(12) UK Patent Application (19) GB (11) 2533333 (13) A

(43) Date of A Publication 22.06.2016

(21) Application No: 1422395.2

(22) Date of Filing: 16.12.2014

(71) Applicant(s):
Visa Europe Limited
(Incorporated in the United Kingdom)
1 Sheldon Square, LONDON, W2 6TT, United Kingdom

(72) Inventor(s):
Nicolas David Mackie

(74) Agent and/or Address for Service:
EIP
Fairfax House, 15 Fulwood Place, LONDON,
WC1V 6HU, United Kingdom

(51) INT CL:
G06Q 20/40 (2012.01) ***G06Q 20/32*** (2012.01)
G06Q 20/34 (2012.01)

(56) Documents Cited:
None

(58) Field of Search:
Other: **No search performed: Section 17(5)(b)**

(54) Title of the Invention: **Transaction authorisation**
Abstract Title: **Authorising contactless payment transactions made at point of sales**

(57) The present invention relates to systems and methods for authorising electronic payment transactions, and in particular, but not exclusively to authorising contactless payment transactions made at point of sales using a payment device 100. A server system receives, from a first computing device, verification information relating to a verification process for verifying a user associated with the first computing device. A verification status associated with the user is set in a memory of the server system, based on the verification information. The server system receives an authorisation request for a payment transaction from a payment terminal, the request including an identifier associated with the user, and having been provided to the payment terminal by a payment device different from the first computing device. Responsive to receipt of the authorisation request, the verification status associated with the user is identified, and a determination as to whether to authorise the paymenttransaction is made at least partly on the basis of the identified verification status.

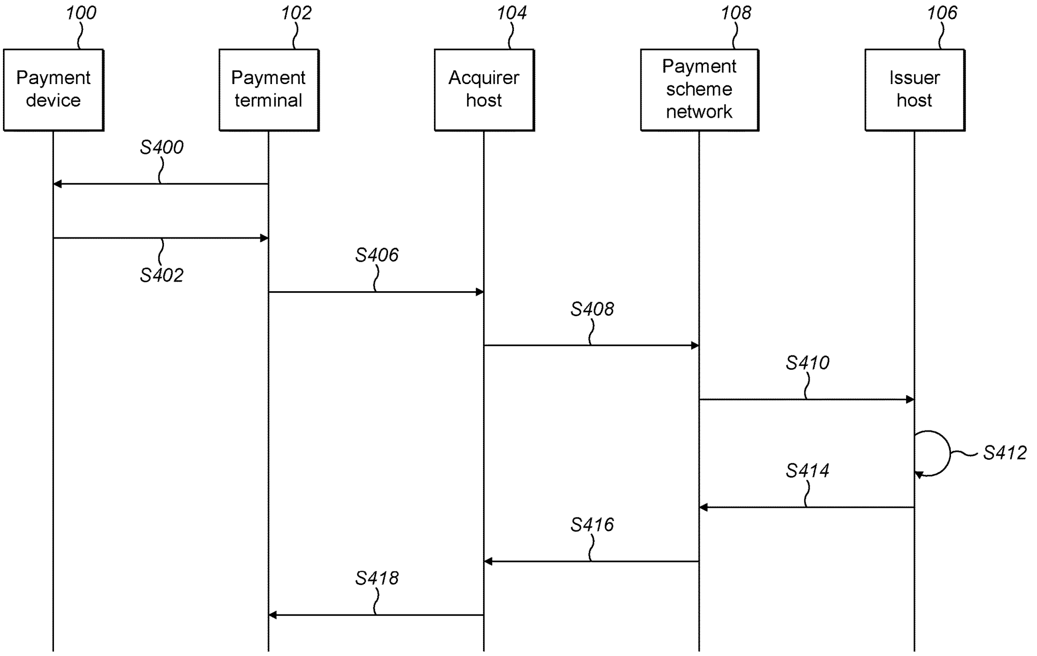


FIG. 4

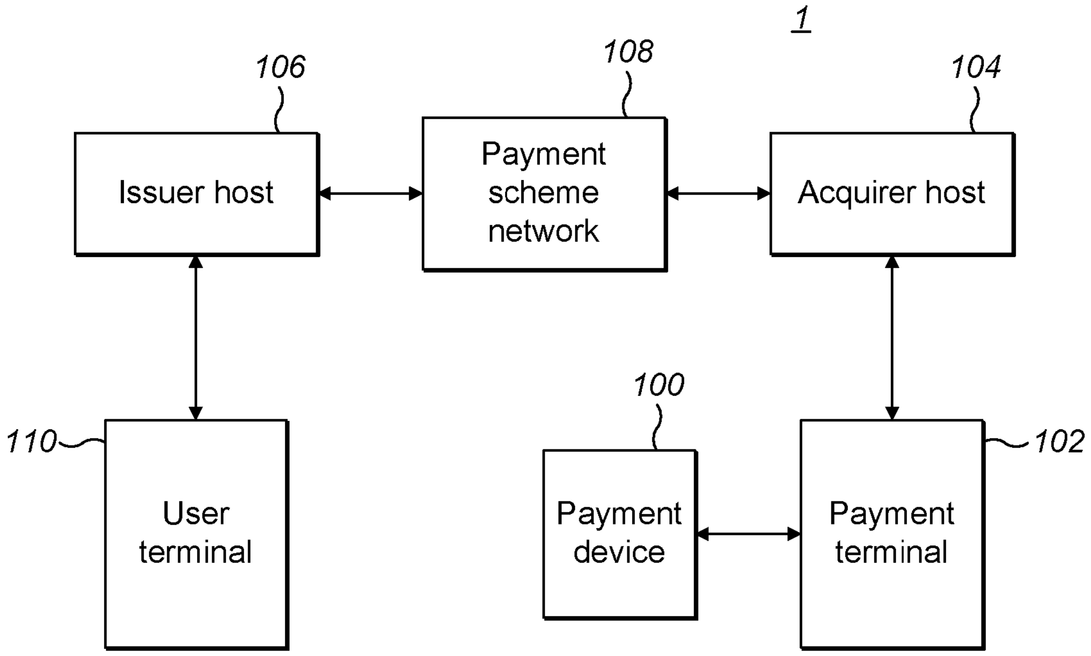

1
106
Issuer host
108
Payment scheme network
104
Acquirer host
110
User terminal
100
Payment device
102
Payment terminal

