Computer system and computer-implemented method for processing a card-not-present transaction initiated from an e-commerce site

Field of the invention

[0001] The present invention relates to a computer system and computer-implemented method for processing a card-not-present transaction. In particular, the invention relates to processing a card-not-present transaction with improved security when initiated from an e-commerce site.

Background of the invention

[0002] Card-not-present transactions are gaining popularity in recent years due to the convenience they provide to customers. Typically in online card-not-present transactions, customers are merely required to input their payment card details to a website to purchase their desired goods and services. This enables the customers to shop e.g. at out of office hours, thereby improving customer experience. Nonetheless, coupled with the accessibility of card-not-present transactions are increased risks of fraud as these payment card details may be stolen physically or electronically. The compromised payment card details may then be used for subsequent fraudulent card-not-present transactions without the knowledge and the authorisation of the customer.

[0003] At present, the most common form of validation for card-not-present transactions is authentication using a card verification code (CVC) associated with a payment card. A CVC is typically printed on a payment card and it can be used to verify the physical presence of the payment card for card-not-present transactions. Nonetheless, if the payment card is stolen, the CVC associated with the payment card is also available to the thief. As such, the CVC may not be an adequate security measure for card-not-present transactions.

[0004] In addition, 3D payment gateways may also send and request a one-time password (OTP) from customers for authenticating card-not-present transactions. However, it is often not mandatory for card-not-present transactions to be processed with an OTP, especially for cross-border or international transactions. As such, this additional security measure may not be available to customers at all times.

[0005] It is therefore an aim of the present invention to provide a computer system and computer-implemented method to improve security for card-not-present transactions carried out at e-commerce sites.

Summary of the invention

[0006] In accordance with a first aspect of the present invention, there is provided a payment network server for processing a card-not-present transaction initiated by a cardholder of a payment card on an e-commerce site. The payment network server comprising:

a transaction module configured to:

receive, from a merchant server associated with the e-commerce site, a payment transaction request, the payment transaction request comprising at least a cardholder account number, a payment amount and a combined code entered by the cardholder, the combined code comprising a card verification code (CVC) associated with the payment card and a personal identification number (PIN) associated with the cardholder; and

transmit, to the merchant server, a payment transaction response comprising an approval or a refusal for the card-not-present transaction; and

an authorisation request module configured to:

transmit a request for authorisation to proceed with the card-not-present transaction to an issuer server, wherein the request for authorisation comprises the cardholder account number, the payment amount and either the combined code or the CVC and the PIN derived from the combined code, for the issuer server to verify the CVC and the PIN.

[0007] Embodiments of the invention therefore provide a payment network server that can be used for processing card-not-present transactions initiated by a cardholder of a payment card on an e-commerce site. In particular, to process a card-not-present transaction, a combined code comprising the CVC associated with the payment card and the PIN associated with the cardholder is required to be entered by the cardholder in a CVC input field of an order request to complete the transaction on the e-commerce site. The CVC and the PIN are verified at an issuer server associated with an issuer institution which issued the payment card before the card-not-present transaction is authorised to proceed. This advantageously enhances security for processing a card-not-present transaction as an additional PIN is required to authenticate the cardholder prior to authorising the transaction. In particular, the additional PIN is only known to the cardholder (or anyone authorised by the cardholder) and it is not printed on the payment card. Therefore, even in an event where details of the payment card is known to a third party (e.g. a thief who has stolen the payment card), the third party will not be able to use the payment card in card-not-present transactions since the third party does not have knowledge of the PIN which stays secured with the cardholder. This is especially pertinent in an event where a 3D payment gateway is not available to process the card-not-present transaction in scenarios as discussed above.

[0008] In addition, embodiments of the invention may advantageously use present infrastructure for processing card-not-present transactions using the combined code so that minimal costs will be incurred to implement the above. The primary set-up required is to

maintain PIN data associated with different cardholders at the issuer server which can be easily implemented using existing memory storages, servers and/or databases.

[0009] In some embodiments, the payment network server may split the combined code into the CVC and the PIN. In other embodiments, the combined code may be split into the CVC and the PIN by the issuer server.

[0010] In accordance with a second aspect of the present invention, there is provided an issuer server for processing a card-not-present transaction initiated by a cardholder of a payment card on an e-commerce site, the issuer server comprising:

an authorisation module configured to:

receive, from a payment network server, a request for authorisation to proceed with the card-not-present transaction, the request for authorisation comprising at least a cardholder account number, a payment amount and either a combined code or a card verification code (CVC) and a personal identification number (PIN) derived from the combined code, the combined code comprising the CVC associated with the payment card and the PIN associated with the cardholder; and

verify the combined code or the CVC and the PIN derived from the combined code; and

authorise the card-not-present transaction if the CVC and the PIN are verified.

[0011] The issuer server may comprise:

a registration module configured to:

receive, from a cardholder electronic device associated with the cardholder, a PIN registration request to register the PIN with the issuer institution, the PIN registration request comprising at least details of the payment card; and

transmit, to the cardholder electronic device, a PIN registration response indicating if the PIN registration request has been accepted or refused.

