

Computer system and computer-implemented method for authenticating a card-not-present payment transaction

Technical Field

[0001] The present disclosure relates to a computer system and computer-implemented method for processing a card-not-present payment transaction, and in particular for authenticating a card-not-present payment transaction.

Background

[0002] With the rise of electronic commerce (e-commerce) in recent years, card-not-present payment transactions are becoming ubiquitous. In order to minimise fraud, regulators in various jurisdictions have mandated specific protocols for authenticating users in card-not-present payment transactions. For example, the Indian regulator requires a second-factor authentication with issuer involvement for all card-not-present payment transactions.

[0003] Although card verification methods such as the second-factor authentication performed by the issuer reduce fraud in card-not-present payment transactions, they increase friction in processing these card-not-present payment transactions. This results in a high drop-off rate and a poor customer experience for users of these card-not-present payment transactions.

Summary

[0004] In accordance with a first aspect of the present invention, there is provided a merchant server for authenticating a card-not-present payment transaction initiated by a user at a merchant portal using a user device. The merchant server comprising a transaction module and an authentication module. The transaction module is configured to receive a transaction request from the user device where the transaction request comprises at least a payment card identifier and a user device identifier associated with the user device. The authentication module is configured to: (i) determine whether the payment card identifier and the user device identifier are registered for making payment at the merchant portal; (ii) transmit an authentication request to the user device to authenticate the card-not-present payment transaction if the payment card identifier and the user device identifier are registered for making payment at the merchant portal where the authentication request comprises a request for an authentication information input; (iii) receive an authentication response from the user device where the authentication response comprises the authentication information input; (iv) authenticate the authentication information input using stored authentication information registered for authenticating card-not-present payment transactions between the user and the merchant using the user device and the payment

card identifier; and (v) transmit an authorisation request comprising an authentication indication to an issuer server to indicate that the authentication information input has been authenticated.

[0005] Embodiments of the present invention provide a merchant server for authenticating a card-not-present payment transaction initiated by a user at a merchant portal using a user device. The server comprises a transaction module and an authentication module. The transaction module is configured to receive a transaction request comprising at least a payment card identifier and a user device identifier associated with the user device from the user device and the authentication module is configured to: (i) determine whether the payment card identifier and the user device identifier are registered for making payment at the merchant portal; (ii) transmit an authentication request to the user device where the authentication request comprises a request for an authentication information input to authenticate the card-not-present payment transaction if the payment card identifier and the user device identifier are registered for making payment at the merchant portal; (iii) receive an authentication response comprising the authentication information input from the user device; (iv) authenticate the authentication information input using stored authentication information registered for authenticating card-not-present payment transactions between the user and the merchant using the user device and the payment card identifier; and (v) transmit, to the issuer server, an authorisation request comprising an authentication indication to indicate that the authentication information input has been authenticated. As will be described in relation to subsequent figures, the authentication information stored in association with the user may be registered either with the merchant server or with a network server. This registered authentication information can then be used to authenticate the user in processing the card-not-present payment transaction. In this way, authentication of the user and the card-not-present payment transaction is delegated from the issuer server (or an access control server (ACS) associated with the issuer server) in the present framework to the merchant server and/or the network server so that it is no longer necessary for the user to be authenticated via a second-factor authentication by the issuer for every card-not-present payment transactions. This provides a better user experience since authentication of the card-not-present payment transaction no longer relies on an accessibility of the second-factor authentication (e.g. a one-time passcode received via Short Messaging Service (SMS) using a telecommunication network), thereby reducing friction in processing the card-not-present payment transaction. This may also improve an efficiency and a reliability in processing card-not-present payment transactions since a reliance on the uptime of the ACS and potential SMS delivery delays can be avoided. This will help to improve the approval rates for card not present transactions.

[0006] In addition, embodiments of the present invention may be readily implemented using existing infrastructures so that minimal costs will be incurred to execute the above. The primary set-up required is to store information in relation to authentication information registered for use in authenticating card-not-present payment transactions. This can be easily implemented using existing memory storages, servers and/or databases. A software development kits (SDK) can be provided to the merchant for incorporating the necessary plug-ins/functions to the merchant portal for executing the exemplary embodiments.

[0007] The authentication module may be configured to: (i) transmit, to the issuer server, an authorisation request if it is determined that the payment card identifier and the user device are not registered for making payment at the merchant portal, the authorisation request comprises a request to generate an authentication code for authenticating the user; (ii) receive, from the user device, an authentication code input; (iii) transmit, to the issuer server, the authentication code input; and (iv) receive, from the issuer server, an authorisation response indicating that the card-not-present payment transaction is authorised if it is determined that the authentication code input matches the authentication code; and the server may comprise an enrolment module configured to: (i) transmit, to the user device, an enrolment request if the card-not-present payment transaction is authorised, the enrolment request comprising a request for registering the authentication information for authenticating card-not-present payment transactions between the user and the merchant using the user device and the payment card identifier; (ii) receive, from the user device, an enrolment response comprising the authentication information; and (iii) store registration information for the user for making payment at the merchant portal, the registration information comprising the authentication information, the payment card identifier and the user device identifier.

[0008] The registration of the user for authenticating card-not-present payment transactions as described above may involve conventional second-factor authentication performed by the issuer server. This helps to ensure an authenticity of the user during registration, while at the same time, may satisfy regulators who require a second-factor authentication with issuer involvement for card-not-present payment transactions.

[0009] The registration and authentication of authentication information may also be performed by a network server such as an identity check Mobile Platform by Mastercard®. Where the authentication information is registered using the network server, the enrolment module may be configured to: (i) retrieve, from a merchant database, a merchant identifier associated with the merchant portal; and (ii) transmit, to the network server, the authentication information, the payment card identifier, the user device identifier and the merchant identifier for registering the authentication information for authenticating card-not-

present payment transactions between the user and the merchant using the user device and the payment card identifier; wherein the registration information is stored at the network server.

[0010] The authentication module may be configured to: (i) transmit, to the network server, a registration determination request comprising the payment card identifier, the user device identifier and the merchant identifier; and (ii) receive, from the network server, a registration determination response comprising a registration indication indicating if the payment card identifier and the user device identifier are registered for making payment at the merchant portal.

[0011] The authentication module may be configured to: (i) transmit, to the network server, a user verification request comprising the authentication information input; and (ii) receive, from the network server, a user verification response comprising an authentication indication if the authentication information input matches the authentication information stored at the network server.

[0012] The merchant server may comprise a monitoring module, the monitoring module may be configured to: (i) analyse past card-not-present payment transactions performed using the user device; (ii) generate a user transaction pattern based on the past card-not-present payment transactions; and (iii) determine that the card-not-present payment transaction is an unusual payment transaction if the card-not-present payment transaction does not conform to the user transaction pattern associated with the past card-not-present payment transactions.

[0013] In accordance with a second aspect of the present invention, there is provided a computer-implemented method for authenticating a card-not-present payment transaction initiated by a user at a merchant portal using a user device. The method comprises: (i) receiving, from the user device, a transaction request comprising at least a payment card identifier and a user device identifier associated with the user device; (ii) determining whether the payment card identifier and the user device identifier are registered for making payment at the merchant portal; (iii) transmitting, to the user device, an authentication request to authenticate the card-not-present payment transaction if the payment card identifier and the user device identifier are registered for making payment at the merchant portal, the authentication request comprising a request for an authentication information input; (iv) receiving, from the user device, an authentication response comprising the authentication information input; (v) authenticate the authentication information input using stored authentication information registered for authenticating card-not-present payment transactions between the user and the merchant using the user device and the payment card identifier; and (vi) transmitting, to an issuer server, an authorisation request

comprising an authentication indication to indicate that the authentication input has been authenticated.

[0014] The method may comprise: (i) transmitting, to the issuer server, an authorisation request if it is determined that the payment card identifier and the user device are not registered for making payment at the merchant portal, the authorisation request comprises a request to generate an authentication code for authenticating the user; (ii) receiving, from the user device, an authentication code input; (iii) transmitting, to the issuer server, the authentication code input; (iv) receiving, from the issuer server, an authorisation response indicating that the card-not-present payment transaction is authorised if it is determined that the authentication code input matches the authentication code; (v) transmitting, to the user device, an enrolment request if the card-not-present payment transaction is authorised, the enrolment request comprising a request for registering the authentication information for authenticating card-not-present payment transactions between the user and the merchant using the user device and the payment card identifier; (vi) receiving, from the user device, an enrolment response comprising the authentication information; and (vii) storing registration information for the user for making payment at the merchant portal, the registration information comprising the authentication information, the payment card identifier and the user device identifier.

[0015] Where the authentication information is registered using a network server like the identity check Platform, the method may comprise: (i) retrieving, from a merchant database, a merchant identifier associated with the merchant portal; and (ii) transmitting, to the network server, the authentication information, the payment card identifier, the user device identifier and the merchant identifier for registering the authentication information for authenticating card-not-present payment transactions between the user and the merchant using the user device and the payment card identifier; wherein the registration information is stored at the network server.

[0016] The method may comprise: (i) transmitting, to the network server, a registration determination request comprising the payment card identifier, the user device identifier and the merchant identifier; and (ii) receiving, from the network server, a registration determination response comprising a registration indication indicating if the payment card identifier and the user device identifier are registered for making payment at the merchant portal.