FIG. 1

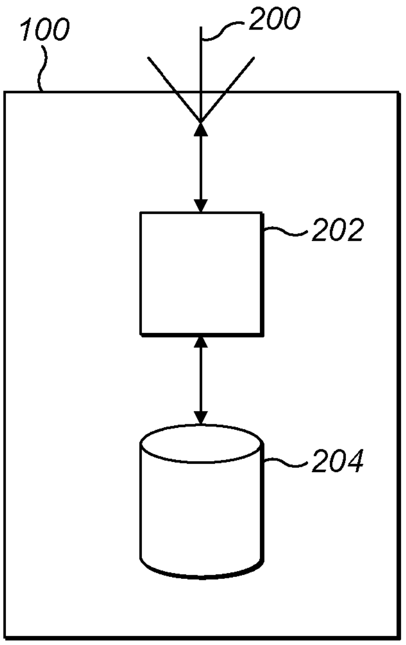


FIG. 2a

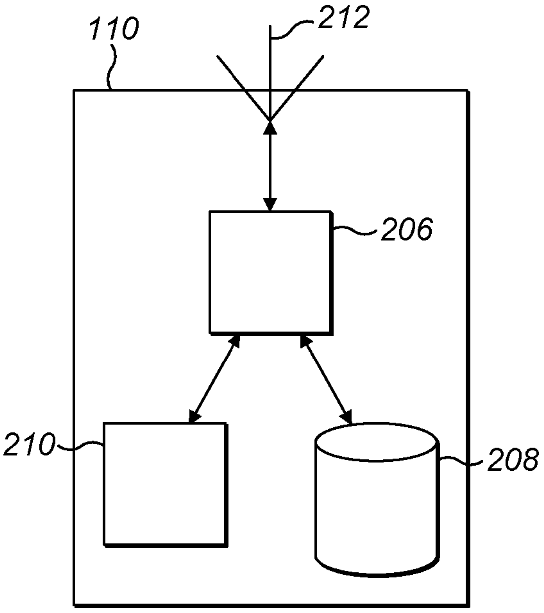


FIG. 2b

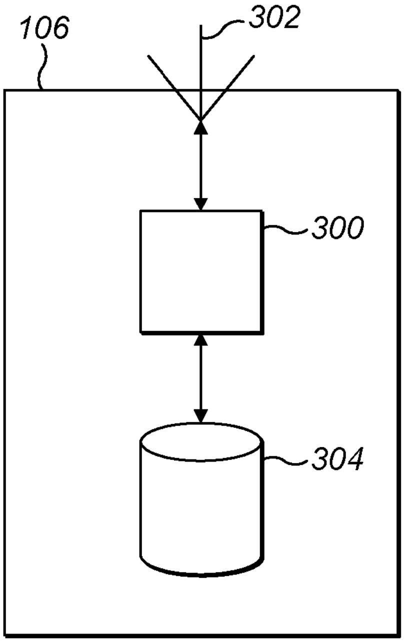
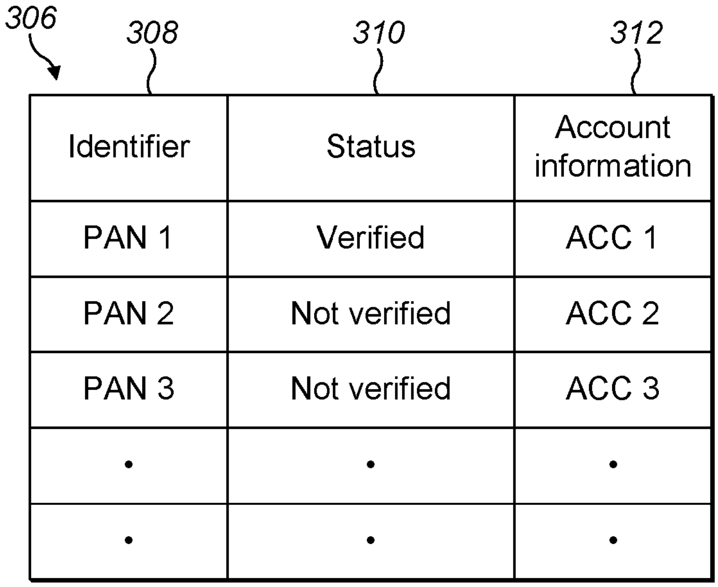


FIG. 3a


306
308
310
312

Identifier	Status	Account information
PAN 1	Verified	ACC 1
PAN 2	Not verified	ACC 2
PAN 3	Not verified	ACC 3
•	•	•
•	•	•

