

Computer system and computer-implemented method for authenticating a card-not-present payment transaction initiated using a user electronic device

Technical Field

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

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, new protocols for authenticating users in card-not-present payment transactions are needed. For example, a second-factor authentication with issuer involvement for card-not-present payment transactions can help to reduce the occurrence of fraud.

[0003] Although card verification methods such as the second-factor authentication performed by the issuer reduce fraud in card-not-present payment transactions, they may also increase friction in processing these card-not-present payment transactions. This can result in a higher drop-off rate and a poor customer experience for users of these card-not-present payment transactions. Therefore, a new system and method for authenticating a card-not-present payment transaction is needed to address these and other limitations.

Summary

[0004] In accordance with a first aspect of the present invention, there is provided a payment authentication system for authenticating a card-not-present payment transaction initiated using a user electronic device. The payment authentication system comprises an authentication server, a directory server and a payment network server. The authentication server comprises an authentication server processor, an authentication server data storage device and an authentication server database, the authentication server database storing a plurality of authentication records, each authentication record comprising a payment card identifier, a mobile number and a secure element identifier, the authentication server data storage device storing computer program instructions operable to cause the authentication server processor to: (i) receive, from the user electronic device, an authentication request comprising a payment card identifier, a mobile number and a secure element identifier associated with the user electronic device; and (ii) validate a combination of the payment card identifier, the mobile number and the secure element identifier of the authentication request by determining if the combination of the payment card identifier, the mobile number

and the secure element identifier matches an authentication record of the plurality of authentication records. The directory server comprises a directory server processor and a directory server data storage device, the directory server data storage device storing computer program instructions operable to cause the directory server processor to: (i) generate a network authentication value (AV) if the combination of the payment card identifier, the mobile number and the secure element identifier has been validated; (ii) store a combination of the network AV and the payment card identifier; and (iii) transmit, to the user electronic device, an authentication response comprising the network AV. The payment network server comprises a payment network server processor and a payment network server data storage device, the payment network server data storage device storing computer program instructions operable to cause the payment network server processor to: (i) receive, from the user electronic device, a transaction request comprising a received payment card identifier and a received network AV; (ii) determine if the received payment card identifier and the received network AV match the stored payment card identifier and the stored network AV; and (iii) transmit, to an issuer server, an authorization request comprising an authentication indication indicating that the card-not-present payment transaction has been authenticated if the received payment card identifier and the received network AV match the stored payment card identifier and the stored network AV.

[0005] Embodiments of the present invention therefore provide a payment authentication system for authenticating a card-not-present transaction initiated using a user electronic device. The payment authentication system comprises the authentication server, the directory server and the payment network server. In particular, the authentication server of the payment authentication system is configured to receive an authentication request from the user electronic device, and to validate a combination of the payment card identifier, the mobile number and the security element identifier by determining if the combination of the payment card identifier, the mobile number and the secure element identifier matches an authentication record. As will be described in relation to Figs. 5 and 11, information for the authentication record may be registered with the authentication server of the payment authentication system. The authentication record can then then used to authenticate the user in processing the card-not-present payment transaction. Once the combination of the payment card identifier, the mobile number and the security element identifier is validated, a request for a network authentication value (AV) is transmitted to the directory server. The directory server is configured to generate a network AV and transmits it to the user electronic device. The directory server is also configured to store the network AV. During a card-not-present payment transaction performed using the user electronic device, the transaction request received at the payment network server comprises at least a received payment card identifier and a received network AV. The payment network server is

configured to determine if the received payment card identifier and the received network AV match the stored payment card identifier and the stored network AV, and to transmit an authorization request comprising an authentication indication indicating that the card-not-present payment transaction has been authenticated to the issuer server if the received payment card identifier and the received network AV match the stored payment card identifier and the stored network AV. Authentication of the network AV during the card-not-present payment process therefore provides additional authentication for 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 payment authentication system 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, which may help to improve the approval rates for card not present transactions. Further, the authentication request made by the user electronic device in processing the card-not-present payment transaction may be performed in the background without any user intervention. For example, once the user initiate a card-not-present payment transaction on the user electronic device, the authentication request for the network AV and the subsequent payment request to the payment network can be performed in the background automatically by the user electronic device. In this way, the card-not-present payment transaction can be authenticated, processed and authorized with a single action by the user. This simplifies the payment transaction process and improves a payment experience of the user.

[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, such as authentication records and network AVs, for use in authenticating card-not-present payment transactions. This can be easily implemented using existing memory storages, servers and/or databases.

[0007] The authentication request may comprise a payment amount, and the directory server data storage device may store computer program instructions operable to cause the directory server processor to: (i) compare the payment amount with a threshold amount,

the card-not-present payment transaction is a high-value transaction if the payment amount is greater than the threshold amount; (ii) transmit, to the issuer server, a request to provide an issuer AV if the payment amount is greater than the threshold amount, the request comprising the mobile number and the secure element identifier; (iii) receive, from the issuer server, the issuer AV; and (iv) transmit, to the user electronic device, the issuer AV.

[0008] The payment network server data storage device may store computer program instructions operable to cause the payment network server processor to: (i) receive, from the user electronic device, a high-value transaction request comprising a received issuer AV, a received payment card identifier and an indication of a high-value payment amount; (ii) transmit, to the issuer server, a high-value authorization request comprising the payment card identifier, the received issuer AV and the received payment card identifier; and (iii) receive, from the issuer server, an authorization response indicating whether the card-not-present payment transaction is authorised to proceed, the card-not-present payment transaction is authorised to proceed if the received issuer AV and the received payment card identifier match the stored issuer AV and the stored payment card identifier at the issuer server.

[0009] The payment card identifier or the received payment card identifier may be a tokenized payment card identifier.

[0010] The transaction request or the high-value transaction request may comprise a device-generated cryptogram, and the payment network server data storage device may store computer program instructions operable to cause the payment network server processor to authenticate a combination of the device-generated cryptogram and the tokenized payment card identifier.

[0011] In accordance with a second aspect of the present invention, there is provided a payment authentication system for authenticating a card-not-present payment transaction initiated using a user electronic device. The payment authentication system comprising an authentication server, a directory server and a payment network server. The authentication server comprising an authentication server processor and an authentication server data storage device, the authentication server data storage device storing computer program instructions operable to cause the authentication server processor to: receive, from the user electronic device, an authentication request comprising a payment card identifier, a mobile number and a secure element identifier associated with the user electronic device. The directory server comprising a directory server processor and a directory server data storage device, the directory server data storage device storing computer program instructions operable to cause the directory server processor to: (i) transmit, to an issuer server, a request to provide an issuer AV, the request comprising the payment card

identifier, the mobile number and the secure element identifier; (ii) receive, from the issuer server, the issuer AV indicating that a combination of the payment card identifier, the mobile number and the secure element identifier matches a stored authentication record comprising the payment card identifier, the mobile number and the secure element identifier; and (iii) transmit, to the user electronic device, an authentication response comprising the issuer AV. The payment network server comprising a payment network server processor and a payment network server data storage device, the payment network server data storage device storing computer program instructions operable to cause the payment network server processor to: (i) receive, from the user electronic device, a transaction request comprising a received payment card identifier and a received issuer AV; and (ii) transmit, to the issuer server, an authorization request comprising the received payment card identifier and the received issuer AV for authenticating the received payment card identifier and the received issuer AV.

[0012] The authentication server may comprise an authentication server database storing a plurality of authentication records, each authentication record comprising a payment card identifier, a mobile number and a secure element identifier, the authentication server data storage device further stores computer program instructions operable to cause the authentication server processor to: validate the combination of the payment card identifier, the mobile number and the secure element identifier by determining if the combination of the payment card identifier, the mobile number and the secure element identifier matches an authentication record of the plurality of authentication records, wherein the request to provide the issuer AV is transmitted to the issuer server if the combination of the payment card identifier, the mobile number and the secure element identifier is validated.

[0013] The payment card identifier or the received payment card identifier may be a tokenized payment card identifier and the transaction request may comprise a device-generated cryptogram, the payment network server data storage device may store computer program instructions operable to cause the payment network server processor to authenticate a combination of the device-generated cryptogram and the tokenized payment card identifier.

[0014] The system may comprise a registration server, the registration server comprising a registration server processor and a registration server data storage device, the registration server data storage device storing computer program instructions operable to cause the registration server processor to: (i) receive, from the user electronic device, a registration request comprising the payment card identifier, the mobile number and the secure element identifier; (ii) store, using a registration server database, a registration record comprising the payment card identifier, the mobile number and the secure element identifier; (iii) transmit, to the issuer server, the registration record for registering with the issuer server;

and (iv) transmit, to the user electronic device, a registration response indicating that the payment card identifier, the mobile number and the secure element identifier have been registered.