[0017] The method may comprise: (i) transmitting, to the network server, a user verification request comprising the authentication information input; and (ii) receiving, from the network server, a user verification response comprising an authentication indication if the

authentication information input matches the authentication information stored at the network server.

[0018] Where a public key and a private key pair may be generated by the user device and the public key may be received at the network server, the authentication information input may be signed using the private key by the user device and may be authenticated by the network server using the public-private key pair.

[0019] The method may comprise: (i) analysing past card-not-present payment transactions performed using the user device; (ii) generating a user transaction pattern based on the past card-not-present payment transactions; and (iii) determining that the card-not-present payment transaction is an unusual payment transaction if the card-not-present payment transaction does not conform to the user transaction pattern or behavior of the user associated with the past card-not-present payment transactions.

[0020] The authentication indication may comprise a cryptogram.

[0021] The determining step on whether the card-not-present payment transaction is an unusual payment transaction may comprise using a transaction time and a payment amount associated with the card-not-present payment transaction.

[0022] The authentication information comprises a PIN/Pattern/Password or a biometric associated with the user and complying with standards of the network.

[0023] In accordance with a third aspect of the present invention, there is provided a computer-implemented method for authenticating a card-not-present payment transaction initiated by a user at a merchant portal using a user device. The method comprises: (i) receiving, from the user device, a transaction request comprising at least a payment card identifier and a user device identifier associated with the user device; (ii) determining whether the payment card identifier and the user device identifier are registered for making payment at the merchant portal; (iii) transmitting, to an issuer server, an authorisation request if it is determined that the payment card identifier and the user device are not registered for making payment at the merchant portal, the authorisation request comprises a request to generate an authentication code for authenticating the user; (iv) receiving, from the user device, an authentication code input; (v) transmitting, to the issuer server, the authentication code input; (vi) receiving, from the issuer server, an authorisation response indicating that the card-not-present payment transaction is authorised if it is determined that the authentication code input matches the authentication code; (vii) transmitting, to the user device, an enrolment request if the card-not-present payment transaction is authorised, the enrolment request comprising a request for registering the authentication information for authenticating card-not-present payment transactions between the user and

the merchant using the user device and the payment card identifier; (viii) receiving, from the user device, an enrolment response comprising the authentication information; and (ix) storing registration information for the user for making payment at the merchant portal, the registration information comprising the authentication information, the payment card identifier and the user device identifier.

[0024] In accordance with a fourth 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.

[0025] Embodiments of the invention may be implemented as a network of communicating devices (i.e. a “computerized network”). Further embodiments comprise a software application downloadable into a computer device to facilitate the method. The software application may be a computer program product, which may be stored on a non-transitory computer-readable medium on a tangible data-storage device (such as a storage device of a server, or one within a user device). The software application may comprise a software development kit (SDK) suitable for implementing the method as described, for example, at a merchant portal.

[0026] Embodiments of the present invention aim to provide a new and useful computer system and computer-implemented method for authenticating a card-not-present payment transaction so as to enhance a user experience by reducing friction in authenticating the card-not-present payment transaction.

[0027] Other desirable features and characteristics will become apparent from the subsequent detailed description and the appended claims, taken in conjunction with the accompanying drawings of the invention.

Brief description of the drawings

[0028] 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 computer system for authenticating a card-not-present payment transaction initiated by a user at a merchant portal using a user device in accordance with an embodiment of the present invention;

Fig. 2 shows a block diagram comprising functional modules of a merchant server of the computer system of Fig. 1 in accordance with an embodiment of the present invention;

Fig. 3 shows steps of a method for authenticating a card-not-present payment transaction which may be performed by the merchant server of Fig. 2 in accordance with an embodiment of the present invention;

Fig. 4 shows steps of a method for registering a user for authenticating a card-not-present payment transaction which may be performed by the merchant server of Fig. 2 in accordance with an embodiment of the present invention;

Fig. 5, comprising Figs. 5A, 5B and 5C, shows method steps performed by the merchant server of Fig. 2 in accordance with an embodiment of the present invention in which authentication of a card-not-present payment transaction is performed using a network server, where Fig. 5A shows steps of a method in relation to registering a user for authenticating a card-not-present payment transaction, Fig. 5B shows steps of a method in relation to determining if a user is registered for authenticating a card-not-present payment transaction, and Fig. 5C shows steps of a method in relation to verifying a user for authenticating the card-not-present payment transaction;

Fig. 6 shows steps of a method for detecting if a card-not-present payment transaction is an unusual payment transaction using the merchant server of Fig. 2 in accordance with an embodiment of the present invention;

Fig. 7 shows message flows in a method for authenticating a card-not-present payment transaction including registering a user for authenticating subsequent card-not-present payment transactions using the merchant server of Fig. 2 in accordance with an embodiment of the present invention;

Fig. 8 shows message flows in a method for authenticating a card-not-present payment transaction using the merchant server of Fig. 2 in accordance with an embodiment of the present invention;

Fig. 9 shows message flows in a method for authenticating a card-not-present payment transaction including registering a user for authenticating subsequent card-not-present payment transactions using the network server comprised in the computer system of Fig. 1 in accordance with an embodiment of the present invention;

Fig. 10 shows message flows in a method for authenticating a card-not-present payment transaction using the network server comprised in the computer system of Fig. 1 in accordance with an embodiment of the present invention;

Fig. 11, comprising Figs. 11A, 11B, 11C, 11D and 11E, shows illustrations for authenticating a card-not-present payment transaction including registering a user for

authenticating subsequent card-not-present payment transactions using the computer system of Fig. 1 in accordance with an embodiment of the present invention;

Fig. 12, comprising Figs. 12A, 12B, 12C and 12D, shows illustrations for processing subsequent card-not-present payment transactions once the user has been registered for authenticating a card-not-present payment transaction in accordance with an embodiment of the present invention;

Fig. 13, comprising Figs. 13A, 13B, 13C and 13D, shows illustrations for authenticating a card-not-present payment transaction including registering a user for authenticating subsequent card-not-present payment transactions using the computer system of Fig. 1 in accordance with an embodiment of the present invention; and

Fig. 14 shows schematically a hardware structure of the merchant server of Fig. 2 which may be used in the computer system of Fig. 1 to implement a method in accordance with an embodiment of the present invention.

Detailed description of the embodiment

[0029] As used herein, the term “card-not-present payment transaction” refers to any payment transaction which may be performed electronically where the payment card is not physically present for the merchant’s examination at the time of the payment transaction. A typical card-not-present payment transaction may involve a user making a purchase of a product on a merchant website associated with a merchant server. Other forms of a card-not-present payment transaction, for example funds transfer or bill payment, are envisaged as long as there involves a movement of funds between two parties.

[0030] The term “payment card” refers to any cashless payment device 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 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. In addition, the “payment card” may exist as application-based stored value accounts associated with an electronic wallet service provider tied in with an issuer institution.

[0031] The term “institution” is used 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.

[0032] As used in this disclosure, 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.

[0033] 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 . . .).

[0034] Fig. 1 shows a computer system 100 for authenticating a card-not-present payment transaction between a user and a merchant in accordance with an embodiment of the present invention. The computer system 100 comprises a user device 102 and a merchant server 104. The user device 102 includes any electronic device associated with the user which enables the user to purchase product(s) online at a merchant portal associated with the merchant. The user device 102 may be a mobile phone, a laptop/notebook, a desktop, a tablet, a personal digital assistant (PDA), a NFC-enabled device, and/or a computer. The merchant server 104 provides the merchant portal on which card-not-present payment transactions can be initiated. The merchant portal may be developed using a software development kit (SDK) to access application interfaces (API) which provide other services (e.g. authentication services provided by other parties). This is described below in relation to Figs. 11 to 13. In addition, for some embodiments, the merchant server 104 is configured to authenticate the user for processing the card-not-present payment transaction. The computer system 100 further comprises an acquirer server 106, a payment network server 108 and an issuer server 110. The acquirer server 106 is operated by an acquirer institution at which the merchant maintains a merchant account to receive funds e.g. for card-not-present payment transactions processed using the merchant portal. The payment network server 108 is associated with a payment network, such as the

Banknet payment network operated by Mastercard®, for facilitating card-not-present payment transactions between the user and the merchant. The issuer server 110 is associated with an issuer institution which maintains at least a user account which can be used e.g. for processing a card-not-present payment transaction using the merchant portal. In some embodiments, the computer system 100 further comprises a network server 112 which may provide for authenticating the user for processing the card-not-present payment transaction. As shown in Fig. 1, the network server 112 may be in communication with the merchant server 104 and/or the user device 102.