FIG. 3b

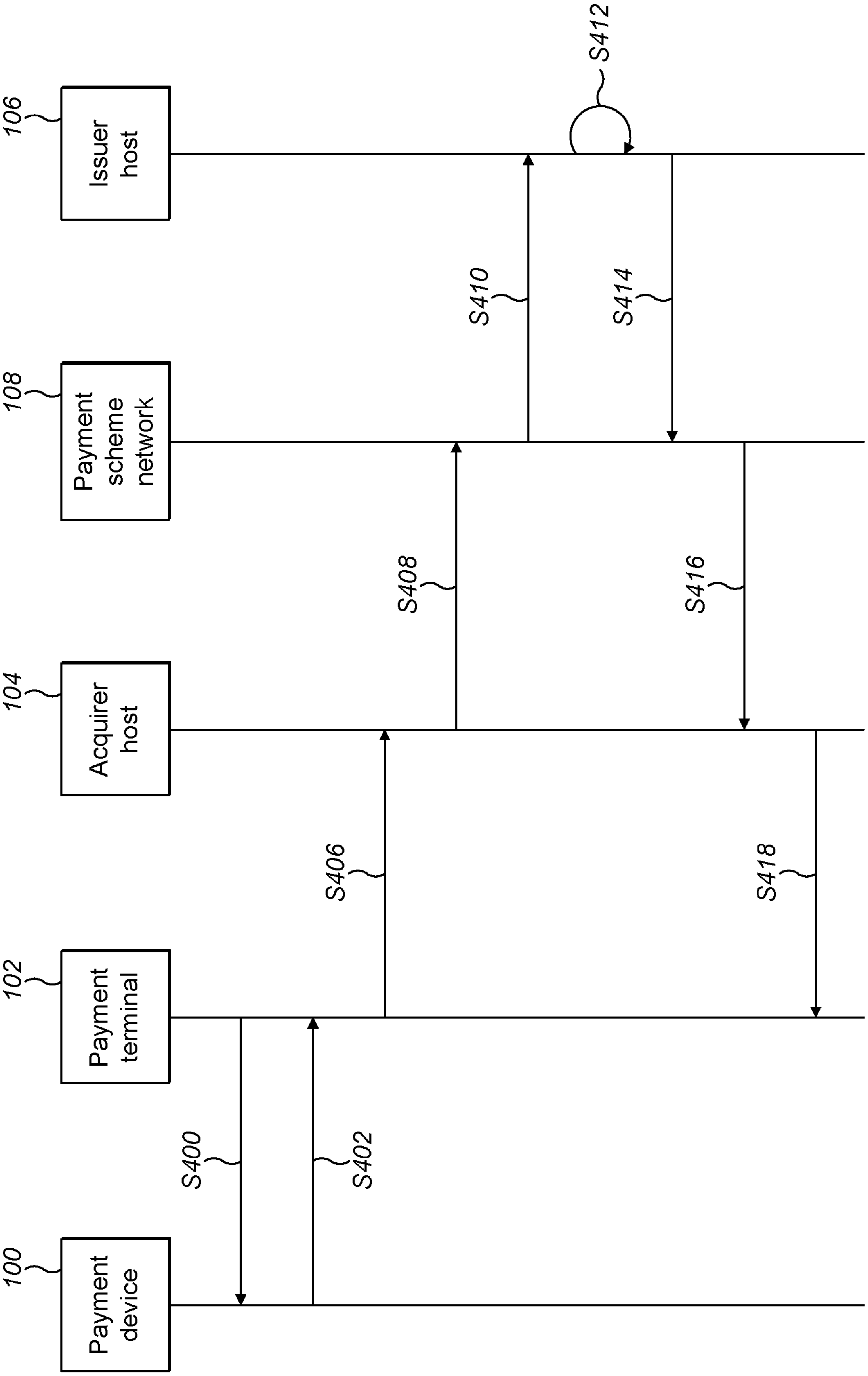

100
Payment device
102
Payment terminal
104
Acquirer host
108
Payment scheme network
106
Issuer host
S400
S402
S406
S408
S410
S412
S414
S416
S418