[0012] In accordance with a third aspect of the present invention, there is provided a computer-implemented method performed at a payment network server for processing a card-not-present transaction initiated by a cardholder of a payment card on an e-commerce site, the method comprising:

receiving, from a merchant server associated with the e-commerce site, a payment transaction request, the payment transaction request comprising at least a cardholder account number, a payment amount and a combined code entered by the cardholder, the combined code comprising a card verification code (CVC) associated with the payment card and a personal identification number (PIN) associated with the cardholder;

transmitting a request for authorisation to proceed with the card-not-present transaction, the request for authorisation comprising the cardholder account number, the payment amount and either the combined code or the CVC and the PIN derived from the combined code; and

transmitting, to the merchant server, a payment transaction response comprising an approval or a refusal for the card-not-present transaction.

[0013] In accordance with a fourth aspect of the present invention, there is provided a computer-implemented method performed at an issuer server for processing a card-not-present transaction initiated by a cardholder of a payment card on an e-commerce site, the method comprising:

receiving, from a payment network server, a request for authorisation to proceed with the card-not-present transaction, the request for authorisation comprising at least a cardholder account number, a payment amount and either a combined code or a card verification code (CVC) and a personal identification number (PIN) derived from the combined code, the combined code comprising the CVC associated with the payment card and the PIN associated with the cardholder;

verifying the combined code or the CVC and the PIN derived from the combined code; and

authorising the card-not-present transaction if the CVC and the PIN are verified.

[0014] The method may comprise:

receiving, from a cardholder electronic device associated with the cardholder, a PIN registration request to register the PIN with the issuer institution, the PIN registration request comprising at least details of the payment card; and

transmitting, to the cardholder electronic device, a PIN registration response indicating if the PIN registration request has been accepted or refused.

[0015] The PIN may be static.

[0016] The PIN may comprise a string of numbers, symbols or alphanumeric characters.

[0017] The PIN may be associated with a plurality of payment cards associated with the cardholder issued by the issuer institution.

[0018] The PIN may be associated with a single payment card associated with the cardholder.

[0019] The PIN may be determined by the cardholder and may be comprised in the PIN registration request.

[0020] The PIN may be generated by the issuer server upon receiving the PIN registration request and may be comprised in the PIN registration response.

[0021] The payment transaction request may comprise an expiry date of the payment card.

[0022] The combined code may be entered by the cardholder in a CVC field of the e-commerce site.

[0023] In accordance with a fifth aspect of the present invention, a non-transitory computer-readable medium having stored thereon program instructions for causing at least one processor to perform the preceding method.

[0024] The present invention aims to provide a new and useful computer system and computer-implemented method for processing a card-not-present transaction on an e-commerce site with improved security through the use of a combined code.

Brief description of the drawings

[0025] Non-limiting embodiments of the invention will now be described for the sake of example only, with reference to the following drawings in which:

Fig. 1 shows a computerised system for processing a card-not-present transaction initiated by a cardholder of a payment card on an e-commerce site in accordance with an embodiment of the invention;

Fig. 2 shows steps of a method for processing a card-not-present transaction initiated by a cardholder of a payment card on an e-commerce site in accordance with an embodiment of the invention;

Fig. 3 shows steps of a method for processing the card-not-present transaction at a payment network server which may be used in the computerised system as shown in Fig. 1 in accordance with an embodiment of the invention;

Fig. 4 shows steps of a method for processing the card-not-present transaction at an issuer server which may be used in the computerised system as shown in Fig. 1 in accordance with an embodiment of the invention;

Fig. 5 shows steps of a method for registering a PIN for use in card-not-present transactions in accordance with an embodiment of the invention;

Fig. 6 shows schematically a functional structure of the payment network server which may be used in the computerised system as shown in Fig. 1 in accordance with an embodiment of the invention;

Fig. 7 shows schematically a functional structure of the issuer server which may be used in the computerised system as shown in Fig. 1 in accordance with an embodiment of the invention; and

Fig. 8 shows schematically a hardware structure of a server which may be used in the computerised system of Fig. 1 to implement a method in accordance with an embodiment of the invention.

Detailed description of the embodiment

[0026] As used in this document, the term "payment card" refers to any electronic cashless payment vehicle associated with a payment account, such as a credit card, a debit card, a prepaid card, a charge card, a membership card, a promotional card, a frequent flyer card, an identification card, a prepaid card, a gift card, and/or any other payment device that may hold payment account information, such as mobile phones, Smartphones, personal digital assistants (PDAs), key fobs, transponder devices, NFC-enabled devices, and/or computers.

[0027] Note that the term "institution" is used here in a sense which is not necessarily limited to organizations which are legally constituted as banks, since in some jurisdictions other organizations may be permitted to maintain financial accounts such as a payment card account. An institution may be one of the following: a bank, a financial technology company, a telecommunication company or a financial institution.