[0035] Databases for storing relevant data used in embodiments of the present invention are also included in the computer system 100. As shown in Fig. 1, the computer system 100 further comprises a merchant database 114 which is connected to the merchant server 104. The merchant database 114 may be configured to store data in relation to at least one card-not-present payment transaction performed at the merchant portal. The data may include a payment amount and/or a payment card identifier associated with the user used for processing the card-not-present payment transaction. The payment card identifier may be the payment card number associated with the payment card, or may be a token associated with the payment card. In some embodiments, the merchant database 114 is configured to store authentication information registered by the user for use in authentication card-not-present payment transactions. The merchant database 114 may also be configured to store a merchant identifier associated with the merchant, where the merchant identifier can be retrieved for authenticating the user at least in embodiments where registration and authentication of the user for authenticating card-not-present payment transactions are performed using the network server 112. Moreover, an issuer database 116 is connected to the issuer server 110 for storing data related to a user account associated with the user which can be used for payment in the card-not-present payment transaction. The data associated with the user account may comprise a user account number (e.g. a payment card number), details associated with the user (e.g. a user name, a user's date of birth etc.), contact details associated with the user (e.g. a user mobile number, a user email address, a user home/work address, a user home number etc.) and details associated with a status of the user account (e.g. an available balance, transaction history etc.). Further, where a network server 112 is included in the computer system 100 for use in authenticating card-not-present payment transactions, a network database 118 connected to the network server 112 may be provided for storing authentication information registered by the user for use in authenticating card-not-present payment transactions. Although the merchant database 114, the issuer database 116 and the network database 118 are shown as external databases in Fig. 1, these databases 114,

116, 118 may also form part of the merchant server 104, the issuer server 110 and the network server 112 respectively.

[0036] While only one user device 102 and only one merchant server 104 is shown in Fig. 1, it is appreciated that a plurality of user devices 102 and a plurality of merchant servers 104 associated with respective merchant portals may also form part of the computer 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 computer system 100. A plurality of network servers 112 may also form part of the computer system 100. Likewise, a plurality of merchant databases 114, issuer databases 116 and/or network databases 118 associated with respective merchant servers 104, issuer servers 110 and network servers 112 respectively may also form part of the computer system 100.

[0037] Communication between the user device 102, servers 104, 107, 110, 112 and databases 114, 116, 118 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.

[0038] Fig. 2 shows a block diagram showing functional modules of the merchant server 104 in accordance with an embodiment of the present invention. As shown in Figure 2, the merchant server 104 comprises a communication module 202, a transaction module 204, an authentication module 206, an enrolment module 208, and a monitoring module 210. The communication module 202 allows the merchant server 104 to communicate with the user device 102 over a network such as the internet. The transaction module 204 is operable to process card-not-present payment transactions initiated at the merchant portal. The authentication module 206 is operable to authenticate the user of the user device 102 using stored authentication information at the merchant database 114. In embodiments where authentication of the user is performed by the network server 112, the authentication module 206 is operable to facilitate the authentication of the user by communicating with the network server 112 e.g. via the communication module 202. The enrolment module 208 is operable to register the user for authenticating card-not-present payment transactions. In embodiments where authentication of the user is performed by the network server 112, the authentication module 206 is operable to facilitate the registration of the user by communicating with the network server 112 e.g. via the communication module 202. The monitoring module 210 is operable to monitor card-not-present payment transactions processed using the merchant server 104 for detecting if an unusual or a potentially fraudulent transaction has been initiated.

[0039] Fig. 3 shows steps of a method 300 for authenticating a card-not-present payment transaction which may be performed by the merchant server 104 of Fig. 2 in accordance with an embodiment of the present invention.

[0040] In a step 302, the transaction module 204 of the merchant server 104 is configured to receive a transaction request from the user device 102. The transaction request comprises at least a payment card identifier (e.g. a payment card number) and a user device identifier (e.g. an international mobile equipment identity (IMEI) number or a device serial number) associated with the user device 102. In some embodiments, the user device 102 is prompted by the merchant portal, at the time the card-not-present payment transaction is initiated, to retrieve the user device identifier e.g. from a user device database (not shown in Fig. 1). The retrieval of the user device identifier and the inclusion of the user device identifier may be performed automatically without the user input and may be invisible to the user. The transaction request may also comprise a payment amount associated with the card-not-present payment transaction and a time and date of initiating the card-not-present payment transaction.

[0041] In a step 304, the authentication module 206 of the merchant server 104 is configured to determine whether the payment card identifier and the user device identifier are registered for making payment at the merchant portal. The step 304 can either be carried out using the merchant database 114 if the registration of the user is performed by the merchant server 104, or it can be carried out using the network server 112 by communicating with the network server 112 via the communication module 202 of the merchant server 104.

[0042] If it is determined in the step 304 that the payment card identifier and the user device identifier are registered for making payment at the merchant portal, in a step 306, the authentication module 206 of the merchant server 104 is configured to transmit an authentication request for authenticating the card-not-present payment transaction to the user device 102. The authentication request comprises a request for an authentication information input. If it is determined in the step 304 that the payment card identifier and the user device identifier are not registered for making payment at the merchant portal, the authentication module will proceed with other form of authenticating, for example a second-factor authentication performed by the issuer server 110, as described later in relation to Fig. 4.

[0043] In a step 308, the authentication module 206 of the merchant server 104 is configured to receive an authentication response comprising the authentication information input from the user. The authentication information input may be entered by the user at the merchant portal associated with the merchant server 104. The authentication information input may

comprise a passcode or a PIN, or a biometric data associated with the user. The passcode or PIN may comprise any number of alphanumeric characters. The passcode or PIN may also comprise a dynamic portion and a static portion. The dynamic portion may be generated by the merchant portal uniquely for the card-not-present payment transaction while the static portion may be provided by the user. In some embodiments, where a public key-private key pair is employed in ensuring an authenticity of the authentication information registered, the authentication information input is signed by the private key of the user device 202 which can subsequently be verified/authenticated by either the merchant server 104 or the network server 112 using the public key.

[0044] Upon receiving the authentication information input from the user device 102 in the step 308, the authentication module 206 of the merchant server 104 is configured to authenticate the authentication information input using stored authentication information. The stored authentication information comprises authentication information registered by the user with the merchant server 104 or the network server 112. The step 308 can be carried out either using the merchant database 114 if the registration of the user is performed by the merchant server 104, or it can be carried out using the network server 112 by communicating with the network server 112 via the communication module 202 of the merchant server 104.

[0045] If authentication of the authentication information input in the step 310 is successful, the authentication module 206 of the merchant server 104 is configured to transmit an authorisation request to the issuer server 110 in a step 312. The authorisation request comprises an authentication indication to indicate that the card-not-present payment transaction has been authenticated. The authentication indication may comprise a cryptogram, and the authentication indication may be included in a field comprised in the authorisation request to provide a notification to the issuer server 110 that further authentication of the user for the card-not-present payment transaction (e.g. by performing a second-factor authentication) is not necessary. The cryptogram may comprise information about the authentication, for example, whether the authentication was performed using a knowledge authenticator like a PIN/ a pattern/ a password or a physical authenticator like biometrics involving a fingerprint, iris recognition, face recognition, vein recognition, palm recognition etc. and also passive/behavioral biometric data. In some embodiments, if the payment card identifier comprises a token associated with the payment card for use in processing the e-commerce transaction, the payment network server 108 is configured to identify the payment card number associated with the payment card using the token. The payment card number is then transmitted to the issuer server 110 as the indication of the payment card for use in authenticating the user of the e-commerce transaction.

[0046] If authentication of the authentication information input in the step 310 is unsuccessful, the authentication module 206 of the merchant server 104 is configured to refuse to proceed with the card-not-present payment transaction in a step 314. In this case, the transaction module 204 of the merchant server 104 may be configured to prompt the user device 102 to re-submit the authentication information input or to provide other form of payment for the card-not-present payment transaction.

[0047] Fig. 4 shows steps of a method 400 for registering a user for authenticating a card-not-present payment transaction using the merchant server of Fig. 2 in accordance with an embodiment of the present invention.

[0048] If a transaction request is received from the user device 102 at the transaction module 204 of the merchant server 104 in the step 302, and that it is determined by the authentication module 206 of the merchant server 104 in the step 304 that the payment card identifier and the user device identifier are not registered for making payment at the merchant portal, the authentication module 206 of the merchant server 104 is configured to transmit an authorisation request to the issuer server 110 in a step 402. The authorisation request comprises a request to generate an authentication code for transmission to the user for authenticating the card-not-present payment transaction (e.g. a second-factor authentication performed by the issuer server 110). The authentication code may be transmitted by the issuer server 110 to the user device 102 associated with the user using user contact details (e.g. mobile number or electronic mail (e-mail) addresses) stored in the issuer database 116. The authentication code may be a one-time password. The authentication code may be valid for a predetermined authentication code time period, within which the authentication code is to be entered at the merchant portal for authenticating the user for the card-not-present payment transaction. The predetermined authentication code time period may be a time period of 10 seconds, 20 seconds, 30 seconds, 40 seconds, 50 seconds, 1 minute, 2 minutes, 3 minutes, 5 minutes, 10 minutes or any appropriate period of time that is considered sufficient for the user to enter the authentication code yet maintaining security for the card-not-present payment transaction.

[0049] In a step 404, the authentication module 206 of the merchant server 104 is configured to receive an authentication code input from the user device 102. The authentication code input may be entered by the user at the merchant portal associated with the merchant server 104.