FIG. 4

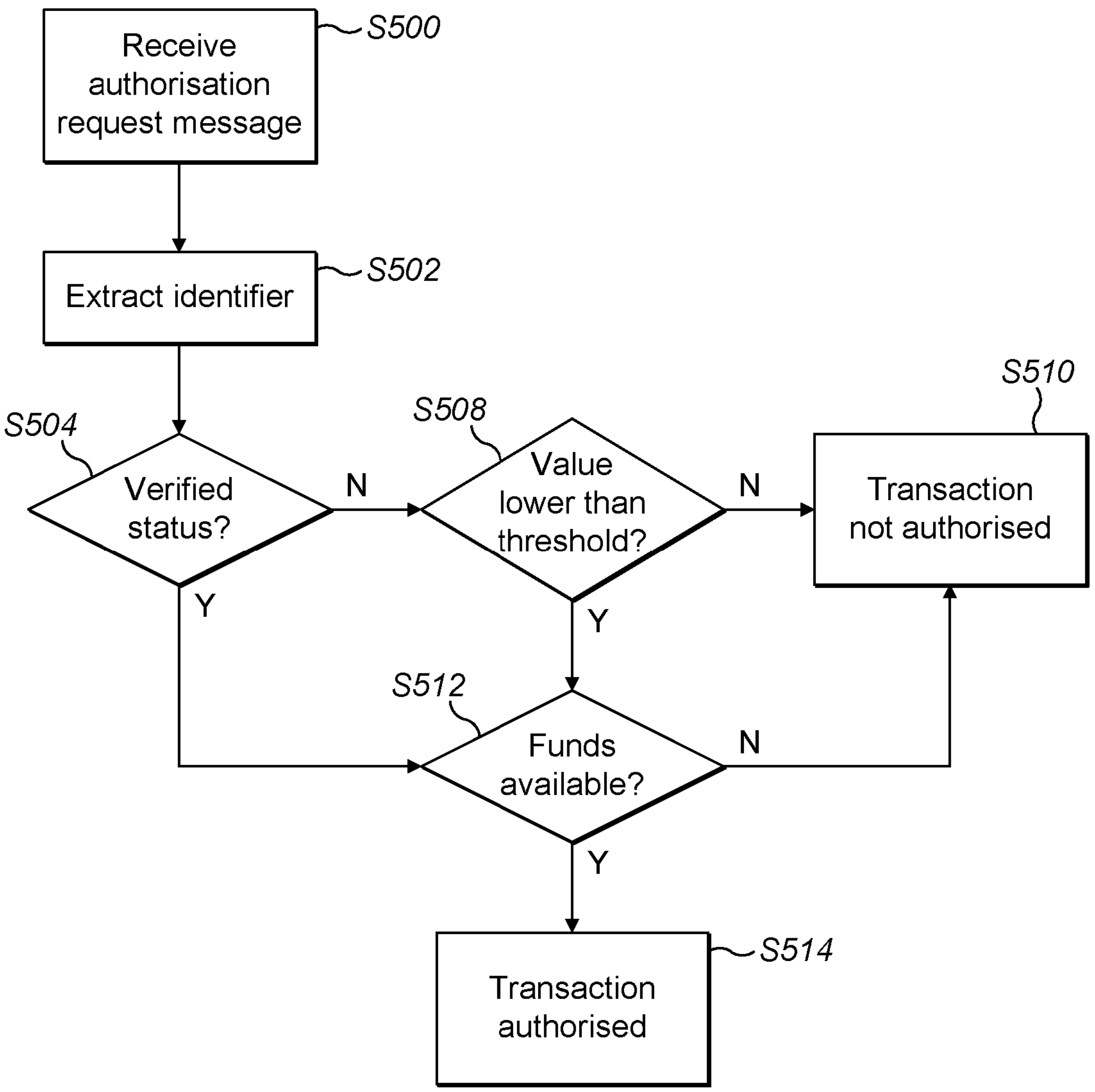

Receive authorisation request message
S500
Extract identifier
S502
S504
Verified status?
N
Y
S508
Value lower than threshold?
N
Y
S510
Transaction not authorised
S512
Funds available?
N
Y
Transaction authorised
S514

FIG. 5

Transaction Authorisation

Field of the Invention

The present invention relates to systems and methods for authorising electronic payment transactions, and in particular, but not exclusively to authorising contactless payment transactions made at a point of sales using a payment device.

Background

A variety of methods for effecting payment transactions without the use of cash exist. For example, payment may be effected using a financial instrument such as a payment card by interacting with an electronic payment terminal, which may be located at a Point of Sales (POS) within an establishment such as a retail establishment or restaurant. The financial instrument may include a magnetic stripe containing information such as data relating to the account holder and an account from where the funds for the transaction may be drawn. The magnetic card is typically swiped through a magnetic card reader which reads data necessary for enacting the transaction. In another example, some financial instruments are embedded with a semiconductor device (a “chip”) storing the above information; an interface is provided on the card for interacting with a card reader, which may take the form of physical pads.

Transactions using financial instruments may involve verification (authentication) of the user by the user providing a signature. Alternatively, the user may be required to input a Personal Identification Number (PIN) on the terminal when prompted, which is sent to a server, in encrypted form, for verification; this is often referred to as online PIN verification. In the case of a financial instrument including a chip as described above, the chip may include a secure memory storing the PIN data. In this case, the user enters a PIN on the terminal when prompted, which is compared with the PIN stored in the card; this is often referred to as offline PIN verification.

Each of the above methods can be time consuming and inconvenient for the user. Payment transaction methods which do not involve verification of the user have also been developed. For example, a so-called contactless payment transaction method may be used. A contactless payment device is provided with an antenna which enables it to interact with a contactless payment terminal when held in close proximity to same, to provide the information necessary to enact a payment transaction as described above.

Such payment transactions often do not require the user to perform a verification process, such as the provision of a signature or a PIN as described above. This enables the payment transactions to be performed quickly and easily, but also involves a lower level of security of the transactions. One countermeasure against fraud that has been implemented is to impose a limit on the value of transactions that may be enacted using contactless payment methods without user verification in all countries which operate such methods. For transactions above this limit, it may be necessary for the user to provide a PIN, for example where the infrastructure for online PIN verification exists, or the user may be required to use a different payment method, such as 'Chip & PIN'. This means that the convenience of contactless payment transactions is reduced.

Summary of the Invention

In accordance with at least one embodiment, methods, devices, systems and software are provided for supporting or implementing functionality to authorise a payment transaction.

This is achieved by a combination of features recited in each independent claim. Accordingly, dependent claims prescribe further detailed implementations of various embodiments.

In accordance with a first aspect, there is provided a method of authorising a payment transaction, the method comprising: receiving, at a server system, from a first computing device, verification information relating to a verification process for verifying a user associated with the first computing device; setting a verification status associated with the user in a memory of the server system, based on the verification information; receiving, at the server system, an authorisation request to authorise a payment transaction, the authorisation request being received from a payment terminal and including an identifier associated with the user, the information having been provided to the payment terminal by a payment device, the payment device being different from the first computing device; responsive to receipt of the authorisation request, identifying the verification status associated with the user based on the identifier; and determining whether to authorise the payment transaction at least partly on the basis of the identified verification status.

The method may comprise: setting the verification status to indicate a verified status on the basis of the verification information; and setting the verification status to indicate a non-verified status in response to one or more predetermined conditions being satisfied.

The one or more predetermined conditions may comprise one or more of: a predetermined time period having elapsed; a predetermined number of transaction requests having been received; and a predefined transaction total being reached.

The payment transaction may comprise a contactless payment transaction, the payment terminal may comprises a contactless payment terminal and the payment device may comprise a contactless payment device. The contactless payment device comprises a fob or tag device.

In some embodiments, the payment transaction does not comprise a verification process to verify the user.

The method may comprise sending a message indicating whether the payment transaction is authorised to the payment terminal in response to said determination.

The determination may be performed partly on the basis of a comparison of a value of the transaction with a predetermined threshold value.

The verification information may comprise an indication that the user has been verified.

Alternatively, the verification information may comprise information input to the first computing device by the user, and the method comprises performing said verification process at the server system on the basis of thereof.