[0015] In accordance with a third aspect, there is provided a payment authentication method for authenticating a card-not-present payment transaction initiated using a user electronic device, the method comprising: (i) receiving, from the user electronic device, an authentication request comprising a payment card identifier, a mobile number and a secure element identifier associated with the user electronic device; (ii) validating, a combination of the payment card identifier, the mobile number and the secure element identifier of the authentication request by determining if the combination of the payment card identifier, the mobile number and the secure element identifier matches an authentication record, the authentication record being one of a plurality of authentication records stored in an authentication server database, each of the plurality of authentication records comprising a payment card identifier, a mobile number and a secure element identifier; (iii) generating, a network authentication value (AV) if the combination of the payment card identifier, the mobile number and the secure element identifier has been validated; (iv) storing, a combination of the network AV and the payment card identifier; (v) transmitting, to the user electronic device, an authentication response comprising the network AV; (vi) receiving, from the user electronic device, a transaction request comprising a received payment card identifier and a received network AV; (vii) determining, if the received payment card identifier and the received network AV match the stored payment card identifier and the stored network AV; and (viii) transmitting, to an issuer server, an authorization request comprising an authentication indication indicating that the card-not-present payment transaction has been authenticated if the received payment card identifier and the received network AV match the stored payment card identifier and the stored network AV.

[0016] The authentication request may comprise a payment amount and the method may comprise: (i) comparing, the payment amount with a threshold amount, the card-not-present payment transaction is a high-value transaction if the payment amount is greater than the threshold amount; (ii) transmitting, to the issuer server, a request to provide an issuer AV if the payment amount is greater than the threshold amount, the request comprising the payment card identifier, the mobile number and the secure element identifier; (iii) receiving, from the issuer server, the issuer AV; and (iv) transmitting, to the user electronic device, the issuer AV.

[0017] The method may comprise: (i) receiving, from the user electronic device, a high-value transaction request comprising a received issuer AV, a received payment card identifier and an indication of a high-value payment amount; (ii) transmitting, to the issuer server, a

high-value authorization request comprising the received issuer AV and the received payment card identifier; and (iii) receiving, from the issuer server, an authorization response indicating whether the card-not-present payment transaction is authorised to proceed, the card-not-present payment transaction is authorised to proceed if the received issuer AV and the received payment card identifier match the stored issuer AV and the stored payment card identifier at the issuer server.

[0018] The payment card identifier or the received payment card identifier may be a tokenized payment card identifier and the transaction request or the high-value transaction request may comprise a device-generated cryptogram, and the method may comprise authenticating a combination of the device-generated cryptogram and the tokenized payment card identifier.

[0019] In accordance with a fourth aspect, there is described a payment authentication method for authenticating a card-not-present payment transaction initiated using a user electronic device, the method comprising: (i) receiving, from the user electronic device, an authentication request comprising a payment card identifier, a mobile number and a secure element identifier associated with the user electronic device; (ii) transmitting, to an issuer server, a request to provide an issuer AV, the request comprising the payment card identifier, the mobile number and the secure element identifier; (iii) receiving, from the issuer server, the issuer AV indicating that a combination of the payment card identifier, the mobile number and the secure element identifier matches a stored authentication record comprising the payment card identifier, the mobile number and the secure element identifier; (iv) transmitting, to the user electronic device, an authentication response comprising the issuer AV; (v) receiving, from the user electronic device, a transaction request comprising a received payment card identifier and a received issuer AV; and (vi) transmitting, to the issuer server, an authorization request comprising the received payment card identifier and the received issuer AV for authenticating the received payment card identifier and the received issuer AV.

[0020] The method may comprise validating the combination of the payment card identifier, the mobile number and the secure element identifier by determining if the combination of the payment card identifier, the mobile number and the secure element identifier matches an authentication record, the authentication record being one of a plurality of authentication records stored in an authentication server database, each of the plurality of authentication records comprising a payment card identifier, a mobile number and a secure element identifier, wherein the request to provide the issuer AV is transmitted to the issuer server if the combination of the payment card identifier, the mobile number and the secure element identifier is validated.

[0021] The payment card identifier or the received payment card identifier may be a tokenized payment card identifier, the transaction request may comprise a device-generated cryptogram, and the method may comprise authenticating a combination of the device-generated cryptogram and the tokenized payment card identifier.

[0022] The method may comprise: (i) receiving, from the user electronic device, a registration request comprising the payment card identifier, the mobile number and the secure element identifier; (ii) storing, using a registration server database, a registration record comprising the payment card identifier, the mobile number and the secure element identifier; (iii) transmitting, to the issuer server, the registration record for registering with the issuer server; and (iv) transmitting, to the user electronic device, a registration response indicating that the payment card identifier, the mobile number and the secure element identifier have been registered.

[0023] The method may comprise: (i) tokenizing the payment card identifier; and (ii) storing the tokenized payment card identifier in the registration record, wherein the payment card identifier comprised in the registration response for transmission to the user electronic device may be a tokenized payment card identifier.

[0024] The method may comprise receiving, from the user electronic device, transaction authentication data comprising the tokenized payment card identifier, the mobile number and the secure element identifier.

[0025] In accordance with a fifth aspect of the present invention, a non-transitory computer-readable medium having stored thereon program instructions for causing at least one processor to perform the preceding methods.

[0026] 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).

[0027] 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.

[0028] 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

[0029] 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 computerized network for authenticating a card-not-present payment transaction in accordance with an embodiment of the present invention;

Fig. 2 shows a block diagram of servers and databases comprised in a payment authentication system of the computerized network of Fig. 1 in accordance with an embodiment of the present invention;

Fig. 3 shows steps of a payment authentication method which may be performed by the payment authentication system of Fig. 2 in accordance with an embodiment of the present invention;

Fig. 4 shows steps of a payment authentication method which may be performed by the payment authentication system of Fig. 2 if a payment amount is greater than a threshold amount in accordance with an embodiment of the present invention;

Fig. 5 shows steps of a method for registering with the payment authentication system of Fig. 2 for authenticating a card-not-present transaction in accordance with an embodiment of the present invention;

Fig. 6 shows steps of a method for tokenizing a payment card identifier which may be performed by the payment authentication system of Fig. 2 in accordance with an embodiment of the present invention;

Fig. 7 shows steps of a method for authenticating a card-not-present payment transaction which may be performed by the payment authentication system 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 payment authentication system 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 using the payment authentication system of Fig. 2 in accordance with an embodiment of the present invention;

Fig. 10 shows a computerized network for authenticating a card-not-present payment transaction using the payment authentication system of Fig. 2 in accordance with an embodiment of the present invention;

Fig. 11 shows message flows in a method for registering with the payment authentication system of Fig. 2 in accordance with an embodiment of the present invention;

Fig. 12 shows a computerized network for registering with the payment authentication system of Fig. 2 for authenticating a card-not-present payment transaction in accordance with an embodiment of the present invention; and

Fig. 13 shows schematically a hardware structure of the payment authentication system which may be used in the computerized network of Figs. 1, 10 and 12 to implement a method in accordance with an embodiment of the present invention.

Detailed description of the embodiment

[0030] 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.

[0031] 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.

[0032] 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.

[0033] 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.

[0034] 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 . . .).

[0035] Fig. 1 shows a computerized network 100 for authenticating a card-not-present payment transaction in accordance with an embodiment of the present invention. The computer system 100 comprises a user electronic device 102 and a merchant server 104. The user electronic device 102 may be any electronic device associated with the user which enables the user to perform a card-not-present payment transaction. 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 a merchant portal on which card-not-present payment transactions can be initiated. The computer system 100 further comprises an acquirer server 106, a payment authentication system 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 authentication system 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. The payment authentication system 108 may comprise one or more servers. An embodiment in which the payment authentication comprises a plurality of servers is described below in relation to Fig. 2.

[0036] Databases for storing relevant data used in embodiments of the present invention are also included in the computerized network 100. As shown in Fig. 1, the computerized network 100 further comprises a payment authentication system database 112 which is connected to the payment authentication system 108. The payment authentication system database 112 may be configured to store a plurality of authentication records, each of the plurality of authentication records comprising a payment card identifier, a mobile number and a security element identifier. The payment card identifier may be a payment card number associated with the payment card, or may be a token associated with the payment card in the form of a tokenized payment card identifier. The mobile number is a registered telecommunication number associated with the user electronic device 102. The mobile number is typically unique to a SIM (subscriber identification module) card which associates a user to a user mobile account registered with a telecommunication company. The secure element identifier is a unique identifier associated with a secure element of the user electronic device 102. A secure element is a microprocessor chip which can be used to store sensitive data that is embedded within the user electronic device 102, with each microprocessor chip having a unique identification number (e.g. similar to an international mobile equipment identity (IMEI) number). The secure element identifier therefore provides a unique identification of the user electronic device 102. Embodiments of the present invention uses a combination of the payment card identifier, the mobile number and the secure element identifier for authentication the user in a card-not-present payment transaction.

[0037] Further, an issuer database 114 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 identifier such as 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.). In embodiments where the issuer server 110 generates an issuer AV for authenticating card-not-present payment transactions, the issuer database 114 stores data associated with the generated issuer AVs and a plurality of authentication records for validating a combination of a payment card identifier, a mobile number and a secure element identifier. Although the payment authentication system database 112 and the issuer database 114 are shown as external databases in Fig. 1, these databases 112, 114 may also form part of the payment authentication system 108 and the issuer server 110 respectively.

[0038] While only one user electronic device 102 and only one merchant server 104 are shown in Fig. 1, it is appreciated that a plurality of user electronic devices 102 and a plurality of merchant servers 104 associated with respective merchant portals may also form part of the computerized network 100. Similarly, a plurality of acquirer servers 106 and a plurality of issuer servers 110 may also be in communication with the payment authentication system 108 and form part of the computerized network 100. Likewise, a plurality of payment authentication system databases 112 and issuer databases 114 associated with the payment authentication system 108 and respective issuer servers 110 respectively may also form part of the computerized network 100.