[0028] As used in this application, the terms "component," "module," "system," "apparatus," "interface," or the like are generally intended to refer to a computer-related entity, either hardware, a combination of hardware and software, software, or software in execution. For example, a component or a module may be, but is not limited to being, a process running on a processor, a processor, an object, an executable, a thread of execution, a program, and/or a computer. By way of illustration, both an application running on a controller and the controller can be a component or a module. One or more components/modules may reside within a process and/or thread of execution and a component may be localized on one computer and/or distributed between two or more computers.

[0029] Furthermore, the claimed subject matter may be implemented as a method, apparatus, or article of manufacture using standard programming and/or engineering techniques to produce software, firmware, hardware, or any combination thereof to control a computer to implement the disclosed subject matter. For instance, the claimed subject matter may be implemented as a computer-readable medium embedded with a computer executable program, which encompasses a computer program accessible from any computer-readable storage device or storage media. For example, computer readable media can include but are not limited to magnetic storage devices (e.g., hard disk, floppy disk, magnetic

strips . . .), optical disks (e.g., compact disk (CD), digital versatile disk (DVD) . . .), smart cards, and flash memory devices (e.g., card, stick, key drive . . .).

[0030] Fig. 1 shows a computerised system 100 for processing a card-not-present transaction initiated by a cardholder of a payment card on an e-commerce site in accordance with an embodiment of the invention. The computerised system 100 comprises a payment network server 108 which facilitates a payment transaction between a cardholder and a merchant. The payment network server 108 is a server associated with a payment network such as the Banknet payment network operated by MasterCard®. As shown in Fig. 1, the payment network server 108 is in communication with an acquirer server 106 and an issuer server 110. The acquirer server 106 is operated by an acquirer institution at which the merchant maintains an account to receive funds. The issuer server 110 is associated with an issuer institution which maintains payment card accounts and provides payment cards to cardholders for performing payment card transactions (e.g. card-not-present transactions) over the payment network. The computerised system 100 further comprises a cardholder electronic device 102 and a merchant server 104. The cardholder electronic device 102 may be any electronic device which enables the cardholder to purchase product(s) online through e-commerce sites. The cardholder electronic device 102 may be a mobile phone, a laptop/notebook, a desktop, a tablet, a personal digital assistants (PDA), a key fob, a transponder device, a NFC-enabled device, and/or a computer. The merchant server 104 is associated with the e-commerce site on which the card-not-present transaction is initiated. Moreover, an issuer database 112 is operationally connected to the issuer server 110. The issuer database 112 serves at least to store data related to personal identification numbers (PINs) associated with a plurality of cardholders of payment cards issued by the issuer institution. Each PIN may be associated with the cardholder such that one PIN is associated with all or some of the payment cards issued by the issuer institution, or each PIN may be uniquely associated with each payment card issued by the issuer institution.

[0031] Compared to conventional methods for card-not-present transactions, the present invention provides a combined code comprising a card verification code (CVC) and a PIN for verifying card-not-present transactions. Once a cardholder confirms his/her order on an e-commerce website, the cardholder is typically directed to a payment page where payment details are required to be filled in to complete the card-not-present transaction. Payment details may include a name of the cardholder, a cardholder account number (e.g. a payment card number), an expiry date of the payment card, a CVC etc. In an embodiment of the present invention, there is provided a field among the payment details where the cardholder is required to input a combined code comprising a CVC of a payment card and a PIN associated with the cardholder. The field maybe a CVC field that allows input of a combined code (e.g. a CVC field that allows input of a longer string of

numerals/characters instead of the standard 3-numeral length CVC found in most payment cards). In an embodiment, the PIN is unique to the payment card used for the card-not-present transaction such that one PIN is associated with each payment card. In another embodiment, the PIN is uniquely associated with each issuer institution. In this case, a same PIN may be used for all payment cards associated with the cardholder that are issued with a same issuer institution. In another embodiments, the same PIN may be used by a cardholder for all of his/her payment cards regardless of whether they are associated with one or more issuer institutions.

[0032] Once the payment details have been completed, the cardholder can submit these details on the e-commerce website to complete the card-not-present transaction. In some embodiments, the payment details comprise at least a cardholder account number associated with the payment card and the combined code. The payment details may comprise an expiry date of the payment card and/or a name of the cardholder. These payment details are comprised in a form of a payment transaction request which is received at the merchant server 104 and subsequently forwarded to the payment network server 108 via the acquirer server 106. The payment network server 108 is configured to receive the payment transaction request. In some embodiments, the payment network server 108 processes the card-not-present transaction in a conventional way such that it is not necessary for the cardholder to register for this service with a service provider (e.g. a payment network service provider) prior to using a combined code for processing the card-not-present transaction.