The verification information may comprise receiving the verification information in a Short Message Service (SMS) message. The verification information may be received from a software application held on the first computing device.

In accordance with a second aspect, there is provided a computer program for authorising a payment transaction, the computer program comprising instructions for a server system to perform a method of authorising a payment transaction, the method comprising: receiving, at a server system, from a first computing device, verification information relating to a verification process for verifying a user associated with the first computing device; setting a verification status associated with the user in a memory of the server system, based on the verification information; receiving, at the server system, an authorisation request to authorise a payment transaction, the authorisation request being received from a payment terminal and including an identifier associated with the user, the information having been provided to the payment terminal by a payment device, the payment device being different from the first computing device; responsive to receipt of the authorisation request, identifying the verification status associated with the user based on the identifier; and determining whether to authorise the payment transaction at least partly on the basis of the identified verification status.

The second aspect may include one or features corresponding to one or more of the features described above in relation to the first aspect.

In accordance with a third aspect, there is provided apparatus for authorising a contactless payment transaction, the apparatus being arranged to: receive from a first computing device, verification information relating to a verification process for verifying a user associated with the first computing device; set a verification status associated with the user in a memory, based on the verification information; receive an authorisation request to authorise a payment transaction, the authorisation request being received from a payment terminal and including an identifier associated with the user, the information having been provided to the payment terminal by a payment device, the payment device being different from the first computing device; responsive to receipt of the authorisation request, identify the verification status associated with the user based on the identifier; and determine whether to authorise the payment transaction at least partly on the basis of the identified verification status.

The third aspect may include one or features corresponding to one or more of the features described above in relation to the first aspect.

Further features and advantages will become apparent from the following description of preferred embodiments, given by way of example only, which is made with reference to the accompanying drawings.

Brief Description of the Drawings

Figure 1 shows a schematic diagram of a payment transaction system in which embodiments of the invention may be practised;

Figure 2a schematically illustrates a payment device for use in an embodiment;

Figure 2b schematically illustrates a payment terminal for use in an embodiment;

Figure 3a schematically illustrates a server system according to an embodiment;

Figure 3b schematically illustrates a look-up table for use in an embodiment;

Figure 4 is a message flow diagram illustrating a message flow according to an embodiment; and

Figure 5 shows a process flow of a verification process performed by a server system according to an embodiment.

Detailed Description of Illustrative Embodiments

Figure 1 illustrates a transaction system 1 in which embodiments may be implemented. The system includes a contactless payment device 100 and a contactless payment terminal 102, which may be used to initiate a contactless payment transaction as described below. The contactless payment terminal 102 may be located at a Point of Sales (POS), such as a business premises, for example a shop, restaurant, cinema, station or other location, and be arranged to process payment transactions on behalf of the business or other entity associated with the POS.

The contactless payment terminal 102 is able to maintain or establish a data connection with an acquirer host 104 which typically takes the form of a server system of one or more computing devices for processing transactions associated with a financial institution, such as a bank, which manages one or more financial accounts of the entity associated with the POS.

An issuer host 106 is a server system of one or more computing devices arranged to process transactions associated with a financial institution, such as a bank, which manages one or more financial accounts of a user of the payment device 100.

Each of the acquirer host 104 and the issuer host 106 is capable of communicating with a payment scheme network 108. The payment scheme network 108 is a server system of computing devices which may be associated with a financial services organisation, for example.

The system 1 also includes a user terminal 110 associated with the user. The user terminal 110 is arranged to participate in a user verification process, as described below.

While the system 1 in Figure 1 shows only one contactless payment terminal 102, it will be appreciated that any given acquirer host 104 will typically be arranged to communicate with many different contactless payment terminals 102, directly or indirectly. Similarly, the issuer host 106 is typically arranged to communicate with multiple acquirer hosts 104 via multiple payment scheme networks 106, and each payment scheme network will typically be arranged to communicate with many different issuer hosts 106. Further, each contactless payment terminal 102 may communicate with multiple contactless payment devices 100 associated with different users, which each use a different user terminal 110 in verification processes as described herein.

Communications between the different entities shown in Figure 1 may take place using one or more of various different communications protocols and methods, including communications via wireless and/or wired communications methods and including the Internet.

Figure 2a illustrates a contactless payment device 100 for use in embodiments. The contactless payment device 100 may take the form of a fob, a tag, a financial instrument such as payment card, or another device such as a smart watch. The contactless payment device 100 includes a communications interface 200, which may comprise an antenna, for wirelessly communicating with a contactless payment terminal using a short range communications technology, for example a radio frequency technology, such as a near field communications (NFC) technology, or an infra-red or other optical communications technology.

The contactless payment device 100 also includes a processing device 202 such as a semiconductor chip and a memory 204. The memory 204 is arranged to store data associated with the user, such as an identifier associated with the user; this identifier may be an identifier of a financial account of the user, such as a primary account number (PAN). The memory 204 may also store other data relating to the financial account to which the PAN relates, such as an expiry date, issue number and/or other data. The memory 204 may also store an indicator indicating that a verification method in accordance with an embodiment is to be used. The stored data may be suitable for use in an EMV transaction.

The contactless payment device 100 is arranged to interact with the contactless transaction terminal 102 to provide some or all of this data via the communications interface 200 and corresponding communications interface (not shown) in the payment terminal 102, when brought into sufficiently close contact with the contactless transaction terminal 102.

In some embodiments, the contactless payment device 100 does not include a user input device, such as a keypad or the like, or any other means of participating in a user verification process. This may be the case where the contactless payment device 100 is a fob or card or the like. This enables the contactless payment device 100 to be of small dimensions and/or low weight, improving the convenience for the user.