[0050] In a step 406, the authentication module 206 of the merchant server 104 is configured to transmit to the issuer server 110 the authentication code input received in the step 404. The authentication module 206 of the merchant server 104 may transmit, via the communication module 202, the authentication code input to the issuer server 110 via the

acquirer server 106 and the payment network server 108. Once the authentication code input is received at the issuer server 110, the issuer server 110 is configured to determine if the authentication code input matches the authentication code generated and transmitted to the user. If it is determined that the authentication code input matches the authentication code generated in response to the step 402, the issuer server 110 is configured to generate an authorisation response to be transmitted to the merchant server 104 indicating that the card-not-present payment transaction is authorised. In some embodiments, the issuer server 110 also perform other conventional checks such as determining if an available balance associated with the payment card identifier is more than or equal to the payment amount associated with the card-not-present payment transaction before authorising the card-not-present payment transaction. If it is determined that the authentication code input does not match the authentication code generated in the step 402, the issuer server 110 is configured to generate an authorisation response to be transmitted to the merchant server 104 indicating that the card-not-present payment transaction is refused.

[0051] In a step 408, the authentication module 206 of the merchant server 104 is configured to receive the authorisation response from the issuer server 110. The authorisation response may be received from the issuer server 110 via the payment network server 108 and the acquirer server 106.

[0052] If the card-not-present payment transaction is authorised, in a step 410, the enrolment module 208 of the merchant server 104 is configured to transmit an enrolment request to the user device 102 to prompt the user to register an authentication information for authenticating card-not-present payment transactions. If the authorisation response indicates that the card-not-present payment transaction is refused in the step 408, the transaction module 204 of the merchant server 104 may inform the user of a failure to process the card-not-present payment transaction and may request another form of payment if the user wishes to continue processing the card-not-present payment transaction.

[0053] In a step 412, the enrolment module 208 of the merchant server 104 is configured to receive an enrolment response from the user device 102. If the user decides to register to authenticate subsequent card-not-present payment transactions using authentication information, the enrolment response transmitted by the user device 102 may comprise the requested authentication information. In some embodiments, where the user decides not to register authentication information for authenticating subsequent card-not-present payment transactions, the enrolment response may comprise an indication that the user decides not to register any authentication information at this time.

[0054] If authentication information is received by the enrolment module 208 of the merchant server 104 in the step 412, the enrolment module 208 of the merchant server 104 is configured to store registration information from the user for making payment at the merchant portal in a step 414. The registration information may comprise the authentication information, the payment card identifier and the user device identifier. The authentication information and/or the registration information may be stored in the merchant database 114.

[0055] Fig. 5, comprising Figs. 5A, 5B and 5C, shows method steps performed at the merchant server 104 in accordance with an embodiment of the present invention. The following method steps are performed in place of or in addition to the method steps described in Figs. 3 and 4 where the registration and the authentication of the user for authenticating card-not-present payment transactions are carried out by the network server 112.

[0056] Fig. 5A shows steps of a method performed by the enrolment module 208 of the merchant server 104 for registering a user for authenticating card-not-present payment transactions with the network server 112.

[0057] Once the authentication information is received from the user device 102 in the step 412, the enrolment module 208 of the merchant server 104 is configured to retrieve from the merchant database 114 a merchant identifier associated with the merchant portal. The merchant identifier may comprise a name of the merchant and/or a merchant category code (MCC) associated with the merchant.

[0058] In a step 504, the enrolment module 208 of the merchant server 104 is configured to transmit the authentication information, the payment card identifier, the user device identifier and the merchant identifier to the network server 112 for registering the user for authenticating card-not-present payment transactions with the network server 112. The authentication information, the payment card identifier, the user device identifier and the merchant identifier may be stored in the network database 118 and this combination may be used to authenticate or verify the user in subsequent card-not-present payment transactions.

[0059] Fig. 5B shows steps of a method performed by the authentication module 206 of the merchant server 104 for determining if a user is registered for authenticating a card-not-present payment transaction. This further defines the step 304 for determining whether the payment card identifier and the user device identifier are registered for making payment at the merchant portal using the network server 112.

[0060] In a step 506, the authentication module 206 of the merchant server 104 is configured to transmit a registration determination request to the network server 112. The registration

determination request comprises the payment card identifier and the user device identifier received in the step 302 as part of the transaction request. The authentication module 206 may be further configured to retrieve the merchant identifier from the merchant database 114 so as to include the merchant identifier in the registration determination request. Upon receipt of the aforementioned information, the network server 112 is configured to determine if this combination of the payment card identifier, the user device identifier and the merchant identifier has been registered with the network server 112 for authenticating card-not-present payment transactions initiated at the merchant portal.

[0061] In a step 508, the authentication module 206 of the merchant server 104 is configured to receive a registration determination response from the network server 112. The registration determination response comprises a registration indication indicating if the payment card identifier and the user device identifier are stored in relation to the merchant identifier for making payment at the merchant portal. Depending on an outcome of the registration determination, once the registration determination response is received, the authentication module 206 of the merchant server 104 can then proceed with either the step 306 or the step 402 as previously described.

[0062] Fig. 5C shows steps of a method performed by the authentication module 206 of the merchant server 104 for verifying a user for authenticating a card-not-present payment transaction. This further defines the step 310 for authenticating the authentication information input using the network server 112.

[0063] In a step 510, the authentication module 206 of the merchant server 104 is configured to transmit a user verification request to the network server 112. The user verification request comprises the authentication information input received from the user device 102 in the step 308. Upon receipt of the authentication information input, the network server 112 is configured to authenticate the authentication information input using stored authentication information (e.g. the authentication information registered using the steps 506 and 508) stored at the network database 118. In some embodiments, where a public key-private key encryption is employed in ensuring an authenticity of the authentication information, the authentication information input is signed by the private key of the user device 202. This may be verified/authenticated by the network server 112 using the public key. This may ensure that the authentication information input is indeed received from the user device and not any other party. Moreover, the authentication information input may also be encrypted (e.g. using a same or another private key/public key pair) so that a third party may not access the authentication information input.

[0064] If authentication of the authentication information input by the network server 112 is successful (e.g. the authentication information input matches the stored authentication

information), in a step 512, the authentication module 206 of the merchant server 104 is configured to receive a user verification response comprising an authentication indication from the network server 112. The authentication indication serves to indicate that the card-not-present payment transaction has been authenticated. Similar to the authentication indication transmitted by the merchant server 104 in the step 312, the authentication indication may comprise a cryptogram, and the authentication indication may be included a field of the authorisation request in the step 312 for transmission to the issuer server 110.

[0065] Fig. 6 shows steps of a method 600 performed by the monitoring module 210 of the merchant server 104 for detecting if a card-not-present payment transaction is an unusual payment transaction using the merchant server 104 of Fig. 2 in accordance with an embodiment of the present invention.

[0066] In a step 602, the monitoring module 210 of the merchant server 104 is configured to analyse past card-not-present payment transactions performed by the user device 102 using the merchant database 114. The analysis of the past card-not-present payment transactions may include categorising the past card-not-present payment transactions completed using the payment card identifier at the merchant portal based on transaction time and/or payment amounts associated with the past card-not-present payment transactions.

[0067] In a step 604, the monitoring module 210 of the merchant server 104 is configured to generate a user transaction pattern based on the past card-not-present payment transactions. The user transaction pattern generated may be based on the analysis performed in the step 602, and may be associated with (i) a frequency of the past card-not-present payment transactions, (ii) payment amounts of the past card-not-present payment transactions, and/or (iii) transaction time of the past card-not-present payment transactions. The user transaction pattern may be generated using conventional statistical analysis tools.

[0068] In a step 606, the monitoring module 210 of the merchant server 104 is configured to determine if the card-not-present payment transaction is an unusual payment transaction (or a potentially fraudulent transaction). The card-not-present payment transaction is an unusual payment transaction if it does not conform to the user transaction pattern associated with the past card-not-present payment transactions as generated in the step 604.

[0069] Fig. 7 shows message flows in a method for authenticating a card-not-present payment transaction including registering a user for authenticating subsequent card-not-present payment transactions using the merchant server 104 of Fig. 2 in accordance with

an embodiment of the present invention. The user may initiate the card-not-present payment transaction online via a merchant portal associated with the merchant server 104. Registration of the user for subsequent card-not-present payment transactions may occur as part of a conventional card-not-present payment transaction with two-factor authentication as described below.

[0070] Fig. 7 shows message flows between the user device 102, the merchant server 104, the payment network 107 and the issuer server 110. The payment network 107 comprises the acquirer server 106 and the payment network server 108. The acquirer server 106 and the payment network server 108 have been collectively grouped under the “payment network 107” in this figure to improve clarity. It should however be understood in this example implementation that any messages transmitted by the merchant server 104 via the payment network 107 to the issuer server 110 may generally involve the messages being received by the acquirer server 106 which are then forwarded to the payment network server 108 in order for these messages to be subsequently transmitted to the issuer server 110. In a similar manner, it should be understood in this example implementation that any messages transmitted by the issuer server 110 via the payment network 107 to the merchant server 104 may involve the messages being received by the payment network server 108 which are then forwarded to the acquirer server 106 in order for these messages to be subsequently transmitted to the merchant server 104.

[0071] In a step 702, the user initiates a card-not-present payment transaction using the user device 102 at the merchant portal associated with the merchant server 104 and transmits a transaction request to the merchant server 104. The transaction request comprises at least a payment card identifier (e.g. a payment card number) and a user device identifier. The user device identifier may be provided manually by the user or may be provided automatically by the user device 102 to the merchant portal when the card-not-present payment transaction is initiated. To do so, the user device 102 may be configured to retrieve the user device identifier and to transmit to the user device identifier as part of the transaction request when the card-not-present payment transaction is initiated. After the card-not-present payment transaction is initiated by the user in the step 702, the authentication module 206 of the merchant server 104 determines whether the payment card identifier and the user device identifier are registered for authenticating card-not-present payment transactions. If it is determined that the payment card identifier and the user device identifier are not registered, the merchant server 104 proceeds with requesting authorisation of the card-not-present payment transaction from the issuer server 110 in a conventional manner which involves two-factor authentication. This is described below in relation to steps 706 to 726.