[0033] The payment network server 108 is configured to identify the issuer institution associated with the payment card used for processing the card-not-present transaction and to transmit a request for authorisation to the issuer server 110 associated with the issuer institution. The request for authorisation may comprise the cardholder account number, the payment amount and either the combined code or the CVC and the PIN derived from the combined code, for the issuer server 110 to verify the CVC and the PIN. The combined code may be split into the CVC and the PIN either at the payment network server 108 prior to transmitting the request for authorisation, or it may be split at the issuer server 110 prior to verifying the CVC and the PIN. In an embodiment, the issuer server 110 may be capable of verifying the CVC and the PIN in their combined form. In any case, the issuer server 110 is configured to verify the CVC and the PIN. Verification of the CVC and the PIN may comprise determining if the CVC and the PIN received in the payment transaction request match those on record in the issuer database 112. Registration of the PIN by the cardholder at the issuer institution is discussed later in conjunction with Fig. 3. The issuer server 110 may perform additional checks such as (i) whether the cardholder account associated with the payment card has sufficient balance to carry out the card-not-present

transaction and/or (ii) whether the expiry date of the payment card is still valid etc. The issuer server 110 may also transmit a dynamic one-time-password (OTP) to the cardholder for further authentication prior to authorisation of the card-not-present transaction. In other words, the present invention of verifying the combined code comprising the CVC and the PIN may work in combination with a dynamic OTP to provide enhanced security for the card-not-present transaction. After at least the CVC and the PIN have been verified by the issuer server 110 (and any other checks performed if necessary), the issuer server 110 is configured to transmit a response for authorisation to the payment network server 108, the response for authorisation indicating if the card-not-present transaction is authorised and can proceed. The payment network server 108 receives the response for authorisation, and in turn transmits a payment transaction response comprising an approval or a refusal for the card-not-present transaction, to the merchant server 104 via the acquirer server 106. The merchant server 104 may notify the cardholder of a result of the card-not-present transaction via the e-commerce website accessible via the cardholder electronic device 102. The issuer server 110 may notify the cardholder that the payment amount has been deducted from his/her payment account if the card-not-present transaction is successful.

[0034] Although only one cardholder electronic device 102 and only one merchant server 104 is shown in Fig. 1, a plurality of cardholder electronic devices 102 and a plurality of merchant servers 104 associated with respective e-commerce sites may also form part of the computerised system 100. Similarly, a plurality of acquirer servers 106 and a plurality of issuer servers 110 may also be in communication with the payment network server 108 and form part of the computerised system 100. Communication between the cardholder electronic device 102, servers and databases may take place via any type of system, for example, a virtual private system (VPN), the Internet, a local area and/or wide area system (LAN and/or WAN), and so on.

[0035] Fig. 2 shows steps of a method 200 for processing a card-not-present transaction initiated by a cardholder of a payment card on an e-commerce site in accordance with an embodiment of the invention. The method 200 may be carried out using the system 100 as shown in Fig. 1. Steps 202, 204 and 208 may be carried out by the payment network server 108 while a step 206 may be carried out by the issuer server 110.

[0036] In the step 202, the payment network server 108 is configured to receive a payment transaction request from the merchant server 104 associated with the e-commerce site (i.e. via the acquirer server 106). The payment transaction request comprises at least the cardholder account number, the payment amount and the combined code entered by the cardholder, the combined code comprising a card verification code (CVC) associated with the payment card and a personal identification number (PIN) associated with the

cardholder. The payment amount is associated with the card-not-present transaction and is an amount which the cardholder is required to pay for his/her order made on the e-commerce site. In some embodiments, the combined code is entered by the cardholder in a CVC field of the e-commerce site.

[0037] In the step 204, the payment network server 108 is configured to transmit a request for authorisation to proceed with the card-not-present transaction. The authorisation request comprises the cardholder account number, the payment amount and either the combined code or the CVC and the PIN derived from the combined code.

[0038] In the step 206, the issuer server 110 is configured to authorise the card-not-present transaction if the CVC and the PIN are verified. After the CVC and the PIN are verified, the issuer server 110 is configured to transmit a response for authorisation to the payment network server 108, where the response for authorisation indicates if the card-not-present transaction is authorised and can proceed.

[0039] In the step 208, the payment network server 108 is configured to transmit, to the merchant server 104, a payment transaction response comprising an approval or a refusal for the card-not-present transaction. The payment network server 108 is configured to transmit the payment transaction response once it has received the response for authorisation of the card-not-present transaction from the issuer server 110 in the step 206.

[0040] Figs. 3 and 4 provide further details of the steps carried out by the payment network server 108 and the issuer server 110 respectively for processing the card-not-present transaction.

[0041] Fig. 3 shows steps of a method 300 for processing the card-not-present transaction at the payment network server 108 which may be used in the computerised system 100 as shown in Fig. 1 in accordance with an embodiment of the invention.