Figure 2b illustrates a user terminal 110 for use in embodiments. The user terminal 110 comprises a computing device such as a personal computer, for example a lap top or desk top computer, or a mobile device such as tablet computer or smartphone. In the embodiment illustrated in Figure 2b the computing device 110 includes one or more processors 206, a memory 208, a user input device 210 and a communications interface 212. The memory 208 may hold a software application or applet including instructions readable by the processor 206 to perform a verification process as described below. The user input 210 device may comprise one or more of a keypad, a touchscreen, a mouse pad and a biometric sensor such as a fingerprint reader. Although not shown, the user terminal 110 typically includes other components such as a display screen.

Figure 3a illustrates an issuer host 106 for use in embodiments. The illustrated issuer host 106 includes one or more processors 300, a communications interface 302 and a memory 304 which holds software including instructions executable for performing processes for authorising a payment transaction as described herein.

The memory 302 may also store data indicating an authorisation status associated with different users. Figure 3b shows an example in the form of a table 306. The table includes a set of identifier entries 308, a corresponding set of status entries 310 and a corresponding set of account information entries 312. The identifier entries 308 may comprise a PAN, or other identifier associated with a financial account. The status entries 310 each include an indicator of a verification status of a user associated with the financial account (e.g. the owner of the account). The indicators may take the form of a flag field, for example. The account information entries 312 include information relating to the financial account associated with the corresponding identifier. This may include an indication of an account balance associated with the financial account, for example.

The issuer host 106 sets the verification status of users indicated in the status field 310, for the accounts or account ranges operating in this mode, based on verification information received from the user terminal 110. For example, the user terminal 110 comprises a user input device 210; this user input device 210 may be used to receive input from the user to perform a verification process. For example, as described above, the memory 208 of the user terminal 110 may store software for performing a process to verify the user, or the user terminal 110 may connect to the issuer host 106 to perform a user verification. For example, when the user wishes to be able to perform contactless payment transactions using the contactless payment device 100, he or she may start up the software in order to perform the verification process. The verification process may be initiated by selection of an option in the software, for example. Once the application has been executed, the user provides information via the user input device 210 in order to verify themselves. The provided information may be for example user credentials such as a username and/or password or passcode, or may take some other form, for example, biometric data such as a fingerprint provided via a fingerprint reader for example.

Once the user input has been received at the user terminal 110 via the user input device 210, the user terminal 110 may itself verify the user by, for example, comparing received user credentials or biometric data with registered data stored in the memory 208. If the user is verified, then the user terminal 110 sends a verification message to the issuer host 106 indicating that the user is verified. The verification message may be protected using a cryptographic mechanism, for example. The verification message may include an identifier associated with the user, such as a PAN; this identifier may be stored in the memory 208 of the user terminal 110, for example. Alternatively or additionally, the verification message may include another identifier, such as a username, on the basis of which the issuer host 106 identifies the user and associated financial account etc, or an identifier of the user terminal 110. Once the issuer host 106 has received the verification message and identified the corresponding entry in the table 306, it sets the appropriate status entry to indicate a verified status.

Alternatively, the verification of the user may be performed by the issuer host 106. In this case, the information received from the user via the user input device 206 is sent to the issuer host 106, and the issuer host 106 performs the verification based on this received information by, for example, comparing it with information stored in the memory 304. If it determines that the user is verified, it set the corresponding status entry to indicate a verified status, as above.

Various other methods of verification may be used. For example, a verification message may be sent in response to a user unlocking the user terminal 110. In another example, a user may send a message such as a Short Message Service (SMS) message to the issuer host 106 via a telephony network including information such as a predetermined alphanumeric code, for verification by the issuer host 106.

Further, the verification process may be based, at least in part, on whether or not the contactless payment device 100 is proximate to the user terminal 110 (for example, whether it is within a certain predefined range). For example, a verification process as described above may only be enabled in the case that the user terminal 110 determines that the contactless payment device 102 is in its proximity. In another example, the user terminal 110 may base verification of the user on the proximity or otherwise of the contactless payment device 100, and send a verification message as described above in response to determining that the contactless payment device 100 is proximate. This may be done periodically, in order to maintain a verified status of the user.

The proximity of the contactless payment device 100 may be detected by, for example, a connection between the contactless payment device 100 and the user terminal 110 provided by technology such as Bluetooth^{TM} or Bluetooth Low Energy^{TM} (Bluetooth LE^{TM}). For example, if a signal from the contactless payment device 100 is detected, it may be determined that it is proximate (e.g. in range). In another example, the issuer host 106 may determine whether the devices are proximate based on GPS coordinates of the user terminal 110 and payment device 100. The GPS coordinates of the payment device 100 could be provided as part of the transaction data, and the GPS coordinates of the user terminal 110 could be provided as part of the verification process, for example.

Once the verification status for a given user has been set to indicate a verified status, the issuer host 106 may be triggered to set the status to indicate a unauthorised status in response to, for example, a predetermined time period elapsing, a number of transactions being authorised, transactions totalling a predetermined value having been authorised, or some combination of these. The conditions which trigger the setting of an unauthorised status may be set by the user, via the application on the user terminal 110 for example.

These features improve security by ensuring that in the event that the contactless payment device 100 is lost or stolen, there is a limit on the extent that it can be used for transactions by a third party, while providing flexibility for the user to set the conditions such that he or she is not required to perform a verification process for each individual transaction, for example.

Figure 4 shows message flows in authorising a contactless payment transaction in accordance with an embodiment. Typically, the contactless payment terminal 102 is configured to initiate a payment by a vendor. For example, the vendor may manually enter a transaction amount into the contactless payment terminal 102, or the value of goods and/or services due for payment may be determined by some other means, such as by a barcode reader reading barcodes provided on products for purchase, for example. In order to initiate a contactless payment transaction, it may be necessary to select a particular option on the contactless payment terminal 102, the contactless payment terminal 102 may be configured only to accept contactless payments or it may be configured to automatically enact a contactless payment transaction on detection of an appropriate contactless payment device 100.