[0039] Communication between the user electronic device 102, the merchant server 104, the acquirer server 106, the payment authentication system 108, the issuer server 110 and databases 112, 114 may take place via any type of communication 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.

[0040] Fig. 2 shows a block diagram showing components of the payment authentication system 108. In an embodiment, the payment authentication system 108 comprises an authentication server 202, a directory server 204, a payment network server 206, and a registration server 208. The authentication server 202 is operable to receive authentication request from the user electronic device 102 to authenticate card-not-present payment transactions initiated by the user electronic device 102 using a plurality of stored authentication records registered with the payment authentication system 108. The directory server 204 is configured to provide an authentication value (AV) to the user electronic device 102 for processing the card-not-present payment transaction. The authentication value may be generated by the directory server 204 as a network AV or it may be received from the issuer server 110 as an issuer AV. The payment network server 206 is operable to facilitate processing of card-not-present payment transactions received from the user electronic device 102, for example, in requesting authorization of the card-not-present payment transactions from the issuer server 110. The registration server 208 is operable to register the user for authenticating card-not-present payment transactions. In addition, each of the servers 202, 204, 206, 208 may comprise a respective database. An authentication server database 212 is in communication with the authentication server 202, and is operable to store a plurality of authentication records for use in authenticating card-not-present payment transactions. Each of the authentication records comprises a payment card identifier, a mobile number and a secure element identifier. A directory server database 214 is in communication with the directory server 204, and is operable to store combinations of a network AV with its associated payment card identifier. A payment network server database 216 is in communication with the payment network server 206,

and is operable to store data in relation to processing card-not-present payment transactions. This may include a copy of the network AV generated by the directory server 204, and other transaction details such as a payment card identifier, a payment amount, a time of transaction etc. of a card-not-present payment transaction. A registration server database 218 is in communication with the registration server 208, and is operable to store a plurality of registration records. Each registration record includes at least a payment card identifier, a mobile number and a secure element identifier. In an embodiment, the registration server is operable to tokenize the payment card identifier. In this case, the registration server database 218 may be operable to store the tokenized payment card identifier.

[0041] Although it is shown here in Fig. 2 that the authentication server database 212, the directory server database 214, the payment network server database 216 and the registration server database 218 are separate databases, in some embodiments, they may form part of the payment authentication system database 112 as shown in Fig. 1.

[0042] Fig. 3 shows steps of a payment authentication method 300 which may be performed by the payment authentication system 108 of Fig. 1 in accordance with an embodiment of the present invention.

[0043] In a step 302, the authentication server 202 of the payment authentication system 108 receives, from the user electronic device 102, an authentication request. The authentication request comprises a payment card identifier, a mobile number and a secure element identifier associated with the user electronic device 102. In an embodiment, the authentication request further comprises a payment amount associated with the card-not-present payment transaction. In some embodiments, the payment card identifier in the authentication request is a tokenized payment card identifier. In these cases, the authentication server 202 may retrieve a payment card identifier (e.g. a payment card number) using the tokenized payment card identifier. This may be performed by communicating with the registration server 208 of the payment authentication system 108. In some embodiments, the authentication request comprises other information such as a token expiry (if the authentication request comprises a tokenized payment card identifier), a currency code, a country code and a transaction time-stamp.

[0044] In a step 304, the authentication server 202 of the payment authentication system 108 validates a combination of the payment card identifier, the mobile number and the secure element identifier in the authentication request. The authentication server 202 validates the combination by determining if the combination of the payment card identifier, the mobile number and the secure element identifier matches an authentication record of the plurality of authentication records using the authentication server database 212.

[0045] If the combination of the payment card identifier, the mobile number and the secure element identifier is validated in the step 304, a request to provide an authentication value is transmitted by the authentication server 202 to the directory server 204.

[0046] In an embodiment where the authentication request comprises the payment amount, in an optional step 306, the directory server 204 of the payment authentication system 108 compares the payment amount with a threshold amount. If it is determined that the payment amount is greater than the threshold amount, the card-not-present payment transaction is considered a high-value transaction. In this case, an issuer authentication value is required for authenticating the high-value transaction. The method for authenticating a high-value transaction is described later in relation to Fig. 4. If it is determined that the payment amount is less than or equal to the threshold amount, the method for authentication a card-not-present payment transaction continues in a step 308. The threshold amount may be altered in response to regulatory requirements imposed by the jurisdiction concerned. In some embodiments, the directory server 204 does not perform the step 306. In these cases, once the combination of the payment card identifier, the mobile number and the secure element identifier is validated in the step 304, the directory server 204 performs a step 308 as described below.

[0047] In the step 308, the directory server 204 of the payment authentication system 108 generates a network authentication value (AV) if the combination of the payment card identifier, the mobile number and the secure element identifier has been validated in the step 304. In an embodiment, the directory server 204 of the payment authentication system 108 generates a network AV if it is determined that the payment amount is less than or equal to the threshold amount. The network AV may comprise any length of a string of alphanumeric and/or symbols, and may be unique for each card-not-present payment transaction.

[0048] In a step 310, the directory server 204 of the payment authentication system 108 stores a combination of the network AV and the payment card identifier. In this case, the network AV is tied to the payment card identifier so that a card-not-present payment transaction requested using the payment card identifier is authenticated with the network AV. The combination of the network AV and the payment card identifier may be stored at the directory server database 214. In some embodiments, the combination of the network AV and the payment card identifier may be transmitted to the payment network server 206 and stored at the payment network server database 216.

[0049] In a step 312, the directory server 204 of the payment authentication system 108 transmits an authentication response to the user electronic device 102. The authentication

response comprises the network AV. The network AV may then be used by the user electronic device 102 for processing the card-not-present payment transaction.

[0050] In a step 314, the payment network server 206 of the payment authentication system 108 receives a transaction request from the user electronic device 102. The transaction request comprises a received payment card identifier and a received network AV. In some embodiments, the received payment card identifier is a tokenized payment card identifier. In some embodiments, the transaction request may comprise a cryptogram associated with the payment card identifier or the tokenized payment card identifier, the cryptogram of the transaction request may be used for further authentication. The cryptogram of the transaction request may be generated by the user electronic device 102. An example of a cryptogram of the transaction request is a digital secure remote payment (DSRP) cryptogram.

[0051] In a step 316, the payment network server 206 of the payment authentication system 108 determines if the received payment card identifier and the received network AV match the stored payment card identifier and the stored network AV. In an embodiment, in order to determine if the received payment card identifier and the received network AV match the stored payment card identifier and the stored network AV, the payment network server 206 queries for the combination of the stored payment card identifier and the stored network AV. In an embodiment where the combination of the stored payment card identifier and the stored network AV is stored in the directory server database 214, the payment network server 206 communicates with the directory server 204 to determine if the stored combination matches the received combination comprised in the transaction request. In some embodiments where a cryptogram is comprised in the transaction request, the payment network server 206 of the payment authentication system 108 may validate the cryptogram.

[0052] If it is determined that the received payment card identifier and the received network AV match the stored payment card identifier and the stored network AV, the payment network server 206 of the payment authentication system 108 generates an authentication indication for indicating that the card-not-present payment transaction is authenticated. In some embodiments where a cryptogram is comprised in the transaction request, the authentication indication is generated if the cryptogram is also validated. The authentication indication may be included in a field comprised in the authorization 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. In some embodiments, if the payment card identifier comprises a tokenized payment card identifier for use in processing the e-commerce

transaction, the payment network server 108 identifies a payment card number using the token. The payment card number is then transmitted to the issuer server 110 as the payment card identifier for use in authenticating the user of the card-not-present payment transaction.

[0053] If it is determined that the received payment card identifier and the received network AV do not match the stored payment card identifier and the stored network AV, the payment network server 206 of the payment authentication system 108 refuses to proceed with the card-not-present payment transaction. In this case, the payment network server 206 of the payment authentication system 108 may prompt the user electronic device 102 to re-submit the transaction request and/or provide other form of payment for the card-not-present payment transaction.

[0054] In a step 318, the payment network server 206 of the payment authentication system 108 transmits an authorization request to the issuer server 110. The authorization request comprises an authentication indication indicating that the card-not-present payment transaction has been authenticated if the received payment card identifier and the received network AV match the stored payment card identifier and the stored network AV. The authentication indication functions to indicate that the card-not-present payment transaction has been authenticated. Therefore, no further authentication may be required to be performed by the issuer server 110. The issuer server 110 may then authorize the card-not-present payment transaction based on the authentication results provided by the payment authentication system 108.

[0055] Fig. 4 shows steps of a payment authentication method 400 which may be performed by the payment authentication system of Fig. 2 in accordance with an embodiment of the present invention. The method 400 follows from the comparing step 306, and may be performed if the payment amount of the card-not-present payment transaction is greater than the threshold amount. The method 400 differs primarily from the method 300 in that the authentication value is provided by the issuer server 110 instead of generated by the directory server 204 of the payment authentication system 108.