[0042] In a step 302, the payment network server 108 is configured to receive a payment transaction request from the merchant server 104 associated with the e-commerce site (i.e. via the acquirer server 106). This is similar to the step 202 as described in the method 200 for processing the card-not-present transaction by the system 100. The payment transaction request comprises at least the cardholder account number, the payment amount and the combined code entered by the cardholder, the combined code comprising a card verification code (CVC) associated with the payment card and a personal identification number (PIN) associated with the cardholder. The payment amount is associated with the card-not-present transaction and is an amount which the cardholder is required to pay for his/her order made on the e-commerce site. In some embodiments, the combined code is entered by the cardholder in a CVC field of the e-commerce site. The

CVC field on the e-commerce site, which typically holds a length of three numerals, may be expanded so as to accommodate the PIN portion of the combined code. The length of the PIN may be decided by the issuer institution. The length of the PIN may be standardised across all issuer institutions which provide authorisation of card-not-present transactions using a combined code. The PIN may comprise a string of numbers, symbols or alphanumeric characters. In some embodiments, the PIN may consist of a string of 3 or 4 numbers.

[0043] In a step 304, the payment network server 108 is configured to transmit a request for authorisation to proceed with the card-not-present transaction to the issuer server 110. The authorisation request comprises the cardholder account number, the payment amount and either the combined code or the CVC and the PIN derived from the combined code. In an embodiment, the payment network server 108 is configured to determine if a combined code is received as part of the payment transaction request for the card-not-present transaction (e.g. by the length of the combined code in comparison with the standard CVC which is generally of a length of 3 numerals). The payment network server 108 may be configured to split the combined code into the CVC and the PIN before transmitting the CVC and the PIN to the issuer server 110.

[0044] In a step 306, the payment network server 108 is configured to transmit, to the merchant server 104, a payment transaction response comprising an approval or a refusal for the card-not-present transaction. The payment network server 108 is configured to transmit the payment transaction response once it has received the response for authorisation of the card-not-present transaction from the issuer server 110.

[0045] Fig. 4 shows steps of a method 400 for processing the card-not-present transaction at the issuer server 110 which may be used in the computerised system 100 as shown in Fig. 1 in accordance with an embodiment of the invention.

[0046] In a step 402, the issuer server 110 is configured to receive, from the payment network server 108, a request for authorisation to proceed with the card-not-present transaction. The authorisation request comprises the cardholder account number, the payment amount and either the combined code or the CVC and the PIN derived from the combined code.

[0047] In a step 404, the issuer server 110 is configured to verify the combined code or the CVC and the PIN derived from the combined code. In an embodiment, if the combined code is not split into the CVC and the PIN, the issuer server 110 is configured to determine if a combined code is received in the step 402 as part of the request for authorisation of the card-not-present transaction (e.g. by the length of the combined code in comparison with the standard CVC which is generally of a length of 3 numerals) and to split the combined

code into the CVC and the PIN. To verify the CVC and the PIN received, the issuer server 110 may be configured to determine if the CVC and the PIN in the payment transaction request match those on record in the issuer database 112. In other words, the step 404 comprises a combined verification of the CVC and the PIN which advantageously minimises processing time for authorisation since the process of verification/authorisation is only carried out by one party (i.e. the issuer server 110).

[0048] In a step 406, the issuer server 110 is configured to authorise the card-not-present transaction if the CVC and the PIN are verified. The issuer server 110 may be configured to transmit a response for authorisation to the payment network server 108, where the response for authorisation indicates if the card-not-present transaction is authorised and can proceed.

[0049] Fig. 5 shows steps of a method for registering a PIN for use in a card-not-present transaction in accordance with an embodiment of the invention. The method 500 may be carried out by the issuer server 110 of the system 100 as shown in Fig. 1.

[0050] In a step 502, the issuer server 110 is configured to receive, from the cardholder electronic device 102 associated with the cardholder, a PIN registration request to register the PIN with the issuer institution. The PIN registration request comprises at least details of the payment card. The details of the payment card may include a name of the cardholder, a cardholder account number, an expiry date of the payment card and/or a CVC of the payment card.

[0051] In a step 504, the issuer server 110 is configured to transmit, to the cardholder electronic device 102, a PIN registration response indicating if the PIN registration request has been accepted or refused. The PIN registration response may comprise the PIN registered at the issuer server 110. Once the PIN registration is successful, the issuer server 110 is configured to store the PIN associated with the payment card (e.g. in the scenario where each PIN is uniquely associated with the payment card) or the cardholder (e.g. in the scenario where each PIN is uniquely associated with all or some of the payment cards issued by the issuer institution in the name of the cardholder) in the issuer database 112. The PIN may be stored in association with relevant data such that it may be retrieved from the issuer database 112 for verification purposes e.g. in the step 404 as described above.

[0052] In some embodiments, the PIN is static. In other words, the PIN is fixed such that the same PIN may be used for multiple card-not-present transactions. The PIN may be determined by the cardholder. In this case, the PIN is predetermined and comprised in the registration request when the registration request is transmitted from the cardholder

electronic device 102 to the issuer server 110. In another embodiment, the PIN is generated by the issuer server 110 upon receiving the PIN registration request from the customer electronic device 102. In this case, the generated PIN may be comprised in the PIN registration response so that the cardholder is notified of the generated PIN upon successful registration. In some embodiments, the cardholder is provided options at registration to select if the PIN registered is to be associated with only one payment card or is to be associated with all or some of the payment cards issued by the issuer institution in the name of the cardholder.