[0072] In a step 706, the authentication module 206 of the merchant server 104 transmits an authorisation request to the payment network 107. The authorisation request comprises a request to generate an authentication code for transmission to the user for authenticating the card-not-present payment transaction (e.g. a second-factor authentication performed by the issuer server 110). The authorisation request is then forwarded by the payment network 107 to the issuer server 110 in a step 708. In a step 710, the issuer server 110 generates the authentication code upon receiving the authorisation request. The authentication code, for example a one-time password, is to be used in authenticating the user for the card-not-present payment transaction. The authentication code may be valid for a predetermined authentication code time period, within which the authentication code is to be entered at the merchant portal for authenticating the user for the card-not-present payment transaction. The predetermined authentication code time period may be a time period of 10 seconds, 20 seconds, 30 seconds, 40 seconds, 50 seconds, 1 minute, 2 minutes, 3 minutes, 5 minutes, 10 minutes or any appropriate period of time that is considered sufficient for the user to enter the authentication code yet maintaining security for the card-not-present payment transaction.

[0073] In a step 712, the issuer server 110 transmits the authentication code to the user device 102 associated with the user. This may be done using user contact details (e.g. mobile number or electronic mail (e-mail) addresses) stored in the issuer database 116. In order to authenticate the user, the user is prompted by the merchant portal to provide an authentication code input, via the user device 102, in a step 714. The authentication module 206 of the merchant server 104 receives the authentication code input from the user device 102 and forwards the authentication code input to the payment network 107 in a step 716. The authentication code input received by the payment network 107 is then forwarded to the issuer server 110 in a step 718 to facilitate authentication of the user. Once the authentication code input is received at the issuer server 110, the issuer server 110 authenticates the authentication code input by determining if the authentication code input matches the authentication code generated in the step 710. If it is determined that the authentication code input matches the authentication code generated in the step 710, the issuer server 110 generates an authorisation response indicating that the card-not-present payment transaction is authorised. In some embodiments, the issuer server 110 also performs other conventional checks, such as determining if an available balance associated with the payment card identifier is more than or equal to the payment amount associated with the card-not-present payment transaction, before authorising the card-not-present payment transaction. If it is determined that the authentication code input does not match the authentication code generated in the step 710, the issuer server 110 generates

an authorisation response indicating that the card-not-present payment transaction is refused.

[0074] In a step 722, the issuer server 110 transmits an authentication response to the payment network 107. The payment network 107 then forwards the authorisation response to the authentication module 206 of the merchant server 104 in a step 724.

[0075] If the authorisation response indicates that the card-not-present payment transaction is authorised, the enrolment module 208 of the merchant server 104 transmits an enrolment request to the user device 102 to prompt the user to register authentication information for authenticating subsequent card-not-present payment transactions in a step 726. The user then provides an enrolment response via the user device 102 at the merchant portal in a step 728. The enrolment response may comprise either authentication information for registering the user for authenticating subsequent card-not-present payment transactions using the authentication information, or an indication that the user does not wish to be registered at this time.

[0076] If the enrolment response comprises the authentication information, the enrolment module 208 of the merchant server 104 stores registration information from the user for making payment at the merchant portal in a step 730 where the registration information comprises the authentication information, the payment card identifier and the user device identifier. The authentication information can be stored in the merchant database 114.

[0077] In a step 732, the transaction module 202 of the merchant server 104 transmits a transaction response to the user device 102 indicating whether the card-not-present payment transaction has been approved or refused. If the transaction response indicates that the card-not-present payment transaction has been refused, the transaction module 204 of the merchant server 104 may request another form of payment if the user wishes to continue processing the card-not-present payment transaction. If the user has registered authentication information via the enrolment response in the step 728, the enrolment module 208 of the merchant server 104 also transmits an enrolment result to the user device 102 in the step 732 to indicate that the user has been registered for authenticating subsequent card-not-present payment transactions.

[0078] Fig. 8 shows message flows in a method for authenticating a card-not-present payment transaction using the merchant server 104 of Fig. 2 in accordance with an embodiment of the present invention. In particular, Fig. 8 shows the message flows in processing a card-not-present payment transaction once the user has been registered in the method as shown in Fig. 4. Similar to Fig. 7, the term "payment network 107" is used in this figure to improve clarity.

[0079] Steps 802 and 804 are similar to the steps 702 and 704 respectively and so details for these two steps are not repeated here. If it is determined that the payment card identifier and the user device identifier are registered for making payment at the merchant portal in the step 804, the authentication module 206 of the merchant server 104 transmits an authentication request for authenticating the card-not-present payment transaction to the user device 102 in a step 806. The authentication request comprises a request for an authentication information input. The authentication information input may be in the form of a passcode or a PIN, or in a form of a biometric associated with the user.

[0080] In a step 808, the user provides an authentication information input at the merchant portal as prompted by the merchant portal. The authentication information input is received by the authentication module 206 of the merchant server 104 as part of an authentication response. The authentication module 206 of the merchant server 104 then authenticates the authentication information input using stored authentication information in a step 810. If authentication of the authentication information input in the step 810 is successful, the authentication module 206 of the merchant server 104 requests authorisation of the card-not-present payment transaction. Otherwise, the authentication module 206 of the merchant server 104 may refuse the card-not-present payment transaction. In this case, the transaction module 204 of the merchant server 104 may prompt the user device 102 to re-submit the authentication information input or to provide other form of payment for the card-not-present payment transaction.

[0081] In the event that the authentication is successful in the step 810, the authentication module 206 of the merchant server 104 transmits, via the communication module 202, an authorisation request to the payment network 107 in a step 812 which is then forwarded to the issuer server 110 in a step 814. The authorisation request comprises an authentication indication to indicate that the card-not-present payment transaction has been authenticated. The authentication indication may comprise a cryptogram, and may be included in a field comprised in the authorisation request. The authentication indication may serve to provide a notification to the issuer server 110 that further authentication of the user for the card-not-present payment transaction (e.g. by performing a second-factor authentication) is not necessary, and that the card-not-present payment transaction has been authenticated on behalf of the issuer server 110.

[0082] Upon receiving the authorisation request in the step 814, the issuer server 110 may perform other conventional checks (e.g. checking a balance of the user account associated with the payment card identifier etc.) before transmitting an authorisation response back to the merchant server 104. Once the other conventional checks, if any, have been performed, an authorisation response is transmitted by the issuer server 110 to the payment network

107 in a step 816. The authorisation response is then forwarded by the payment network 107 to the merchant server 104 in a step 818. The authorisation response comprises an indication on whether the card-not-present payment transaction is authorised or not. The card-not-present payment transaction may be authorised if the card-not-present payment transaction has been authenticated, and that any other necessary conditions (e.g. a balance of the user account associated with the payment card identifier is more than or equal to the payment amount associated with the card-not-present payment transaction) associated with the conventional checks performed have been met. In a step 820, the transaction module 204 of the merchant server 104 transmits a transaction response to the user device 102 indicating that the card-not-present payment transaction is approved if the card-not-present payment transaction is authorised by the issuer server 110. Otherwise, the transaction response indicates to the user that the card-not-present payment transaction is refused.

[0083] As described in the foregoing, authentication of the user and the card-not-present payment transaction therefore does not involve any ACS or any 3DS authentication page to be loaded from the issuer server 110 during authentication. Instead, the merchant (and therefore the merchant server 104) has complete control over the authentication process.

[0084] Fig. 9 shows message flows in a method for authenticating a card-not-present payment transaction including registering a user for authenticating subsequent card-not-present payment transactions using the network server 112 comprised in the computer system 100 of Fig. 1 in accordance with an embodiment of the present invention. A main difference between Fig. 7 and Fig. 9 is that the registration of authentication information for authenticating the user in card-not-present payment transactions is performed by the network server 112 as shown in relation to Fig. 9, rather than by the merchant server 104 as described in relation to Fig. 7. Similar to Figs. 7 and 8, the term “payment network 107” is used in this figure to improve clarity.

[0085] In a step 902, the transaction module 204 of the merchant server 104 receives a transaction request, similar to the steps 702 and 802 as previously described. However, unlike the step 704 and 804 where the authentication module 206 of the merchant server 104 determines if the payment card identifier and the user device identifier are registered for making payment at the merchant portal, this determination process is being performed at the network server 112 where the user is registered. Therefore, in a step 904, the authentication module 206 of the merchant server 104 retrieves a merchant identifier associated with the merchant server 104 which is subsequently used by the network server 112 in performing the determination process. In a step 906, the authentication module 206 of the merchant server 104 transmits a registration determination request to

the network server 112. The registration determination request comprises the payment card identifier and the user device identifier received in the step 902 as part of the transaction request, as well as the merchant identifier retrieved in the step 904. Upon receipt of the aforementioned information, the network server 112 determines if this combination of the payment card identifier, the user device identifier and the merchant identifier has been registered with the network server 112 for authenticating card-not-present payment transactions in a step 908. Once the determination process is completed, the network server 112 transmits a registration determination response to the merchant server 104 in a step 910. The registration determination response comprises a registration indication indicating if the payment card identifier and the user device identifier are stored in relation to the merchant identifier for making payment at the merchant portal. Once the registration determination response is received by the merchant server 104 in the step 910 and if it is determined that the payment card identifier and the user device identifier are not stored in relation to the merchant identifier, the authentication module 206 of the merchant server 104 requests authorisation for the card-not-present payment transaction in steps 912 to 932. The steps 912 to 930 are similar to their respective steps of 706 to 724 previously described, the description of which is therefore not repeated here for succinctness.