[0056] In a step 402, the directory server 204 of the payment authentication system 108 transmits a request to the issuer server 110 to provide an issuer AV if the payment amount is greater than the threshold amount. The request comprises the payment card identifier, the mobile number and the secure element identifier. Upon receiving the request, the issuer server 110 determines if the payment card identifier, the mobile number and the secure element identifier provided in the request match the payment card identifier, the mobile number and the secure element identifier registered with the issuer server 110. Detail of the registration process is discussed later in relation to Fig. 5. Once the issuer

server 110 determines that the payment card identifier, the mobile number and the secure element identifier received from the directory server 204 match those registered, the issuer server 110 generates an issuer AV and transmits the issuer AV to the directory server 204 of the payment authentication system 108. The issuer server 110 may then store the combination of the generated issuer AV and the payment card identifier. An example of an issuer AV is an accountholder authentication value (AAV) generated by an access control server (ACS) server associated with the issuer institution.

[0057] In a step 404, the directory server 204 of the payment authentication system 108 receives the issuer AV from the issuer server 110.

[0058] In a step 406, the directory server 204 of the payment authentication system 108 transmits the issuer AV to the user electronic device 102. The user electronic device 102 may then use the issuer AV for processing the card-not-present payment transaction.

[0059] In a step 408, the payment network server 206 of the payment authentication system 108 receives a high-value transaction request from the user electronic device 102. The high-value transaction request comprises a received issuer AV, a received payment card identifier and an indication of a high-value payment amount. Similar to the step 314, in some embodiments, the received payment card identifier is a tokenized payment card identifier. In some embodiments, the high-value transaction request may comprise a cryptogram associated with the payment card identifier or the tokenized payment card identifier, the cryptogram of the transaction request may be used for further authentication. If a cryptogram is comprised in the transaction request, the payment network server 206 may validate the cryptogram in a similar manner as aforementioned described in relation to the step 316. In some embodiments, if the payment card identifier comprises a tokenized payment card identifier for use in processing the e-commerce transaction, the payment network server 108 identifies a payment card number using the token. The payment card number is then transmitted to the issuer server 110 as the payment card identifier for use in authenticating the user of the card-not-present payment transaction.

[0060] In a step 410, the payment network server 206 of the payment authentication system 108 transmits a high-value authorization request to the issuer server 110. The high-value authorization request comprises the received issuer AV and the received payment card identifier. The received issuer AV and the received payment card identifier are transmitted to the issuer server 110 for the issuer server 110 to validate the combination of the received issuer AV and the received payment card identifier. The issuer server 110 may validate the combination of the received issuer AV and the received payment card identifier using the stored combination of the generated issuer AV and the payment card identifier.

[0061] In a step 412, the payment network server 206 of the payment authentication system 108 receives an authorization response from the issuer server 110. The authorization response indicates whether the card-not-present payment transaction is authorised to proceed. The card-not-present payment transaction is authorised to proceed if the received issuer AV and the received payment card identifier match the stored issuer AV and the stored payment card identifier at the issuer server as aforementioned described.

[0062] Fig. 5 shows steps of a method 500 for registering with the payment authentication system 108 of Fig. 2 for authenticating a card-not-present transaction in accordance with an embodiment of the present invention.

[0063] In a step 502, the registration server 208 of the payment authentication system 108 receives, from the user electronic device 102, a registration request. The registration request comprises a payment card identifier, a mobile number and a secure element identifier.

[0064] In a step 504, the registration server 208 of the payment authentication system 108 stores, using the registration server database 218, a registration record. The registration record comprises the payment card identifier, the mobile number and the secure element identifier received in the step 502.

[0065] In a step 506, the registration server 208 of the payment authentication system 108 transmits the registration record to the issuer server 110. The registration record transmitted to the issuer server 208 is stored by the issuer server 110 for use in authenticating a card-not-present payment transaction involving a payment amount that is greater than a threshold amount.

[0066] In a step 508, the registration server 208 of the payment authentication system 108 transmits a registration response to the user electronic device 102. The registration response indicates that the payment card identifier, the mobile number and the secure element identifier have been registered.

[0067] Fig. 6 shows steps of a method 600 for tokenizing a payment card identifier which may be performed by the payment authentication system of Fig. 2 in accordance with an embodiment of the present invention.

[0068] In a step 602, the registration server 208 of the payment authentication system 108 tokenizes the payment card identifier received in the registration request in the step 502.

[0069] In a step 604, the registration server 208 of the payment authentication system 108 stores the tokenized payment card identifier together with the payment card identifier, the

mobile number and the secure element identifier in the registration record in the registration server database 218.

[0070] In embodiments where the payment card identifier is tokenized by the registration server 208 of the payment authentication system 108, the registration server 208 of the payment authentication system 108 may transmit a registration response to the user electronic device 102. The registration response comprises the tokenized payment card identifier. The tokenized payment card identifier may be included in the registration response in addition to or in place of the payment card identifier.

[0071] Fig. 7 shows steps of a method 700 for authenticating a card-not-present payment transaction which may be performed by the payment authentication system 108 of Fig. 2 in accordance with an embodiment of the present invention. The primary difference in the method 700 as compared to the method 300 is that the validation of a combination of a payment card identifier, a mobile number and a secure element identifier is performed by the issuer server 110 so as to generate an issuer authentication value for use in processing the card-not-present payment transaction. In this embodiment, it may not be necessary for the directory server 204 to compare a payment amount associated with the card-not-present payment transaction with a threshold amount (as described in the step 306).

[0072] In a step 702, the authentication server 202 of the payment authentication system 108 receives an authentication request from the user electronic device 102. The authentication request comprises a payment card identifier, a mobile number and a secure element identifier associated with the user electronic device 102. Upon receipt of the authentication request, the authentication server 202 communicates the authentication request to the directory server 204 of the payment authentication system 108. In an embodiment, the authentication server 202 performs validation of a combination of the payment card identifier, the mobile number and the secure element identifier. In some embodiments, the authentication request may comprise a tokenized payment card identifier. In this case, the authentication server 202 may retrieve a payment card identifier using the tokenized payment card identifier.

[0073] In a step 704, the directory server 204 of the payment authentication system 108 transmits a request to the issuer server 110 to provide an issuer AV. The request comprises the payment card identifier, the mobile number and the secure element identifier. Upon receiving the request, the issuer server 110 determines if the payment card identifier, the mobile number and the secure element identifier provided in the request match the payment card identifier, the mobile number and the secure element identifier registered with the issuer server 110. Once the issuer server 110 determines that the payment card

identifier, the mobile number and the secure element identifier received from the directory server 204 match those registered, the issuer server 110 generates an issuer AV and transmits the issuer AV to the directory server 204 of the payment authentication system 108. The issuer server 110 may then store the combination of the generated issuer AV and the payment card identifier in the issuer server database 114.

[0074] In a step 706, the directory server 204 of the payment authentication system 108 receives the issuer AV from the issuer server 110. The receipt of the issuer AV from the issuer server 110 indicates that the combination of the payment card identifier, the mobile number and the secure element identifier matches the stored authentication record at the issuer server 110.

[0075] In a step 708, the directory server 204 of the payment authentication system 108 transmits the issuer AV to the user electronic device 102. The user electronic device 102 may then use the issuer AV for processing the card-not-present payment transaction.

[0076] In a step 710, the payment network server 206 of the payment authentication system 108 receives a transaction request from the user electronic device 102. The transaction request comprises a received issuer AV and a received payment card identifier. In some embodiments, the transaction request comprises a tokenized received payment card identifier. In this case, the payment network server 206 retrieves a received payment card identifier using the tokenized received payment card identifier by communicating with the registration server 208. In some embodiments, the transaction request comprises a cryptogram associated with the payment card identifier or the tokenized payment card identifier.

[0077] In a step 712, the payment network server 206 of the payment authentication system 108 transmits an authorization request to the issuer server 110. The authorization request comprises the received issuer AV and the received payment card identifier. The received issuer AV and the received payment card identifier are transmitted to the issuer server 110 for the issuer server 110 to validate the combination of the received issuer AV and the received payment card identifier. The issuer server 110 may validate the combination of the received issuer AV and the received payment card identifier using the stored combination of the generated issuer AV and the payment card identifier. In some embodiments where the transaction request comprises a cryptogram associated with the payment card identifier or the tokenized payment card identifier, the payment network server 206 may be configured to validate the cryptogram. In these cases, the authorization request may be transmitted by the payment network server 206 to the issuer server 110 if the cryptogram is validated.

[0078] In a step 714, the payment network server 206 of the payment authentication system 108 receives an authorization response from the issuer server 110. The authorization response indicates whether the card-not-present payment transaction is authorised to proceed. The card-not-present payment transaction is authorised to proceed if the received issuer AV and the received payment card identifier match the stored issuer AV and the stored payment card identifier at the issuer server as aforementioned described.

[0079] As described above with reference to Figs. 3, 4 and 7, there are three different embodiments for authenticating a card-not-present payment transaction. In particular, the method 300 of Fig. 3 can be performed regardless of a value of the card-not-present payment transaction. In some embodiments, the step 306 is performed by the directory server 204 of the payment authentication system 108. In these embodiments, if a payment amount of the card-not-present payment transaction is greater than a threshold amount, the validation of a combination of a payment card identifier, a mobile number and a secure element identifier and the generation of an authentication value for processing the card-not-present transaction are performed by the issuer server 110 as described in the method 400 of Fig. 4, in place of the payment authentication system 108 of the method 300 of Fig. 3. In yet other embodiments, the validation of a combination of a payment card identifier, a mobile number and a secure element identifier and the generation of an authentication value for processing the card-not-present transaction is performed by the issuer server 110 as described in the method 700 of Fig. 7, regardless of the value of the payment amount of the card-not-present payment transaction.