[0053] Fig. 6 shows schematically a structure 600 of the payment network server 108 comprised in the computerised system 100 in accordance with embodiments of the invention. The structure 600 of the payment network server 108 comprises at least a communication module 602, a transaction module 604 and an authorisation request module 606.

[0054] The communication module 602 is configured to enable the payment network server 108 to communicate with at least the acquirer server 106 and the issuer server 110 as provided in the computerised system 100. The communication module 602 is configured to work in tandem with other modules of the payment network server 108 as discussed in more detail below.

[0055] The transaction module 604 is configured to allow the payment network server 108 to process a payment transaction request. In other words, the transaction module 602 is configured, via the communication module 602, to receive the payment transaction request from the merchant server 104 associated with the e-commerce site where the payment transaction request comprises at least the cardholder account number, the payment amount and the combined code entered by the cardholder. After the card-not-present transaction has been processed, the transaction module 602 is configured, via the communication module 602, to transmit a payment transaction response comprising an approval or a refusal for the card-not-present transaction to the merchant server 104. In an embodiment, the transaction module 604 is configured to split the combined code received in the payment transaction request to the CVC and the PIN. The transaction module 604 may transmit the relevant information isolated from the payment transaction request to other modules of the payment network server 108 for further processing.

[0056] The authorisation request module 606 is configured to transmit, via the communication module 602, a request for authorisation to proceed with the card-not-present transaction to the issuer server 110. The request for authorisation comprises the cardholder account number, the payment amount and either the combined code or the pair of CVC and PIN derived from the combined code. In the embodiment where the transaction module 404

has split the combined code received to the CVC and the PIN, the authorisation request module 606 is configured to transmit the pair of CVC and PIN to the issuer server 110 for authorisation of the card-not-present transaction.

[0057] Fig. 7 shows schematically a structure 700 of the issuer server 110 comprised in the computerised system 100 in accordance with embodiments of the invention. The structure 700 of the issuer server 110 comprises a communication module 702, an authorisation module 704 and a registration module 706.

[0058] The communication module 702 is configured to enable the issuer server 110 to communicate with at least the payment network server 108 and the cardholder electronic device 102 as provided in the computerised system 100. The communication module 502 is configured to work in tandem with other modules of the issuer server 110 as discussed in more detail below.

[0059] The authorisation module 704 is configured to receive, from the payment network server 108, a request for authorisation to proceed with the card-not-present transaction. The request for authorisation may comprise at least a cardholder account number, a payment amount and either a combined code or a card verification code (CVC) and a personal identification number (PIN) derived from the combined code. The authorisation module 704 may be configured to split the combined code into the CVC and the PIN if the combined code has not been split at the payment network server 108. In some embodiments, the authorisation module 704 is configured to verify the CVC and the PIN derived from the combined code. In other embodiments, the authorisation module 704 is configured to verify the CVC and the PIN in their combined form (i.e. the combined code as it is). To verify the CVC and the PIN, the authorisation module 704 may be configured to determine if the CVC and the PIN received in the payment transaction request match those on record in the issuer database 112. The authorisation module 704 may be configured to perform additional checks such as (i) whether the cardholder account associated with the payment card has sufficient balance to carry out the card-not-present transaction and/or (ii) whether the expiry date of the payment card is still valid etc. The authorisation module 704 may be configured to transmit a dynamic one-time-password (OTP) to the cardholder for further authentication prior to authorisation of the card-not-present transaction. In an embodiment, the authorisation module 704 may be configured to verify the combined code comprising the CVC and the PIN in combination with a dynamic OTP to provide enhanced security for processing the card-not-present transaction. The authorisation module 704 may be configured to authorise the card-not-present transaction if at least the CVC and the PIN are verified. After the necessary verifications/checks have been completed, the authorisation module 704 may be

configured, via the communication module 702, to transmit a response for authorisation to the payment network server 108 where the response for authorisation indicates if the card-not-present transaction is authorised and can proceed.

[0060] The registration module 706 is configured to register cardholders/payment cards for authorisation of card-not-present transactions using a combined code with the issuer database 112. In particular, the registration module 706 may be configured to receive, via the communication module 702, a PIN registration request to register the PIN with the issuer institution from the cardholder via the cardholder electronic device 102. The PIN registration request comprises at least details of the payment card. The details of the payment card may include a name of the cardholder, a cardholder account number, an expiry date of the payment card and/or a CVC of the payment card. Once the registration has been processed, the registration module 706 may be configured, via the communication module 702, to transmit a PIN registration response indicating if the PIN registration request has been accepted or refused to the cardholder electronic device 102. In an embodiment where the PIN is determined by the cardholder, the predetermined PIN is comprised in the registration request when the registration request is transmitted from the cardholder electronic device 102 to the issuer server 110. The registration module 706 may be configured to extract the predetermined PIN from the registration request and store it in the issuer database 112. In an embodiment, the PIN is generated by the registration module 706 upon receiving the PIN registration request from the customer electronic device 102. In this case, the generated PIN may be comprised in the PIN registration response so that the cardholder is notified of the generated PIN upon successful registration. A copy of the generated PIN is also stored in the issuer database 112 in this case.