[0086] Following on from the step 930, if the authorisation response received from the payment network 107 indicates that the card-not-present payment transaction is authorised, the enrolment module 208 of the merchant server 104 transmits an enrolment request to the user device 102 in a step 932. The enrolment request comprises a request for the user to register authentication information for authenticating subsequent card-not-present payment transactions. In a step 934, the user provides an enrolment response via the user device 102 at the merchant portal. The enrolment response may comprise either authentication information for authenticating the user in subsequent card-not-present payment transactions, or an indication that the user does not wish to be registered at this time.

[0087] In a step 936, if the user has provided authentication information for registering with the network server 112, the enrolment module 208 of the merchant server 104 forwards the enrolment response to the network server 112 comprising the authentication information together with other registration information such as the payment card identifier, the user device identifier and the merchant identifier to the network server 112 for registering the user for authenticating subsequent card-not-present payment transactions. Upon receipt of the authentication information and the other registration information, the network server 112 stores the authentication information in relation to the payment card identifier, the user device identifier and the merchant identifier using the network database

118 in a step 938. Results of the enrolment is then transmitted by the network server 112 to the merchant server 104 indicating that the user has been registered for authenticating subsequent card-not-present payment transactions in a step 940.

[0088] In a step 942, the transaction module 202 of the merchant server 104 transmits a transaction response to the user device 102 indicating whether the card-not-present payment transaction has been approved or refused. If the transaction response indicates that the card-not-present payment transaction has been refused, the transaction module 204 of the merchant server 104 may request another form of payment if the user wishes to continue processing the card-not-present payment transaction. If the user has provided authentication information via the enrolment response in the step 934, the enrolment module 208 of the merchant server 104 forwards the enrolment results also in the step 942 to indicate that the user has been registered for authenticating subsequent card-not-present payment transactions.

[0089] Fig. 10 shows message flows in a method for authenticating a card-not-present payment transaction using the network server 112 comprised in the computer system 100 of Fig. 1 in accordance with an embodiment of the present invention. A main difference between Fig. 8 and Fig. 10 is that authentication of the authentication information input provided by the user is performed by the network server 112 as shown in relation to Fig. 10, rather than by the merchant server 104 as described in relation to Fig. 8. Similar to Figs. 7, 8 and 9, the term “payment network 107” is used in this figure to improve clarity.

[0090] Steps 1002 to 1010 as shown in Fig. 10 are similar to the steps 902 to 910 as previously described in relation to Fig. 9, and description thereof is therefore not repeated here for succinctness.

[0091] In a step 1012, if it is determined that the payment card identifier and the user device identifier are stored in relation to the merchant identifier for making payment at the merchant portal, the authentication module 206 of the merchant server 104 transmits an authentication request for authenticating the card-not-present payment transaction to the user device 102. The authentication request comprises a request for an authentication information input. The authentication information input may be in the form of a passcode or a PIN, or in a form of a biometric associated with the user.

[0092] In a step 1014, the user provides an authentication information input at the merchant portal as prompted by the merchant portal. The authentication information input is received by the authentication module 206 of the merchant server 104 as part of an authentication response. Upon receipt of the authentication information input, the authentication module 206 of the merchant server 104 transmits a user verification request to the network server

112 in a step 1016. The user verification request comprises the authentication information input received from the user device 102 in the step 1014. Upon receipt of the authentication information input, the network server 112 authenticates the authentication information input using stored authentication information at the network database 118 in a step 1018. In some embodiments, where a public key-private key encryption is employed in ensuring an authenticity of the authentication information input, the authentication information input is signed by the private key of the user device 202 which is then subsequently verified/authenticated by the network server 112 using the public key previously provided to the network server 112.

[0093] In a step 1020, the authentication module 206 of the merchant server 104 receives a user verification response from the network server 112. If authentication of the authentication information input by the network server 112 is successful, the authentication module 206 of the merchant server 104 receives a user verification response comprising an authentication indication from the network server 112. The authentication indication serves to indicate that the card-not-present payment transaction has been authenticated. The authentication indication may comprise a cryptogram and may be included in a field of an authorisation request subsequently sent to the issuer server 110 to indicate that the card-not-present payment transaction has been authenticated. If the authentication is unsuccessful, the authentication module 206 of the merchant server 104 refuses the card-not-present payment transaction. In this case, the transaction module 204 of the merchant server 104 may prompt the user device 102 to re-submit the authentication information input or to provide other form of payment for the card-not-present payment transaction.

[0094] If authentication of the authentication information input in the step 1020 is successful, the authentication module 206 of the merchant server 104 requests authorisation of the card-not-present payment transaction from the issuer server 110 in a step 1022. Steps 1022 to 1030 lay out the steps for requesting authorisation from the issuer server 110 and for transmitting a transaction response to the user via the user device 102. As the steps 1022 to 1030 are similar to the respective steps of 812 to 820, the description of which are not repeated here for succinctness.

[0095] In some embodiments, the merchant portal may be developed using a software development kit (SDK) to access application interfaces (API) which provide other services (e.g. authentication services provided by other parties) for performing the aforementioned methods. The SDK may be provided to the merchants in the form of a non-transitory computer-readable medium having stored thereon program instructions for causing at least one processor of the merchant server 104 to perform the aforementioned methods.

[0096] Fig. 11, comprising Figs. 11A, 11B, 11C, 11D and 11E, shows illustrations of the merchant portal for authenticating a card-not-present payment transaction including registering a user for authenticating subsequent card-not-present payment transactions using the computer system 100 of Fig. 1 in accordance with an embodiment of the present invention. In particular, Fig. 11 shows an embodiment which may be performed using a mobile application on the user device 102.

[0097] Fig. 11A shows a check-out page of the merchant portal on an exemplary user device 102. An item to be purchased has been placed in a shopping cart associated with the merchant portal and the card-not-present payment transaction is ready to be initiated by the user e.g. by using the "Place Order" button as displayed on the screen of the user device 102 as shown in Fig. 11A.

[0098] Once the card-not-present payment transaction is initiated by the user, the merchant portal prompts the user to enter personal details for completing the card-not-present payment transaction as shown in Fig. 11B. As shown in Fig. 11B, the user may be required to provide his/her particulars e.g. a delivery address for the item and billing information for the card-not-present payment transaction. In addition, the user may be required to provide payment information. The payment information may include payment card details such as a name of the cardholder associated with the payment card, a payment card number, an expiry date of the payment card and/or a card verification code (CVC2) of the payment card. The user may move forward with processing the card-not-present payment transaction using the button "Next Step" as shown on the screen of the user device 102 in Fig. 11B.

[0099] Following this, a number of processing steps occur to facilitate processing of the card-not-present payment transaction. For example, if the registration and authentication of the card-not-present payment transaction is to be performed by the network server 112 as described in Figs. 9 and 10, the merchant portal may cause the user device 102 to retrieve a user device identifier to be included as part of the transaction request for processing the card-not-payment payment transaction. Upon receiving the necessary information, the merchant server 104 is configured to determine whether the payment card identifier and the user device identifier are registered for authenticating the card-not-present payment transaction, for example, either internally by using the merchant database 114 as described in the step 704 or by using the network server 112 as described in the steps 904 to 910. If it is determined that the payment card and the user device identifier are not registered for use in authenticating the card-not-present payment transaction, further authentication (e.g. a second-factor authentication performed by the issuer server 110) may be necessary. This is previously described, for example, in relation to the steps 706

to 724 or the steps 912 to 930. In either of these embodiments, the SDK provided may configure the merchant portal to carry out the necessary processes for processing the card-not-present payment transaction. This may for example include retrieving the user device identifier and/or facilitating the determination of whether the payment card identifier and the user device identifier are registered for authenticating the card-not-present payment transaction (e.g. using the merchant server 104 or the network server 112).

[00100] In the present example, the payment card identifier and the user device identifier are not registered for authenticating the card-not-present payment transaction. Therefore, as shown in Fig. 11C, the user is prompted with the authentication code, for example, via Short Messaging Service (SMS) for authentication the card-not-present payment transaction. As shown in Fig. 11C, the merchant portal is configured to prompt the user to provide an authentication code input at the merchant portal for authenticating the purchase.