[0080] Figs. 8 and 9 show message flows for methods 800, 900 for authenticating a card-not-present payment transaction. For simplicity, only the payment authentication system 108 is shown in Figs. 8 and 9 as a collective representation of the different servers 202, 204, 206, 208 comprised in the payment authentication system 108 as described in relation to Fig. 2.

[0081] Fig. 8 shows message flows in a method 800 for authenticating a card-not-present payment transaction using the payment authentication system of Fig. 2 in accordance with an embodiment of the present invention. The user is required to be pre-registered with the payment authentication system 108 prior to using a combination of a payment card identifier, a mobile number and a secure element identifier for authenticating a card-not-present payment transaction. The message flow of the method 800 described below corresponds to the method 300 described in relation to Fig. 3.

[0082] To begin a card-not-present payment transaction, the user initiates a card-not-present payment transaction using the user electronic device 102. This may involve using an electronic wallet associated with the user electronic device 102 by the user to perform a purchase at a merchant portal associated with the merchant server 104. In order to

process the card-not-present payment transaction, the card-not-present payment transaction needs to be authenticated. In a step 802, the user electronic device 102 transmits an authentication request to the payment authentication system 108. Although it is shown in Fig. 8 that the authentication request is transmitted to the payment authentication system 108 directly, in some embodiments, the user electronic device 102 transmits the authentication request to the payment authentication system 108 via the merchant server 104 and/or the acquirer server 106. The authentication request comprises a payment card identifier, a mobile number and a secure element identifier associated with the user electronic device. In an embodiment, the authentication request further comprises a payment amount associated with the card-not-present payment transaction. In some embodiments, the authentication request further comprises a currency code and a country code associated with the card-not-present payment transaction, and a time of initiation of the card-not-present payment transaction. In some embodiments where a tokenized payment card identifier is used, the authentication request comprises the tokenized payment card identifier in place of the payment card identifier and includes a token expiry associated with the tokenized payment card identifier. If the authentication request comprises a tokenized payment card identifier, the authentication server 202 may communicate with the registration server 208 to retrieve a payment card identifier associated with the tokenized payment card identifier. The payment card identifier, the mobile and/or the secure element identifier may be provided automatically by the user electronic device 102 in the authentication request. To do so, the user device 102 may be configured to retrieve the payment card identifier, the mobile number and/or the secure element identifier and to transmit the payment card identifier, the mobile number and/or the secure element identifier as part of the authentication request when the card-not-present payment transaction is initiated.

[0083] Upon receipt of the authentication request from the user electronic device 102 in the step 802, the authentication server 202 of the payment authentication system 108 validates a combination of the payment card identifier, the mobile number and the secure element identifier of the authentication request. This may be performed by determining if the combination of the payment card identifier, the mobile number and the secure element identifier matches an authentication record of the plurality of authentication records stored in the authentication server database 212. If the combination of the payment card identifier, the mobile number and the secure element identifier is validated in the step 804, a request to provide an authentication value is transmitted by the authentication server 202 of the payment authentication system 108 to the directory server 204 of the payment authentication system 108. In a step 806, in response to the request to provide an authentication value, the directory server 204 of the payment authentication system

generates a network authentication code. As described above, in some embodiments, the authentication request comprises the payment amount and the directory server 204 of the payment authentication system 108 compares the payment amount of the card-not-present payment transaction with a threshold amount. If it is determined that the payment amount is greater than the threshold amount, the card-not-present payment transaction is considered a high-value transaction. In this case, an issuer authentication value is required for authenticating the high-value transaction. The method 400 for authenticating a high-value transaction was described in relation to Figure 4, and the message flow for this method is later described in relation to Fig. 9. If it is determined that the payment amount is less than or equal to the threshold amount, the method for authentication a card-not-present payment transaction continues in the step 806 as described above so that the directory server 204 of the payment authentication system 108 generates a network authentication code.

[0084] Once the network AV is generated in the step 806, the directory server 204 of the payment authentication system 108 stores a combination of the network AV and the payment card identifier. The combination of the network AV and the payment card identifier may be stored in the directory server database 214. In some embodiments, a record of the combination of the network AV and the payment card identifier is communicated to the payment network server 206 of the payment authentication system 108, and stores in the payment network server database 216.

[0085] In a step 810, the directory server 204 of the payment authentication system 108 transmits an authentication response comprising the network AV to the user electronic device 102. The network AV may then be used by the user electronic device 102 for processing the card-not-present payment transaction. In a step 812, the user electronic device 102 uses the received network AV for processing the card-not-present payment transaction and transmits a transaction request to the merchant server 104. The transaction request comprises at least the payment card identifier, and the received network AV. The transaction request may comprise a tokenized payment card identifier instead of the payment card identifier. In a step 814, the merchant server 104 forwards the transaction request to the acquirer server 106, which subsequently forwards the transaction request to the payment network server 206 of the payment authentication system 108 in a step 816. Upon receipt of the transaction request, the payment network server 206 of the payment authentication system 108 determines if the received payment card identifier and the received network AV match the stored payment card identifier and the stored network AV in a step 818. In embodiments where the transaction request comprises a tokenized payment card identifier, the payment network server 208 may communicate with the registration server 208 to retrieve the payment card identifier using

the tokenized payment card identifier. In an embodiment, in order to determine if the received payment card identifier and the received network AV match the stored payment card identifier and the stored network AV, the payment network server 206 is configured to query for the combination of the stored payment card identifier and the stored network AV. In an embodiment where the combination of the stored payment card identifier and the stored network AV is stored in the directory server database 214, the payment network server 206 communicates with the directory server 204 to determine if the stored combination matches the received combination comprised in the transaction request. In an embodiment where a record of the combination of the network AV and the payment card identifier is stored in the payment network server database 216, the payment network server 206 queries the payment network server database 216 to retrieve the record for determining if the received payment card identifier and the received network AV match the stored payment card identifier and the stored network AV.

[0086] If it is determined that the received payment card identifier and the received network AV match the stored payment card identifier and the stored network AV, the payment network server 206 of the payment authentication system 108 generates a network authentication indication. The authentication indication functions to indicate that the card-not-present payment transaction has been authenticated. Therefore, no further authentication may be required to be performed by the issuer server 110. The issuer server 110 may then authorize the card-not-present transaction based on the authentication results provided by the payment authentication system 108. In some embodiments, if the payment card identifier comprises a tokenized payment card identifier for use in processing the e-commerce transaction, the payment network server 108 identifies a payment card identifier (e.g. a payment card number) associated with the tokenized payment card identifier. The payment card number is then transmitted to the issuer server 110 as the payment card identifier for use in authorizing the card-not-present payment transaction. If it is determined that the received payment card identifier and the received network AV do not match the stored payment card identifier and the stored network AV, the payment network server 206 of the payment authentication system 108 is configured to refuse to proceed with the card-not-present payment transaction. In this case, the payment network server 206 of the payment authentication system 108 may be configured to prompt the user electronic device 102 to provide other form of payment for the card-not-present payment transaction.

[0087] Upon receipt of the authorization request from the payment network server 206 of the payment authentication system 108, the issuer server 110 authorizes the card-not-present payment transaction in a step 822. In some embodiments, the issuer server 110 performs other checks on a user account associated with the payment card identifier for authorizing

the card-not-present payment transaction. For example, the issuer server 110 may determine if a balance in the user account associated with the payment card identifier is equal to or more than a payment amount of the card-not-present payment transaction, and authorizes the card-not-present payment transaction if the balance is equal to or more than the payment amount. In a step 824, the issuer server 110 transmits an authorization response to the payment network server 206 of the payment authentication system 108. The authorization response indicates if the card-not-present payment transaction is authorized to proceed. In a step 826, the payment network server 206 of the payment authentication system 108 forwards the authorization response to the acquirer server 106, which is in turn forwarded to the merchant server in a step 828. In a step 830, the merchant server 104 forwards the authorization response to the user electronic device 102.

[0088] 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 payment authentication system 108 has complete control over the authentication process.

[0089] Fig. 9 shows message flows in a method 900 for authenticating a card-not-present payment transaction using the payment authentication system of Fig. 2 in accordance with an embodiment of the present invention. The user is required to be pre-registered with the issuer server 110 prior to using a combination of a payment card identifier, a mobile number and a secure element identifier for authenticating a card-not-present payment transaction. As described above, the method 900 may be performed for embodiments where the card-not-present payment transaction is a high-value transaction. In some embodiments, the method 900 may be performed for all card-not-present payment transactions regardless of a value of the card-not-present payment transaction.