Once the contactless payment terminal 102 has been appropriately configured, the user (e.g. customer at a retail establishment) brings the contactless payment device 100 into proximity with the contactless payment terminal 102. This results, for example, in the contactless payment terminal 102 sending, at step S400, a request to the contactless payment device 100 to provide data for enacting the payment transaction. In response, the payment transaction device 100 retrieves data from the memory 204 and sends same to the contactless payment terminal 102 at step S402. The provided data may include data identifying a payment account from which funds are to be drawn in the payment transaction, such as a PAN and an identifier of the issuer associated with the contactless payment device 100. The response may also include a verification method identifier that a verification method in accordance with embodiments is to be used. This identifier may be included in a data field of the response, such as a data field used for identifying a verification method to be used in a transaction or to indicate that the user has been verified. This field, which may be referred to as a cardholder verification method (CVM) field, may be a field such as the Card Transaction Qualifiers (CTQ) field in an EMV-compliant message indicating a type of verification method to be used in the transaction; depending on the value in the

CVM field, the user may be required to, for example, enter a PIN or provide a signature. Alternatively, the CVM field (e.g. CTQ field) may indicate that cardholder verification has already been performed on the contactless payment device 100.

The response message sent by the contactless payment device 100 at step S402 may be in protected form. For example, it may comprise a cryptogram, for example an EMV compliant Authorisation ReQuest Cryptogram (ARQC).

On receipt of the response message, the contactless payment terminal 102 determines, based on, for example, the presence of an ARQC that it is to obtain authorisation information from the issuer host 106. The contactless payment terminal 102 then sends an authorisation request message to acquirer host 104 at step S406, the message including the information received from the contactless payment device 100 at step S402. The message may also include a transaction identifier to identify the transaction, the identifier being included in the message by the contactless payment terminal 102. The message may also include other data added by the contactless payment terminal 102, such as a value of the transaction.

On receipt of the message, the acquirer host 104 forwards same to the payment scheme network at step S408. In the present embodiment, the payment scheme network 108 routes the message to the issuer host 106 (for example, based on an indicator of the issuer included in the message) at step S410.

The issuer host 106 receives the authorisation request message, cryptographically verifying same where appropriate, and performs a determination process to determine whether to authorise the contactless payment transaction at step S412. The determination is based, at least in part, on information received in the message received at step S410. This process is described in detail below with reference to Figure 5.

At step S414 the issuer host 106 returns a result of the determination to the payment scheme network 108 in a message sent at step S414. The message includes an indicator as to whether or not the transaction is authorised. It may also include a transaction identifier the same as or corresponding to the transaction identifier provided by the contactless payment terminal 102 as described above.

The message sent by the issuer host 106 is routed to the contactless payment terminal 102 via the payment scheme network 108 and acquirer hosts 104 at steps S416 and S418. On receipt of the message, the payment terminal 102 identifies the result of the verification based on the content of the message, and may indicate same, for example on a display screen of the contactless payment terminal 102. If the contactless payment transaction is not authorised, the user may be presented with further options for completing the transaction. Additionally or alternatively, if the contactless payment transaction is not authorised, the issuer host 106 may send a message, such as a push notification to the user terminal 110 to prompt the user to perform a verification process as described above in order that the transaction may be authorised.

An exemplary process by which the issuer host 106 determines whether to authorise the contactless payment transaction is now described with reference to Figure 5.

At step S500 the issuer host 106 receives the authorisation request message received from the contactless payment terminal 102, as described above. At Step S502 the issuer host extracts the identifier (e.g. PAN) included in the request message. At step S504, the issuer host compares the extracted identifier with those included in the identifier field 308 of the table 306. If no matching or corresponding identifier is found, an error message may be sent to the contactless payment terminal 102.

If a matching or corresponding identifier is found, at step S504 determines a verification status associated with the user by reading the entry in the status field 310 of the table 306 corresponding to the matching or corresponding identifier. If the entry indicates that the user is verified, the process proceeds to step S512 where the issuer host performs further checks to determine whether or not to authorise the transaction. As shown, this may involve determining whether sufficient funds are available for the transaction, for example by retrieving data from the account information field 312 of the table 306. The further checks may additionally or alternatively comprise checking other information associated with the account, such as an expiry date associated with the contactless payment device, for example.

If, based on the further checks performed at step S512, the issuer host 106 determines that the transaction is authorised (for example, sufficient funds are available), the issuer host authorises the transaction at step S514 and sends an authorisation message as described above in relation to step S414 and subsequent steps. If, based on the further checks performed at step S512, the issuer host 106 determines that the transaction is not authorised, the issuer host 106 sends a non-authorisation message as described above in relation to step S414 and subsequent steps.

Returning to step S504, if the issuer host 106 determines that the verification status is not-verified, the process proceeds to step S508. At step S508, the issuer host 106 determines a value of the transaction, for example based on information included in the authorisation request message received at step S500, and determines whether the determined value is lower than a threshold value. If it is determined that the value is not lower than the threshold value, process proceeds to step S510 where the issuer host 106 determines that the transaction is not authorised, as described above.

On the other hand, if the value of the transaction is lower than the threshold value, the process proceeds to step S512, where the further checks described above are performed.

It should be noted that the order of the steps described above in relation to Figure 5 may be varied and/or some steps may be omitted. For example, the step of comparing the value of the transaction with a threshold value as described above at step S508 provides the advantage that transactions below a predetermined value may be authorised, without requiring the user to verify themselves as described above. However, in some cases this comparison may be omitted. In still other cases, the comparison may be performed prior to the determination of verification status at step S504, with the determination of verification status only being performed in the case that it is determined that the transaction value is not lower than the threshold value.

Similarly, the further checks described above in relation to step S512 may be omitted, or performed prior to the determination of verification status, for example.

