 Sep 2015
US 2010/0320266 A1	23 December 2010	US 2010320266 A1	23 Dec 2010
		US 8955747 B2	17 Feb 2015

End of Annex

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.