[0090] Similar to that described in relation to Fig. 8, to begin a card-not-present payment transaction, the user initiates a card-not-present payment transaction using the user electronic device 102. In a step 902, the user electronic device 102 transmits an authentication request to the payment authentication system 108. Similar to Fig. 8, although it is shown in Fig. 9 that the authentication request is transmitted to the payment authentication system 108 directly, in some embodiments, the user electronic device 102 transmits the authentication request to the payment authentication system 108 via the merchant server 104 and/or the acquirer server 106. The authentication request comprises a payment card identifier, a mobile number and a secure element identifier associated with the user electronic device. In an embodiment, the authentication request further comprises a payment amount associated with the card-not-present payment transaction. In some embodiments, the authentication request further comprises a currency code and a country

code associated with the card-not-present payment transaction, and a time of initiation of the card-not-present payment transaction. In some embodiments where a tokenized payment card identifier is used, the authentication request comprises the tokenized payment card identifier in place of the payment card identifier and includes a token expiry associated with the tokenized payment card identifier. The payment card identifier, the mobile and/or the secure element identifier may be provided automatically by the user electronic device 102 in the authentication request. To do so, the user device 102 may be configured to retrieve the payment card identifier, the mobile number and/or the secure element identifier and to transmit the payment card identifier, the mobile number and/or the secure element identifier as part of the authentication request when the card-not-present payment transaction is initiated. If the authentication request comprises a tokenized payment card identifier, the authentication server may communicate with the registration server 208 to retrieve a payment card identifier using the tokenized payment card identifier.

[0091] Upon receipt of the authentication request from the user electronic device 102 in the step 902, the authentication server 202 of the payment authentication system 108 forwards the authentication request to the directory server 204 of the payment authentication system 108. The directory server 204 of the payment authentication system 108 then transmits a request to provide an issuer AV to the issuer server in a step 904. The request to provide an issuer AV comprises the payment card identifier, the mobile number and the secure element identifier received in the authentication request. In some embodiments, the authentication server 202 of the payment authentication system 108 validates a combination of the payment card identifier, the mobile number and the secure element identifier received in the authentication request prior to forwarding the authentication request to the directory server 204. In these cases, the authentication server 202 may forward the authentication request to the directory server 204 if it is determined that the combination of the payment card identifier, the mobile number and the secure element identifier matches an authentication record of the plurality of authentication records stored in the authentication server database 212.

[0092] Upon receipt of the request to provide an issuer AV, in a step 906, the issuer server 110 validates the combination of the payment card identifier, the mobile number and the secure element identifier by determining if the combination of the payment card identifier, the mobile number and the secure element identifier matches one of the registration records stored in the issuer server database 114. If the combination is validated in the step 906 by the issuer server 110, the issuer server 110 generates an issuer authentication code. Once the issuer AV is generated in the step 906, the issuer server 110 stores a combination of the issuer AV and the payment card identifier in the issuer server database

114 in a step 910. In a step 912, the issuer server 110 transmits the generated issuer AV to the directory server 204 of the payment authentication system 108. In a step 914, upon receipt of the issuer AV, the directory server 204 of the payment authentication system 108 transmits an authentication response comprising the issuer AV to the user electronic device 102. The issuer AV may then be used by the user electronic device 102 for processing the card-not-present payment transaction.

[0093] In a step 916, the user electronic device 102 uses the received issuer AV for processing the card-not-present payment transaction and transmits a transaction request to the merchant server 104. The transaction request comprises at least the payment card identifier, and the received network AV. In some embodiments, the transaction request comprises a tokenized received payment card identifier instead of the payment card identifier. In a step 918, the merchant server 104 forwards the transaction request to the acquirer server 106, which subsequently forwards the transaction request to the payment network server 206 of the payment authentication system 108 in a step 920. Upon receipt of the transaction request, the payment network server 206 of the payment authentication system 108 transmits an authorization request comprising a received issuer AV and a received payment card identifier to the issuer server 110 in a step 922. If the transaction request comprises a tokenized received payment card identifier, the payment network server 206 may communicate with the registration server 208 to retrieve the received payment card identifier using the received tokenized payment card identifier, before transmitting the received payment card identifier and the received issuer AV to the issuer server 110. In a step 924, the issuer server 110 determines if the received payment card identifier and the received issuer AV match the stored payment card identifier and the stored network AV in the issuer server database 114. If the received payment card identifier and the received issuer AV match the stored payment card identifier and the stored network AV in the issuer server database 114, the issuer server 110 authorizes the card-not-present payment transactions. In some embodiments, the issuer server 110 may perform other checks on a user account associated with the payment card identifier for authorizing the card-not-present payment transaction. For example, the issuer server 110 may determine if a balance in the user account associated with the payment card identifier is equal to or more than a payment amount of the card-not-present payment transaction, and authorizes the card-not-present payment transaction if the balance is equal to or more than the payment amount.

[0094] In a step 926, the issuer server 110 transmits an authorization response to the payment network server 206 of the payment authentication system 108. The authorization response indicates if the card-not-present payment transaction is authorized to proceed. In a step 928, the payment network server 206 of the payment authentication system 108

forwards the authorization response to the acquirer server 106, which is in turn forwarded to the merchant server in a step 930. In a step 932, the merchant server 104 forwards the authorization response to the user electronic device 102.

[0095] As described above, the primary difference between the method 800 and the method 900 is that the method 800 comprises validation of the combination of the payment card identifier, the mobile number and the secure element identifier at the payment authentication system 108 so that a network authentication value is generated by the payment authentication system 108 if the combination of the payment card identifier, the mobile number and the secure element identifier is validated. On the other hand, the method 900 comprises validation of the combination of the payment card identifier, the mobile number and the secure element identifier at the issuer server 110 so that an issuer authentication value is generated by the issuer server 110 if the combination of the payment card identifier, the mobile number and the secure element identifier is validated. In some embodiments, the directory server 204 of the payment authentication system 108 is configured to compare a payment amount of the card-not-present payment transaction with a threshold amount and transmit to the issuer server 110 a request to provide an issuer AV if the payment amount is greater than the threshold amount. In this embodiment, the issuer server 110 remains responsible for authenticating the card-not-present payment transaction if the card-not-present payment transaction is of a high-value (i.e. the payment amount of the card-not-present payment transaction is greater than the threshold amount).

[0096] Fig. 10 shows a computerized network 1000 for authenticating a card-not-present payment transaction using the payment authentication system 108 of Fig. 2 in accordance with an embodiment of the present invention. In particular, Fig. 10 illustrates an example of how the different servers 202, 204, 206 of the payment authentication system 108 may be arranged to form part of the computerized network 1000 in authenticating a card-not-present payment transaction. As shown in Fig. 10, each of the servers 202, 204, 206 may be in communication with its respective database 212, 214, 216.

[0097] Fig. 10 also shows the message flows between the different entities in the computerized network 1000. The reference numbers of the message flows follow from those as described in relation to Figs. 8 and 9 above. For example, as shown in Fig. 10, the steps 802, 902 denote that the user electronic device 102 transmits an authentication request comprising a payment card identifier, a mobile number and a security element identifier as aforementioned described. It follows that in the step 804, the authentication server 202 of the payment authentication system 108 validates a combination of the payment card identifier, the mobile number and the security element identifier using the authentication server database 212. In a step 1002, the authentication server 202

transmits a request to provide an authentication value to the directory server 204 of the payment authentication system 108. In some embodiments (for example, in the embodiment as described in Fig. 8), the step 1002 is performed by the authentication server 202 if the combination of the payment card identifier, the mobile number and the security element identifier is validated.

[0098] In the embodiment as described in Fig. 8, the directory server 204 of the payment authentication system then generates a network authentication code if the combination of the payment card identifier, the mobile number and the security element identifier is validated. The generated network authentication code may be stored either at the directory server database 214 as shown in the step 818, or may be transmitted to the payment network server 206 to be stored in the payment network server database 216 in a step 1004. In some embodiments, for example in the embodiment as described in Fig. 9, the directory server 204 of the payment authentication system 108 transmits a request to provide an issuer AV to the issuer server in the step 904. This may be for a card-not-present payment transaction with a payment amount greater than a threshold amount. In this case, the issuer server 110 validates the combination of the payment card identifier, the mobile number and the secure element identifier by determining if the combination match one of the registration records stored in the issuer database 114 in the step 906. If the combination of the payment card identifier, the mobile number and the secure element identifier is validated, the issuer server 110 generates an issuer AV in the step 908 and stores a combination of the issuer AV and the payment card identifier in the step 910 using the issuer database 114. The issuer server 110 then transmits the issuer AV generated in the step 908 to the directory server 204 of the payment authentication system 108 in the step 912.

[0099] Once the directory server 204 of the payment authentication system 108 is in possession of either the network AV or the issuer AV, the directory server 204 transmits an authentication response comprising either the network AV (in the step 810) or the issuer AV (in the step 914) to the user electronic device 102. Either the network AV or the issuer AV may then be used by the user electronic device 102 for processing the card-not-present payment transaction. To process the card-not-present payment transaction, the user electronic device 102 transmits a transaction request via the merchant server 104 and the acquirer server 106 to the payment network server 206 of the payment authentication system 108, as aforementioned described in relation to the steps 812, 814, 816 or the steps 916, 918, 920. The transaction request comprises either a received network AV or a received issuer AV. The transaction request also comprises the payment card identifier and optionally the payment amount associated with the card-not-present payment transaction.