[0061] Fig. 8 is a block diagram showing a technical architecture of the payment network server 108. The issuer server 110 and/or the acquirer server 106 may also have this technical architecture. The merchant server 104 may share a similar technical architecture.

[0062] The technical architecture includes a processor 802 (which may be referred to as a central processor unit or CPU) that is in communication with memory devices including secondary storage 804 (such as disk drives), read only memory (ROM) 806, and random access memory (RAM) 808. The processor 802 may be implemented as one or more CPU chips. The technical architecture may further comprise input/output (I/O) devices 810, and system connectivity devices 812.

[0063] The secondary storage 804 is typically comprised of one or more disk drives or tape drives and is used for non-volatile storage of data and as an over-flow data storage device if RAM 808 is not large enough to hold all working data. Secondary storage 804 may be

used to store programs which are loaded into RAM 808 when such programs are selected for execution.

[0064] In this embodiment, the secondary storage 804 has a processing component 804a comprising non-transitory instructions operative by the processor 802 to perform various operations of the method of the present disclosure. The ROM 806 is used to store instructions and perhaps data which are read during program execution. The secondary storage 804, the RAM 808, and/or the ROM 806 may be referred to in some contexts as computer readable storage media and/or non-transitory computer readable media.

[0065] I/O devices 810 may include printers, video monitors, liquid crystal displays (LCDs), plasma displays, touch screen displays, keyboards, keypads, switches, dials, mice, track balls, voice recognizers, card readers, paper tape readers, or other input devices.

[0066] The system connectivity devices 812 may take the form of modems, modem banks, Ethernet cards, universal serial bus (USB) interface cards, serial interfaces, token ring cards, fiber distributed data interface (FDDI) cards, wireless local area system (WLAN) cards, radio transceiver cards that promote radio communications using protocols such as code division multiple access (CDMA), global system for mobile communications (GSM), long-term evolution (LTE), worldwide interoperability for microwave access (WiMAX), near field communications (NFC), radio frequency identity (RFID), and/or other air interface protocol radio transceiver cards, and other system devices. These system connectivity devices 812 may enable the processor 812 to communicate with the Internet or one or more intranets. With such a system connection, it is contemplated that the processor 802 might receive information from the system, or might output information to the system in the course of performing the above-described method operations. Such information, which is often represented as a sequence of instructions to be executed using processor 802, may be received from and outputted to the system, for example, in the form of a computer data signal embodied in a carrier wave.

[0067] The processor 802 executes instructions, codes, computer programs, scripts which it accesses from hard disk, floppy disk, optical disk (these various disk based systems may all be considered secondary storage 804), flash drive, ROM 806, RAM 808, or the system connectivity devices 812. While only one processor 802 is shown, multiple processors may be present. Thus, while instructions may be discussed as executed by a processor, the instructions may be executed simultaneously, serially, or otherwise executed by one or multiple processors.

[0068] Although the technical architecture is described with reference to a computer, it should be appreciated that the technical architecture may be formed by two or more computers in

communication with each other that collaborate to perform a task. For example, but not by way of limitation, an application may be partitioned in such a way as to permit concurrent and/or parallel processing of the instructions of the application. Alternatively, the data processed by the application may be partitioned in such a way as to permit concurrent and/or parallel processing of different portions of a data set by the two or more computers. In an embodiment, virtualization software may be employed by the technical architecture to provide the functionality of a number of servers that is not directly bound to the number of computers in the technical architecture. In an embodiment, the functionality disclosed above may be provided by executing an application and/or applications in a cloud computing environment. Cloud computing may comprise providing computing services via a system connection using dynamically scalable computing resources. A cloud computing environment may be established by an enterprise and/or may be hired on an as-needed basis from a third party provider.

[0069] It is understood that by programming and/or loading executable instructions onto the technical architecture, at least one of the CPU 802, the RAM 808, and the ROM 806 are changed, transforming the technical architecture in part into a specific purpose machine or apparatus having the novel functionality taught by the present disclosure. It is fundamental to the electrical engineering and software engineering arts that functionality that can be implemented by loading executable software into a computer can be converted to a hardware implementation by well-known design rules.

[0070] Whilst the foregoing description has described exemplary embodiments, it will be understood by those skilled in the art that many variations of the embodiments can be made within the scope of the present invention as defined by the claims. Moreover, features of one or more embodiments may be mixed and matched with features of one or more other embodiments.