[00101] Following a receipt of the authentication code input (e.g. as described in the step 714 or the step 920), the merchant portal is configured to obtain authorisation from the issuer server 110 as described in the steps 716 to 724 or the steps 922 to 930. Once the card-not-present payment transaction is authorised, the merchant portal is configured (e.g. by using the SDK) to prompt the user for registering an authentication information (e.g. a four-digit PIN as shown in Fig. 11D) for authenticating subsequent card-not-present payment transactions using the authentication information. This is in relation to the step 726 or 932 as described in Fig. 7 and Fig. 9 respectively. Once the user has provided his/her authentication information, the user can complete the card-not-present payment transaction using the "Complete Checkout" button as shown in Fig. 11D. In some embodiments (not shown in Fig. 11D), the user is provided with an option to complete the card-not-present payment transaction without registering the authentication information.

[00102] Upon receipt of the authentication information from the user, enrolment of the authentication information for the user to authenticate subsequent card-not-present payment transactions is performed (see e.g. the processes as described in the steps 728 to 730 or the steps 934 to 940). The merchant portal is then configured to inform the user that the order has been completed and that the authentication information has been registered successfully as shown in Fig. 11E.

[00103] Fig. 12, comprising Figs. 12A, 12B, 12C and 12D, shows illustrations for processing subsequent card-not-present payment transactions once the user has been registered for authenticating subsequent card-not-present payment transactions in accordance with an embodiment of the present invention.

[00104] Figs. 12A shows that the desired item is included in a shopping cart at the merchant portal for purchase while Fig. 12B shows that personal particulars (e.g. a user name, a delivery address and a billing address etc.) and payment information (e.g. a cardholder name, a payment card number, a payment card expiry date etc.) are requested from the user in order to complete the purchase. The processes performed in relation to Figs. 12A and 12B are similar to those performed in relation to Figs. 11A and 11B respectively and their descriptions are therefore not repeated here.

[00105] Once the personal particulars and the payment information have been received at the merchant portal, either the merchant server 104 (as described in relation to the step 704) or the network server 112 (as described in relation to the steps 904 to 910) may be used to determine whether the payment card identifier and the user device identifier are registered for use in authenticating the card-not-present payment transaction. In the present example, the payment card identifier and the user device identifier are registered for authenticating the card-not-present payment transaction. Therefore, the merchant portal is configured to prompt the user to provide an authentication information input to authenticate the card-not-present payment transaction as shown in Fig. 12C in order to complete the card-not-present payment transaction. In an event where the user forgets the authentication information, the user may initiate to reset the authentication information for example by using a link "Reset it now" as shown in Fig. 12C. In an embodiment, resetting the authentication information requires the user to be authenticated, for example by a second-factor authentication process performed by the issuer server 110, again.

[00106] Following receipt of the authentication information input (e.g. as described in the step 714 or the step 920) at the merchant portal, authentication of the authentication information input can be performed. The authentication process can either be carried out by the merchant server 104 as described in relation to the step 810 or by the network server as described in relation to the steps 1016 to 1020. If the authentication process is to be performed by the network server 112, the merchant portal is configured to transmit a user verification request comprising the authentication information input to the network server 112 and to receive a user verification response comprising a result of the authentication from the network server 112 (e.g. as described in the steps 1016 and 1020 respectively).

[00107] Once the authentication input has been authenticated, the merchant portal is configured to obtain authorisation for the card-not-present payment transaction from the issuer server 110 as described in the steps 812 to 820 or the steps 1022 to 1030. Upon authorisation of the card-not-present payment transaction, the merchant portal is configured to inform the user that the order has been completed as shown in Fig. 12D.

[00108] Fig. 13, comprising Figs. 13A, 13B, 13C and 13D, shows illustrations for authenticating a card-not-present payment transaction including registering a user for authenticating subsequent card-not-present payment transactions using the computer system 100 of Fig. 1 in accordance with an embodiment of the present invention. In particular, Fig. 13 shows an embodiment where the card-not-present payment transaction is performed using a browser of the user device 102 where the merchant portal on the browser does not support web authentication.

[00109] Figs. 13A shows that the desired item is included in a shopping cart at the merchant portal for purchase while Fig. 13B shows that personal particulars (e.g. a user name, a delivery address and a billing address etc.) and payment information (e.g. a cardholder name, a payment card number, a payment card expiry date etc.) are requested from the user in order to complete the purchase. The processes performed in relation to Figs. 13A and 13B are similar to those performed in relation to Figs. 11A and 11B respectively and their descriptions are therefore not repeated here.

[00110] In the present example, as the merchant portal does not support web authentication, as shown in Fig. 13C, the user is redirected to a relevant application (e.g. a Mastercard® application as shown) for registering and/or authenticating the user for the card-not-present payment transaction. Although not shown here in Fig. 13, if the user is determined by the relevant application that he/she is not registered for authenticating the card-not-present payment transaction, the user may be required to authenticate the card-not-present payment transaction in a conventional manner, e.g. using a second-factor authentication administered by the issuer server 110. The user may also be prompted to provide authentication information for registering to authenticate subsequent card-not-present payment transactions, for example in a similar manner as described in relation to Figs. 11C and 11D. Upon receipt of the authentication information from the user, the processes as described in the steps 728 to 730 or the steps 934 to 940 are carried out. The merchant portal is then configured to inform the user that the order has been completed and that the authentication information has been registered successfully as shown in Fig. 13D.

[00111] Although the aforementioned methods described in Figs. 9 and 10 are performed using a network server 112 in communication with the merchant server 104, similar methods for registering and authenticating the user for processing the card-not-present payment transaction can be performed in embodiments where the network server 112 is directly connected to the user device 102.

[00112] For example, in relation to registering the user for authenticating subsequent card-not-present payment transactions, the merchant portal (or the merchant server 104)

may be configured to transmit the registration determination request to the network server 112 via the user device 102, instead of what was previously described which involves the merchant server 104 transmitting the registration determination request directly to the network server 112 in the step 906. Similarly, once the step 908 is performed at the network server 112, the registration determination response transmitted by the network server 112 can be received at the merchant server 104 via the user device 102 in the step 910. The steps 932 to 942 may also be carried out where the network server 112 is in direct communication with the user device 102. For example, the enrolment response in the step 934 may be directly communicated to the network server 112 for storing the authentication information and the other registration information at the network server 112 and the enrolment results may subsequently be directly communicated to the user device 102 by the network server 112.

[00113] In relation to authenticating the user for subsequent card-not-present payment transactions, once it is determined that the user has been registered with the network server 112, the network server 112 may be configured to request an authentication information input from the user device 102 directly if it is determined that the combination of the payment card identifier, the user device identifier and the merchant identifier are previously registered with the network server 112 (c.f. the steps 1010 and 1012 of Fig. 10). Similarly, the authentication information input may be provided from the user device 102 to the network server 112 directly (c.f. the steps 1014 and 1016 of Fig. 10). Once the authentication information input is received from the user device 102 at the network server 112, the network server 112 may be configured to authenticate the authentication information input using the stored authentication information. If the authentication information input is authenticated, the network server 112 may be configured to generate an authentication indication and transmit the authentication indication directly to the user device 102. An indication that the user has been authenticated together with the authentication indication are then forwarded by the user device 102 to the merchant server 104 via the merchant portal. The merchant server 104 is then configured to proceed with obtaining authorisation for the card-not-payment transaction as described in the steps 1022 to 1030. In a variation, once the network server 112 has authenticated the authentication information input and has generated the authentication indication, the network server 112 is configured to transmit the authentication indication to the merchant server 104 similar to the step 1020 as previously described so that the steps 1022 to 1030 can be performed by the merchant server 104 for authorising the card-not-present payment transaction.

[00114] Fig. 14 is a block diagram showing a technical architecture of the merchant server 104 according to an embodiment of the present invention. The technical

architecture of the merchant server 104 is for performing steps of exemplary methods as described above. Typically, the methods are implemented by a number of computers each having a data-processing unit. The block diagram as shown in Figure 14 illustrates a technical architecture of a computer which is suitable for implementing one or more embodiments herein.

[00115] The technical architecture includes a processor 1402 (which may be referred to as a central processor unit or CPU) that is in communication with memory devices including secondary storage 1404 (such as disk drives), read only memory (ROM) 1406, and random access memory (RAM) 1408. The processor 1402 may be implemented as one or more CPU chips. The technical architecture may further comprise input/output (I/O) devices 1410, and system connectivity or network devices 1412.

[00116] The secondary storage 1404 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 1408 is not large enough to hold all working data. Secondary storage 1404 may be used to store programs which are loaded into RAM 1408 when such programs are selected for execution. In this embodiment, the secondary storage 1404 has a communication module 202, a transaction module 204, an authentication module 206, an enrolment module 208 and a monitoring module 210 comprising non-transitory instructions operative by the processor 1402 to perform various operations of the methods of the present invention. As depicted in Figure 14, the modules 202, 204, 206, 208, 210 are distinct modules which perform respective functions implemented by the merchant server 104. It will be appreciated that the boundaries between these modules are exemplary only, and that alternative embodiments may merge modules or impose an alternative decomposition of functionality of modules. For example, the modules discussed herein may be decomposed into sub-modules to be executed as multiple computer processes, and, optionally, on multiple computers. Moreover, alternative embodiments may combine multiple instances of a particular module or sub-module. It will also be appreciated that, while a software implementation of the modules 202, 204, 206, 208, 210 is described herein, these may alternatively be implemented as one or more hardware modules (such as field-programmable gate array(s) or application-specific integrated circuit(s)) comprising circuitry which implements equivalent functionality to that implemented in software. The ROM 1406 is used to store instructions and perhaps data which are read during program execution. The secondary storage 1404, the ROM 1406, and/or the RAM 1408 may be referred to in some contexts as computer readable storage media and/or non-transitory computer readable media. In some embodiments, the instructions and data used for implementing the aforementioned methods are provided in the form of a software development kit (SDK). The SDK may be provided to the merchant for use in configuring

the merchant portal so as to implement the methods described in the aforementioned embodiments.