[00100] In embodiments where the transaction request comprises the received network AV and the payment card identifier, the payment network server 206 determines if the received network AV and the received payment card identifier match the stored received network AV and the received payment card identifier in the step 818. This determination step may be performed by the payment network server 206 either by using the payment network server database 216 if the combination of the network AV and the payment card identifier is transmitted to the payment network server 206 to be stored at the payment network server database 216 in the step 1004 earlier. Otherwise, in some embodiments, the payment network server 206 communicates with the directory server 204 in a step 1006 to determine if the stored combination matches the received combination comprised in the transaction request. If it is determined that the received payment card identifier and the received network AV match the stored payment card identifier and the stored network AV, the payment network server 206 of the payment authentication system 108 generates a network authentication indication for indicating that the card-not-present payment transaction has been authenticated. Therefore, no further authentication may be required to be performed by the issuer server 110. The issuer server 110 may then authorize the card-not-present transaction based on the authentication results provided by the payment authentication system 108 in the step 822 and the payment network server 206 of the payment authentication system 108 receives an authentication response from the issuer server 110 indicating whether the card-not-present payment transaction is authorized to proceed in the step 824.

[00101] In embodiments where the transaction request comprises the received issuer AV and the payment card identifier, the payment network server 206 transmits an authorization request comprising the received issuer AV and the received payment card identifier to the issuer server 110 in the step 922. The issuer server 110 then determines if the received payment card identifier and the received issuer AV match the stored payment card identifier and the stored network AV in the issuer server database 114 in the step 924. If the received payment card identifier and the received issuer AV match the stored payment card identifier and the stored network AV in the issuer server database 114, the issuer server 110 authorizes the card-not-present payment transactions and transmits an authorization response to the payment network server 206 of the payment authentication system 108 in the step 926. The authorization response indicates if the card-not-present payment transaction is authorized to proceed.

[00102] In any one of the embodiments, once the payment network server 206 of the payment authentication system 108 receives the authorization response from the issuer server 110, the payment network server 206 of the payment authentication system 108 forwards the authorization response to the user electronic device 102 via the acquirer

server 106 and the merchant server 104 in the steps 826, 828, 830 or the steps 928, 930, 932. The authorization response may indicate that the card-not-present payment transaction is completed if the card-not-present payment transaction is authorized to proceed.

[00103] Fig. 11 shows message flows in a method 1100 for registering with the payment authentication system 108 of Fig. 2 in accordance with an embodiment of the present invention.

[00104] In a step 1102, the user electronic device 102 transmits a registration request to the registration server 208 of the payment authentication system 108. The registration request comprises a payment card identifier, a mobile number and a secure element identifier. In some embodiments, the registration server 208 tokenizes the payment card identifier received in the registration request in a step 1104. In a step 1106, the registration server 208 of the payment authentication system 108 stores a registration record using the registration server database 218. The registration record comprises the payment card identifier, the mobile number and the secure element identifier received in the step 1102. In some embodiments where the payment card identifier is tokenized, the registration record comprises the tokenized payment card identifier. In a step 1108, the registration server 208 of the payment authentication system 108 transmits the registration record to the issuer server 110 for registering with the issuer server 110. The registration record comprises the payment card identifier, the mobile number and the security element identifier. The registration record transmitted to the issuer server 208 may be stored by the issuer server 110 using the issuer server database 114 for use in authenticating a card-not-present payment transaction in a step 1110. In a step 1112, the registration server 208 of the payment authentication system 108 transmits, to the user electronic device 102, a registration response indicating that the payment card identifier, the mobile number and the secure element identifier have been registered. In some embodiments, the registration response comprises the tokenized payment card identifier if the payment card identifier is tokenized in the step 1106. In some embodiments, the user electronic device 102 transmits transaction authentication data to the authentication server 202 of the payment authentication system 108. The transaction authentication data may include the tokenized payment card identifier and/or the payment card identifier, the mobile number and the secure element identifier. The transaction authentication data may be used to form an authentication record to be stored in the authentication server database 212 of the payment authentication system 108.

[00105] Fig. 12 shows a computerized network 1200 for registering with the payment authentication system 108 of Fig. 2 for authenticating a card-not-present payment

transaction in accordance with an embodiment of the present invention. In particular, Fig. 12 illustrates an example of how the different servers 202, 208 of the payment authentication system 108 may be arranged to form part of the computerized network 1000 in registering a combination of the payment card identifier, the mobile number and the secure element identifier for authenticating a card-not-present payment transaction.

[00106] Fig. 12 also shows the message flows between the different entities in the computerized network 1200. The reference numbers of the message flows follow from those as described in relation to Fig. 11 above, and the description of these steps are therefore not repeated here. A step 1202 as shown in Fig. 12 represents the aforementioned described step where the user electronic device 102 transmits transaction authentication data to the authentication server 202 of the payment authentication system 108. The transaction authentication data may be used to form an authentication record to be stored in the authentication server database 212 of the payment authentication system 108 in a step 1204. The authentication record may comprise the payment card identifier, the mobile number and the secure element identifier.

[00107] Although the aforementioned methods are described to be performed by different servers 202, 204, 206, 208 comprised in the payment authentication system 108, it is appreciated that these different methods may be also be performed by a single server of the payment authentication system 108.

[00108] Fig. 13 is a block diagram showing a technical architecture of the authentication server 202, the directory server 204, the payment network server 206, or the registration server 208 according to an embodiment of the present invention. The technical architecture of the authentication server 202, the directory server 204, the payment network server 206, or the registration server 208 is for performing steps of exemplary methods as described above. In an embodiment, the payment authentication system 108 is formed by a single payment authentication server and the functions performed by the different servers 202, 204, 206, 208 as aforementioned described are performed by different modules in the single payment authentication server. In this case, the payment authentication server may also be represented by the technical architecture as shown in Fig. 13. Typically, the methods are implemented by a number of computers each having a data-processing unit. The block diagram as shown in Figure 13 illustrates a technical architecture of a computer which is suitable for implementing one or more embodiments herein.

[00109] The technical architecture includes a processor 1302 (which may be referred to as a central processor unit or CPU) that is in communication with memory devices including secondary storage 1304 (such as disk drives), read only memory (ROM) 1306,

and random access memory (RAM) 1308. The processor 1302 may be implemented as one or more CPU chips. The technical architecture may further comprise input/output (I/O) devices 1310, and system connectivity or network devices 1312.

[00110] The secondary storage 1304 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 1308 is not large enough to hold all working data. Secondary storage 1304 may be used to store programs which are loaded into RAM 1308 when such programs are selected for execution. Although not shown in Fig. 13, in the embodiment where the aforementioned methods are performed by a single payment authentication server, the secondary storage 1304 has an authentication module, a directory module, a payment network module, and a registration module comprising non-transitory instructions operative by the processor 1302 to perform various operations of the methods of embodiments of the present invention. Although distinct servers 202, 204, 206, 208 are described to perform respective functions implemented by the payment authentication system 108 or different modules are described to performed respective functions in the payment authentication server, it will be appreciated that the boundaries between these servers or modules are exemplary only, and that alternative embodiments may merge servers or modules or impose an alternative decomposition of functionality of servers or 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 servers 202, 204, 206, 208 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 1306 is used to store instructions and perhaps data which are read during program execution. The secondary storage 1304, the ROM 1306, and/or the RAM 1308 may be referred to in some contexts as computer readable storage media and/or non-transitory computer readable media.

[00111] I/O devices 1310 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.

[00112] The system connectivity or network devices 1312 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 1312 may enable the processor 1302 to communicate with the Internet or one or more intranets. With such a system connection, it is contemplated that the processor 1302 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 1302, may be received from and outputted to the system, for example, in the form of a computer data signal embodied in a carrier wave.

[00113] The processor 1302 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 1304), flash drive, ROM 1306, RAM 1308, or the system connectivity or network devices 1312. While only one processor 1302 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.

[00114] 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.

[00115] It is understood that by programming and/or loading executable instructions onto the technical architecture, at least one of the CPU 1302, the ROM 1306, and the RAM 1308 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.

[00116] 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 payment authentication system for authenticating a card-not-present payment transaction initiated using a user electronic device, the payment authentication system comprising:

an authentication server comprising an authentication server processor, an authentication server data storage device and an authentication server database, the authentication server database storing a plurality of authentication records, each authentication record comprising a payment card identifier, a mobile number and a secure element identifier, the authentication server data storage device storing computer program instructions operable to cause the authentication server processor to:

receive, from the user electronic device, an authentication request comprising a payment card identifier, a mobile number and a secure element identifier associated with the user electronic device; and

validate a combination of the payment card identifier, the mobile number and the secure element identifier of the authentication request by determining if the combination of the payment card identifier, the mobile number and the secure element identifier matches an authentication record of the plurality of authentication records;

a directory server comprising a directory server processor and a directory server data storage device, the directory server data storage device storing computer program instructions operable to cause the directory server processor to:

generate a network authentication value (AV) if the combination of the payment card identifier, the mobile number and the secure element identifier has been validated;

store a combination of the network AV and the payment card identifier; and

transmit, to the user electronic device, an authentication response comprising the network AV; and

a payment network server comprising a payment network server processor and a payment network server data storage device, the payment network server data storage device storing computer program instructions operable to cause the payment network server processor to:

receive, from the user electronic device, a transaction request comprising a received payment card identifier and a received network AV;

determine if the received payment card identifier and the received network AV match the stored payment card identifier and the stored network AV; and

transmit, to an issuer server, an authorization request comprising an authentication indication indicating that the card-not-present payment transaction has been authenticated if the received payment card identifier and the received network AV match the stored payment card identifier and the stored network AV.