Although many of the processes described above were described as being performed by the issuer host 106, in some embodiments, part or all of the process is performed by one or more other entities. For example, the payment scheme network 104 may store table 306 and perform the user verification process described above. In this case, the determination of verification status described above may be performed by the payment scheme network 104 in response to receiving the verification request message at step S408 above; the payment scheme network may also perform the comparison with a threshold value described above in relation to step S508. The payment scheme network 104 may then add an indication that the transaction is validated into the authorisation request message, which it then sends to the issuer host 106, which may then perform the further checks described above in relation to step S512, for example.

Although the above systems and methods have been described in the context of contactless payment transactions, other types of payment transactions may be used. For example, the above payment authorisation methods may be used for payments in which a financial instrument such as a debit or credit card is brought into contact with a payment terminal, for example by swiping a magnetic strip on the card on a reader of the payment terminal or inserting a card including a chip into a reader on the payment terminal.

The systems and methods above provide a convenient and secure way of authorising payment transactions. Because the verification status of the user is stored in a memory of the entity authorising the transaction, the user is relieved from the burden of having to verify themselves at the time of making the transaction, without compromising the security of the transaction. Further, secure transactions are enabled even in the case that the payment device 100 does not include an input means, or any facility for verifying the user.

The various memories described above may take the form of any suitable date store, including Random Access Memory (RAM) and/or Read Only Memory (ROM) data stores. The various processors may take the form of a semiconductor chip, such as a Central Processing Unit (CPU) for example.

The above embodiments are to be understood as illustrative examples of the invention. Further embodiments of the invention are envisaged. For example, although in the above example, the contactless payment device 100 provided an indicator for the contactless payment terminal 102 to request authorisation from the issuer host 106 and/or payment scheme network 108, in some cases this may not be necessary. For example, the payment terminal may be arranged to request verification from the issuer host 106 and/or payment scheme network 108 for all transactions, without requiring an indicator of a verification method to be used.

Further, the software application or applet held on the user terminal 110 may include other features not described above. For example, it may provide access to account information of the financial account associated with the user.

It is to be understood that any feature described in relation to any one embodiment may be used alone, or in combination with other features described, and may also be used in combination with one or more features of any other of the embodiments, or any combination of any other of the embodiments. Furthermore, equivalents and modifications not described above may also be employed without departing from the scope of the invention, which is defined in the accompanying claims. The features of the claims may be combined in combinations other than those specified in the claims.

Claims

1. A method of authorising a payment transaction, the method comprising:

receiving, at a server system, from a first computing device, verification information relating to a verification process for verifying a user associated with the first computing device;

setting a verification status associated with the user in a memory of the server system, based on the verification information;

receiving, at the server system, an authorisation request to authorise a payment transaction, the authorisation request being received from a payment terminal and including an identifier associated with the user, the information having been provided to the payment terminal by a payment device, the payment device being different from the first computing device;

responsive to receipt of the authorisation request, identifying the verification status associated with the user based on the identifier; and

determining whether to authorise the payment transaction at least partly on the basis of the identified verification status.

2. A method according to claim 1, comprising:

setting the verification status to indicate a verified status on the basis of the verification information; and

setting the verification status to indicate a non-verified status in response to one or more predetermined conditions being satisfied.

3. A method according to claim 2, wherein the one or more predetermined conditions comprises one or more of: a predetermined time period having elapsed; a predetermined number of transaction requests having been received; and a predefined transaction total being reached.

4. A method according to any preceding claim, wherein the payment transaction comprises a contactless payment transaction, the payment terminal comprises a contactless payment terminal and the payment device comprises a contactless payment device.

5. A method according to claim 4, wherein the contactless payment device comprises a fob or tag device.

6. A method according to any preceding claim, wherein the payment transaction does not comprise a verification process to verify the user.

7. A method according to any preceding claim, comprising a sending a message indicating whether the payment transaction is authorised to the payment terminal in response to said determination.

8. A method according to any preceding claim, wherein the determination is performed partly on the basis of a comparison of a value of the transaction with a predetermined threshold value.

9. A method according to any preceding claim, wherein the verification information comprises an indication that the user has been verified.

10. A method according to any of claim 1 to claim 8, wherein the verification information comprises information input to the first computing device by the user, and the method comprises performing said verification process at the server system on the basis of thereof.

11. A method according to claim 10, comprising receiving the verification information in a Short Message Service (SMS) message.

12. A method according to any of claim 1 to claim 10, comprising receiving the verification information from a software application held on the first computing device.

13. A method according to any preceding claim, wherein the first computing device comprises a mobile communications device.

14. A computer program for authorising a payment transaction, the computer program comprising instructions for a server system to perform a method of authorising a payment transaction, the method comprising:

receiving, at a server system, from a first computing device, verification information relating to a verification process for verifying a user associated with the first computing device;

setting a verification status associated with the user in a memory of the server system, based on the verification information;

receiving, at the server system, an authorisation request to authorise a payment transaction, the authorisation request being received from a payment terminal and including an identifier associated with the user, the information having been provided to the payment terminal by a payment device, the payment device being different from the first computing device;

responsive to receipt of the authorisation request, identifying the verification status associated with the user based on the identifier; and

determining whether to authorise the payment transaction at least partly on the basis of the identified verification status.

15. Apparatus for authorising a contactless payment transaction, the apparatus being arranged to:

receive from a first computing device, verification information relating to a verification process for verifying a user associated with the first computing device;

set a verification status associated with the user in a memory, based on the verification information;

receive an authorisation request to authorise a payment transaction, the authorisation request being received from a payment terminal and including an identifier associated with the user, the information having been provided to the payment terminal by a payment device, the payment device being different from the first computing device;

responsive to receipt of the authorisation request, identify the verification status associated with the user based on the identifier; and

determine whether to authorise the payment transaction at least partly on the basis of the identified verification status.