[00117] I/O devices 1410 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.

[00118] The system connectivity or network devices 1412 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 or network devices 1412 may enable the processor 1402 to communicate with the Internet or one or more intranets. With such a system connection, it is contemplated that the processor 1402 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 1402, may be received from and outputted to the system, for example, in the form of a computer data signal embodied in a carrier wave.

[00119] The processor 1402 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 1404), flash drive, ROM 1406, RAM 1408, or the system connectivity or network devices 1412. While only one processor 1402 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.

[00120] 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.

[00121] It is understood that by programming and/or loading executable instructions onto the technical architecture, at least one of the CPU 1402, the ROM 1406, and the RAM 1408 are changed, transforming the technical architecture in part into a specific purpose machine or apparatus having the novel functionality taught by the present invention. 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.

[00122] 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 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 merchant server for authenticating a card-not-present payment transaction initiated by a user at a merchant portal using a user device, the server comprising:

- a transaction module configured to receive, from the user device, a transaction request comprising at least a payment card identifier and a user device identifier associated with the user device; and

- an authentication module configured to:

- determine, whether the payment card identifier and the user device identifier are registered for making payment at the merchant portal;

- transmit, to the user device, an authentication request to authenticate the card-not-present payment transaction if the payment card identifier and the user device identifier are registered for making payment at the merchant portal, the authentication request comprising a request for an authentication information input;

- receive, from the user device, an authentication response comprising the authentication information input;

- authenticate the authentication information input using stored authentication information registered for authenticating card-not-present payment transactions between the user and the merchant using the user device and the payment card identifier; and

- transmit, to an issuer server, an authorisation request comprising an authentication indication to indicate that the authentication information input has been authenticated.

2. The server of claim 1, wherein the authentication module is further configured to:

- transmit, to the issuer server, an authorisation request if it is determined that the payment card identifier and the user device are not registered for making payment at the merchant portal, the authorisation request comprises a request to generate an authentication code for authenticating the user;

- receive, from the user device, an authentication code input;

- transmit, to the issuer server, the authentication code input; and

- receive, from the issuer server, an authorisation response indicating that the card-not-present payment transaction is authorised if it is determined that the authentication code input matches the authentication code;

- the server further comprises an enrolment module configured to:

- transmit, to the user device, an enrolment request if the card-not-present payment transaction is authorised, the enrolment request comprising a request for registering the authentication information for authenticating card-not-present payment

transactions between the user and the merchant using the user device and the payment card identifier;

receive, from the user device, an enrolment response comprising the authentication information; and

store registration information for the user for making payment at the merchant portal, the registration information comprising the authentication information, the payment card identifier and the user device identifier.

3. The server of claim 2, wherein the authentication information is registered using a network server, the enrolment module is further configured to:

retrieve, from a merchant database, a merchant identifier associated with the merchant portal; and

transmit, to the network server, the authentication information, the payment card identifier, the user device identifier and the merchant identifier for registering the authentication information for authenticating card-not-present payment transactions between the user and the merchant using the user device and the payment card identifier;

wherein the registration information is stored at the network server.

4. The server of claim 3, wherein the authentication module is further configured to:

transmit, to the network server, a registration determination request comprising the payment card identifier, the user device identifier and the merchant identifier; and

receive, from the network server, a registration determination response comprising a registration indication indicating if the payment card identifier and the user device identifier are registered for making payment at the merchant portal.

5. The server of claim 3 or claim 4, wherein the authentication module is further configured to:

transmit, to the network server, a user verification request comprising the authentication information input; and

receive, from the network server, a user verification response comprising an authentication indication if the authentication information input matches the authentication information stored at the network server.

6. The server of claim 5, wherein a public key and a private key pair is generated by the user device and the public key is received at the network server, the authentication information input is signed using the private key by the user device and is authenticated by the network server using the public key.

7. The server of any one of the preceding claims, wherein the authentication indication comprises a cryptogram.

8. The server of any one of the preceding claims, further comprising a monitoring module, the monitoring module is configured to:

analyse past card-not-present payment transactions performed using the user device;

generate a user transaction pattern based on the past card-not-present payment transactions; and

determine that the card-not-present payment transaction is an unusual payment transaction if the card-not-present payment transaction does not conform to the user transaction pattern associated with the past card-not-present payment transactions.

9. A computer-implemented method for authenticating a card-not-present payment transaction initiated by a user at a merchant portal using a user device, the method comprising:

receiving, from the user device, a transaction request comprising at least a payment card identifier and a user device identifier associated with the user device;

determining whether the payment card identifier and the user device identifier are registered for making payment at the merchant portal;

transmitting, to the user device, an authentication request to authenticate the card-not-present payment transaction if the payment card identifier and the user device identifier are registered for making payment at the merchant portal, the authentication request comprising a request for an authentication information input;

receiving, from the user device, an authentication response comprising the authentication information input;

authenticate the authentication information input using stored authentication information registered for authenticating card-not-present payment transactions between the user and the merchant using the user device and the payment card identifier; and

transmitting, to an issuer server, an authorisation request comprising an authentication indication to indicate that the authentication input has been authenticated.

10. The method of claim 9, further comprising:

transmitting, to the issuer server, an authorisation request if it is determined that the payment card identifier and the user device are not registered for making payment at the merchant portal, the authorisation request comprises a request to generate an authentication code for authenticating the user;

receiving, from the user device, an authentication code input;

transmitting, to the issuer server, the authentication code input;

receiving, from the issuer server, an authorisation response indicating that the card-not-present payment transaction is authorised if it is determined that the authentication code input matches the authentication code;

transmitting, to the user device, an enrolment request if the card-not-present payment transaction is authorised, the enrolment request comprising a request for registering the authentication information for authenticating card-not-present payment transactions between the user and the merchant using the user device and the payment card identifier;

receiving, from the user device, an enrolment response comprising the authentication information; and

storing registration information for the user for making payment at the merchant portal, the registration information comprising the authentication information, the payment card identifier and the user device identifier.

11. The method of claim 10, wherein the authentication information is registered using a network server, the method further comprises:

retrieving, from a merchant database, a merchant identifier associated with the merchant portal; and

transmitting, to the network server, the authentication information, the payment card identifier, the user device identifier and the merchant identifier for registering the authentication information for authenticating card-not-present payment transactions between the user and the merchant using the user device and the payment card identifier;

wherein the registration information is stored at the network server.

12. The method of claim 11, further comprising:

transmitting, to the network server, a registration determination request comprising the payment card identifier, the user device identifier and the merchant identifier; and

receiving, from the network server, a registration determination response comprising a registration indication indicating if the payment card identifier and the user device identifier are registered for making payment at the merchant portal.

13. The method of claim 11 or claim 12, further comprising:

transmitting, to the network server, a user verification request comprising the authentication information input; and

receiving, from the network server, a user verification response comprising an authentication indication if the authentication information input matches the authentication information stored at the network server.

14. The method of claim 12, wherein a public key and a private key pair is generated by the user device and the public key is received at the network server, the authentication information input is signed using the private key by the user device and is authenticated by the network server using the public key.

15. The method of any one of claims 9 to 14, wherein the authentication indication comprises a cryptogram.

16. The method of any one of claims 9 to 15, further comprising:

- analysing past card-not-present payment transactions performed using the user device;
- generating a user transaction pattern based on the past card-not-present payment transactions; and

- determining that the card-not-present payment transaction is an unusual payment transaction if the card-not-present payment transaction does not conform to the user transaction pattern associated with the past card-not-present payment transactions.

17. The method of claim 16, wherein the determining step comprises using a transaction time and a payment amount associated with the card-not-present payment transaction.

18. The method of any one of claims 9 to 17, wherein the authentication information comprises a PIN or a biometric associated with the user.

19. A computer-implemented method for authenticating a card-not-present payment transaction initiated by a user at a merchant portal using a user device, the method comprising:

- receiving, from the user device, a transaction request comprising at least a payment card identifier and a user device identifier associated with the user device;

- determining whether the payment card identifier and the user device identifier are registered for making payment at the merchant portal;

- transmitting, to an issuer server, an authorisation request if it is determined that the payment card identifier and the user device are not registered for making payment at the merchant portal, the authorisation request comprises a request to generate an authentication code for authenticating the user;

- receiving, from the user device, an authentication code input;

- transmitting, to the issuer server, the authentication code input;

- receiving, from the issuer server, an authorisation response indicating that the card-not-present payment transaction is authorised if it is determined that the authentication code input matches the authentication code;

transmitting, to the user device, an enrolment request if the card-not-present payment transaction is authorised, the enrolment request comprising a request for registering the authentication information for authenticating card-not-present payment transactions between the user and the merchant using the user device and the payment card identifier;

receiving, from the user device, an enrolment response comprising the authentication information; and

storing registration information from the user for making payment at the merchant portal, the registration information comprising the authentication information, the payment card identifier and the user device identifier.

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 9 to 19.