Claims

1. A payment network server for processing a card-not-present transaction initiated by a cardholder of a payment card on an e-commerce site, the payment network server comprising:

a transaction module configured to:

receive, from a merchant server associated with the e-commerce site, a payment transaction request, the payment transaction request comprising at least a cardholder account number, a payment amount and a combined code entered by the cardholder, the combined code comprising a card verification code (CVC) associated with the payment card and a personal identification number (PIN) associated with the cardholder; and

transmit, to the merchant server, a payment transaction response comprising an approval or a refusal for the card-not-present transaction; and

an authorisation request module configured to:

transmit a request for authorisation to proceed with the card-not-present transaction to an issuer server, wherein the request for authorisation comprises the cardholder account number, the payment amount and either the combined code or the CVC and the PIN derived from the combined code, for the issuer server to verify the CVC and the PIN.

2. An issuer server for processing a card-not-present transaction initiated by a cardholder of a payment card on an e-commerce site, the issuer server comprising:

an authorisation module configured to:

receive, from a payment network server, a request for authorisation to proceed with the card-not-present transaction, the request for authorisation comprising at least a cardholder account number, a payment amount and either a combined code or a card verification code (CVC) and a personal identification number (PIN) derived from the combined code, the combined code comprising the CVC associated with the payment card and the PIN associated with the cardholder;

verify the combined code or the CVC and the PIN derived from the combined code; and

authorise the card-not-present transaction if the CVC and the PIN are verified.

3. The server of claim 2 further comprising a registration module configured to:

receive, from a cardholder electronic device associated with the cardholder, a PIN registration request to register the PIN with the issuer institution, the PIN registration request comprising at least details of the payment card; and

transmit, to the cardholder electronic device, a PIN registration response indicating if the PIN registration request has been accepted or refused.

4. The server of claim 2 or claim 3 wherein the PIN is static.

5. The server of any one of claims 2 to 4 wherein the PIN comprises a string of numbers, symbols or alphanumeric characters.

6. The server of any one of claims 2 to 5 wherein the PIN is associated with a plurality of payment cards associated with the cardholder issued by the issuer institution.

7. The server of any one of claims 2 to 5 wherein the PIN is associated with a single payment card associated with the cardholder.

8. The server of any one of claims 3 to 7 wherein the PIN is determined by the cardholder and is comprised in the PIN registration request.

9. A computer-implemented method performed at a payment network server for processing a card-not-present transaction initiated by a cardholder of a payment card on an e-commerce site, the method comprising:

receiving, from a merchant server associated with the e-commerce site, a payment transaction request, the payment transaction request comprising at least a cardholder account number, a payment amount and a combined code entered by the cardholder, the combined code comprising a card verification code (CVC) associated with the payment card and a personal identification number (PIN) associated with the cardholder;

transmitting a request for authorisation to proceed with the card-not-present transaction, the request for authorisation comprising the cardholder account number, the payment amount and either the combined code or the CVC and the PIN derived from the combined code; and

transmitting, to the merchant server, a payment transaction response comprising an approval or a refusal for the card-not-present transaction.

10. A computer-implemented method performed at an issuer server for processing a card-not-present transaction initiated by a cardholder of a payment card on an e-commerce site, the method comprising:

receiving, from a payment network server, a request for authorisation to proceed with the card-not-present transaction, the request for authorisation comprising at least a cardholder account number, a payment amount and either a combined code or a card

verification code (CVC) and a personal identification number (PIN) derived from the combined code, the combined code comprising the CVC associated with the payment card and the PIN associated with the cardholder;

verifying the combined code or the CVC and the PIN derived from the combined code; and

authorising the card-not-present transaction if the CVC and the PIN are verified.

11. The method of claim 10 further comprising:

receiving, from a cardholder electronic device associated with the cardholder, a PIN registration request to register the PIN with the issuer institution, the PIN registration request comprising at least details of the payment card; and

transmitting, to the cardholder electronic device, a PIN registration response indicating if the PIN registration request has been accepted or refused.

12. The method of claim 10 or claim 11 wherein the PIN is static.

13. The method of any one of claims 10 to 12 wherein the PIN comprises a string of numbers, symbols or alphanumeric characters.

14. The method of any one of claims 10 to 13 wherein the PIN is associated with a plurality of payment cards associated with the cardholder issued by the issuer institution.

15. The method of any one of claims 10 to 13 wherein the PIN is associated with a single payment card associated with the cardholder.

16. The method of any one of claims 11 to 15 wherein the PIN is determined by the cardholder and is comprised in the PIN registration request.

17. The method of any one of claims 11 to 15, wherein the PIN is generated by the issuer server upon receiving the PIN registration request and is comprised in the PIN registration response.

18. The method of any one of claims 10 to 17, wherein the payment transaction request further comprises an expiry date of the payment card.

19. The method of any one of claims 10 to 18, wherein the combined code is entered by the cardholder in a CVC field of the e-commerce site.

20. A non-transitory computer-readable medium having stored thereon program instructions for causing at least one processor to perform the method according to any one of claims 10 to 19.