2. The system of claim 1, wherein the authentication request further comprises a payment amount, the directory server data storage device further stores computer program instructions operable to cause the directory server processor to:

- compare the payment amount with a threshold amount, the card-not-present payment transaction is a high-value transaction if the payment amount is greater than the threshold amount;

- transmit, to the issuer server, a request to provide an issuer AV if the payment amount is greater than the threshold amount, the request comprising the payment card identifier, the mobile number and the secure element identifier;

- receive, from the issuer server, the issuer AV; and

- transmit, to the user electronic device, the issuer AV.

3. The system of claim 2, wherein the payment network server data storage device further stores computer program instructions operable to cause the payment network server processor to:

- receive, from the user electronic device, a high-value transaction request comprising a received issuer AV, a received payment card identifier and an indication of a high-value payment amount;

- transmit, to the issuer server, a high-value authorization request comprising the received issuer AV and the received payment card identifier; and

- receive, from the issuer server, an authorization response indicating whether the card-not-present payment transaction is authorised to proceed, the card-not-present payment transaction is authorised to proceed if the received issuer AV and the received payment card identifier match the stored issuer AV and the stored payment card identifier at the issuer server.

4. The system of any one of claims 1 to 3, wherein the payment card identifier or the received payment card identifier is a tokenized payment card identifier.

5. The system of claim 4, wherein the transaction request or the high-value transaction request further comprises a device-generated cryptogram, the payment network server data storage device further stores computer program instructions operable to cause the payment network server processor to authenticate a combination of the device-generated cryptogram and the tokenized payment card identifier.

6. A payment authentication system for authenticating a card-not-present payment transaction initiated using a user electronic device, the payment authentication system comprising:

- an authentication server comprising an authentication server processor and an authentication server data storage device, the authentication server data storage device storing computer program instructions operable to cause the authentication server processor to:

 - receive, from the user electronic device, an authentication request comprising a payment card identifier, a mobile number and a secure element identifier associated with the user electronic device;

 - a directory server comprising a directory server processor and a directory server data storage device, the directory server data storage device storing computer program instructions operable to cause the directory server processor to:

 - transmit, to an issuer server, a request to provide an issuer AV, the request comprising the payment card identifier, the mobile number and the secure element identifier;

 - receive, from the issuer server, the issuer AV indicating that a combination of the payment card identifier, the mobile number and the secure element identifier matches a stored authentication record comprising the payment card identifier, the mobile number and the secure element identifier; and

 - transmit, to the user electronic device, an authentication response comprising the issuer AV; and

- a payment network server comprising a payment network server processor and a payment network server data storage device, the payment network server data storage device storing computer program instructions operable to cause the payment network server processor to:

 - receive, from the user electronic device, a transaction request comprising a received payment card identifier and a received issuer AV; and

 - transmit, to the issuer server, an authorization request comprising the received payment card identifier and the received issuer AV for authenticating the received payment card identifier and the received issuer AV.

7. The system of claim 6, wherein the authentication server further comprises an authentication server database storing a plurality of authentication records, each authentication record comprising a payment card identifier, a mobile number and a secure element identifier, the authentication server data storage device further stores computer program instructions operable to cause the authentication server processor to:

validate the combination of the payment card identifier, the mobile number and the secure element identifier by determining if the combination of the payment card identifier, the mobile number and the secure element identifier matches an authentication record of the plurality of authentication records,

wherein the request to provide the issuer AV is transmitted to the issuer server if the combination of the payment card identifier, the mobile number and the secure element identifier is validated.

8. The system of claim 6 or claim 7, wherein the payment card identifier or the received payment card identifier is a tokenized payment card identifier and the transaction request further comprises a device-generated cryptogram, the payment network server data storage device further stores computer program instructions operable to cause the payment network server processor to authenticate a combination of the device-generated cryptogram and the tokenized payment card identifier.

9. The system of any one of the preceding claims, further comprising a registration server, the registration server comprises a registration server processor and a registration server data storage device, the registration server data storage device storing computer program instructions operable to cause the registration server processor to:

receive, from the user electronic device, a registration request comprising the payment card identifier, the mobile number and the secure element identifier;

store, using a registration server database, a registration record comprising the payment card identifier, the mobile number and the secure element identifier;

transmit, to the issuer server, the registration record for registering with the issuer server; and

transmit, to the user electronic device, a registration response indicating that the payment card identifier, the mobile number and the secure element identifier have been registered.

10. A payment authentication method for authenticating a card-not-present payment transaction initiated using a user electronic device, the method comprising:

receiving, from the user electronic device, an authentication request comprising a payment card identifier, a mobile number and a secure element identifier associated with the user electronic device;

validating, a combination of the payment card identifier, the mobile number and the secure element identifier of the authentication request by determining if the combination of the payment card identifier, the mobile number and the secure element identifier matches an authentication record, the authentication record being one of a plurality of authentication

records stored in an authentication server database, each of the plurality of authentication records comprising a payment card identifier, a mobile number and a secure element identifier;

generating, a network authentication value (AV) if the combination of the payment card identifier, the mobile number and the secure element identifier has been validated;

storing, a combination of the network AV and the payment card identifier;

transmitting, to the user electronic device, an authentication response comprising the network AV;

receiving, from the user electronic device, a transaction request comprising a received payment card identifier and a received network AV;

determining, if the received payment card identifier and the received network AV match the stored payment card identifier and the stored network AV; and

transmitting, to an issuer server, an authorization request comprising an authentication indication indicating that the card-not-present payment transaction has been authenticated if the received payment card identifier and the received network AV match the stored payment card identifier and the stored network AV.

11. The method of claim 10, wherein the authentication request further comprises a payment amount, the method further comprises:

comparing, the payment amount with a threshold amount, the card-not-present payment transaction is a high-value transaction if the payment amount is greater than the threshold amount;

transmitting, to the issuer server, a request to provide an issuer AV if the payment amount is greater than the threshold amount, the request comprising the payment card identifier, the mobile number and the secure element identifier;

receiving, from the issuer server, the issuer AV; and

transmitting, to the user electronic device, the issuer AV.

12. The method of claim 11, further comprising:

receiving, from the user electronic device, a high-value transaction request comprising a received issuer AV, a received payment card identifier and an indication of a high-value payment amount;

transmitting, to the issuer server, a high-value authorization request comprising the received issuer AV and the received payment card identifier; and

receiving, from the issuer server, an authorization response indicating whether the card-not-present payment transaction is authorised to proceed, the card-not-present payment transaction is authorised to proceed if the received issuer AV and the received

payment card identifier match the stored issuer AV and the stored payment card identifier at the issuer server.

13. The method of any one of claims 10 to 12, wherein the payment card identifier or the received payment card identifier is a tokenized payment card identifier and the transaction request or the high-value transaction request further comprises a device-generated cryptogram, the method further comprises authenticating a combination of the device-generated cryptogram and the tokenized payment card identifier.

14. A payment authentication method for authenticating a card-not-present payment transaction initiated using a user electronic device, the method comprising:

- receiving, from the user electronic device, an authentication request comprising a payment card identifier, a mobile number and a secure element identifier associated with the user electronic device;

- transmitting, to an issuer server, a request to provide an issuer AV, the request comprising the payment card identifier, the mobile number and the secure element identifier;

- receiving, from the issuer server, the issuer AV indicating that a combination of the payment card identifier, the mobile number and the secure element identifier matches a stored authentication record comprising the payment card identifier, the mobile number and the secure element identifier;

- transmitting, to the user electronic device, an authentication response comprising the issuer AV;

- receiving, from the user electronic device, a transaction request comprising a received payment card identifier and a received issuer AV; and

- transmitting, to the issuer server, an authorization request comprising the received payment card identifier and the received issuer AV for authenticating the received payment card identifier and the received issuer AV.

15. The method of claim 14, further comprising:

- validating the combination of the payment card identifier, the mobile number and the secure element identifier by determining if the combination of the payment card identifier, the mobile number and the secure element identifier matches an authentication record, the authentication record being one of a plurality of authentication records stored in an authentication server database, each of the plurality of authentication records comprising a payment card identifier, a mobile number and a secure element identifier,

wherein the request to provide the issuer AV is transmitted to the issuer server if the combination of the payment card identifier, the mobile number and the secure element identifier is validated.

16. The method of claim 14 or claim 15, wherein the payment card identifier or the received payment card identifier is a tokenized payment card identifier and the transaction request further comprises a device-generated cryptogram, the method further comprises authenticating a combination of the device-generated cryptogram and the tokenized payment card identifier.

17. The method of any one of claims 10 to 16, further comprising:

- receiving, from the user electronic device, a registration request comprising the payment card identifier, the mobile number and the secure element identifier;

- storing, using a registration server database, a registration record comprising the payment card identifier, the mobile number and the secure element identifier;

- transmitting, to the issuer server, the registration record for registering with the issuer server; and

- transmitting, to the user electronic device, a registration response indicating that the payment card identifier, the mobile number and the secure element identifier have been registered.

18. The method of claim 17, further comprising:

- tokenizing the payment card identifier; and

- storing the tokenized payment card identifier in the registration record,

- wherein the payment card identifier comprised in the registration response for transmission to the user electronic device is a tokenized payment card identifier.

19. The method of claim 18, further comprising:

- receiving, from the user electronic device, transaction authentication data comprising the tokenized payment card identifier, the mobile number and the secure element 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 10 to 19.