

(21) Application No: **1519676.9**

(22) Date of Filing: **06.11.2015**

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

(72) Inventor(s):
Lewis Graham

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

(51) INT CL:
G06Q 20/32 (2012.01) **G06Q 20/38** (2012.01)
G06Q 20/40 (2012.01)

(56) Documents Cited:
WO 2013/151797 A1 **WO 2013/015179 A1**
WO 2012/078964 A1 **US 20130173474 A1**
Proxama, 2015, "EMV-TT A virtualised payment system", Proxama.com, [online], Available from: <http://www.proxama.com/wp-content/uploads/2015/09/EMV-TT-A-VIRTUALISED-PAYMENT-SYSTEM.pdf> [Accessed 22 April 2016].

(58) Field of Search:
 INT CL **G06Q**
 Other: **EPODOC, WPI, INTERNET**

(54) Title of the Invention: **Transaction authorisation**
 Abstract Title: **Contactless transaction authorisation**

(57) A method of authorising an electronic transaction where a user device 100 receives a shared secret and a shared secret identifier. On receipt of transaction data from a transaction terminal 102, the user device calculates a hash value from data comprising the shared secret, generates authentication data comprising the hash value and the shared secret identifier, and transmits the authentication data to the transaction terminal. The application further relates to Host Card Emulation (HCE) without a Secure Element (SE), wherein tokenisation is utilised in order to facilitate offline transactions. Tokens are therefore obtained by a first communications link and comprise an indexed link of shared secrets in which each shared secret is associated with a corresponding shared secret identifier. Data provided by these tokens is then hashed in order to provide an EMV compliant Authorisation ReQuest Cryptogram (ARQC) for transmission to a transaction terminal which accepts the ARQC in place of the usual PAN and therefore requires no modification.

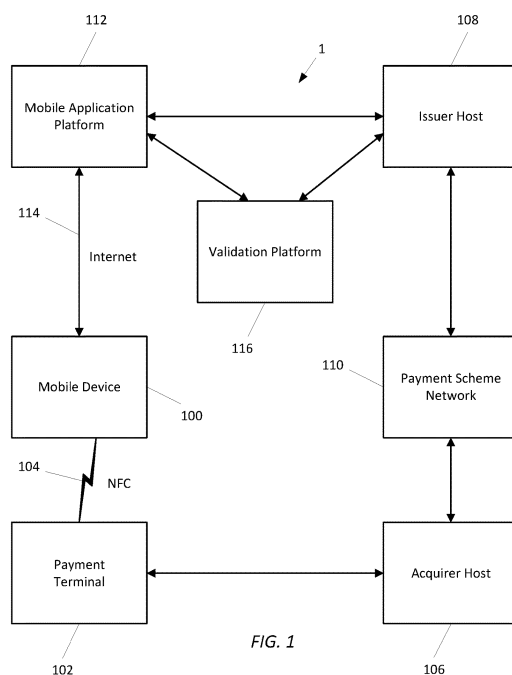


FIG. 1

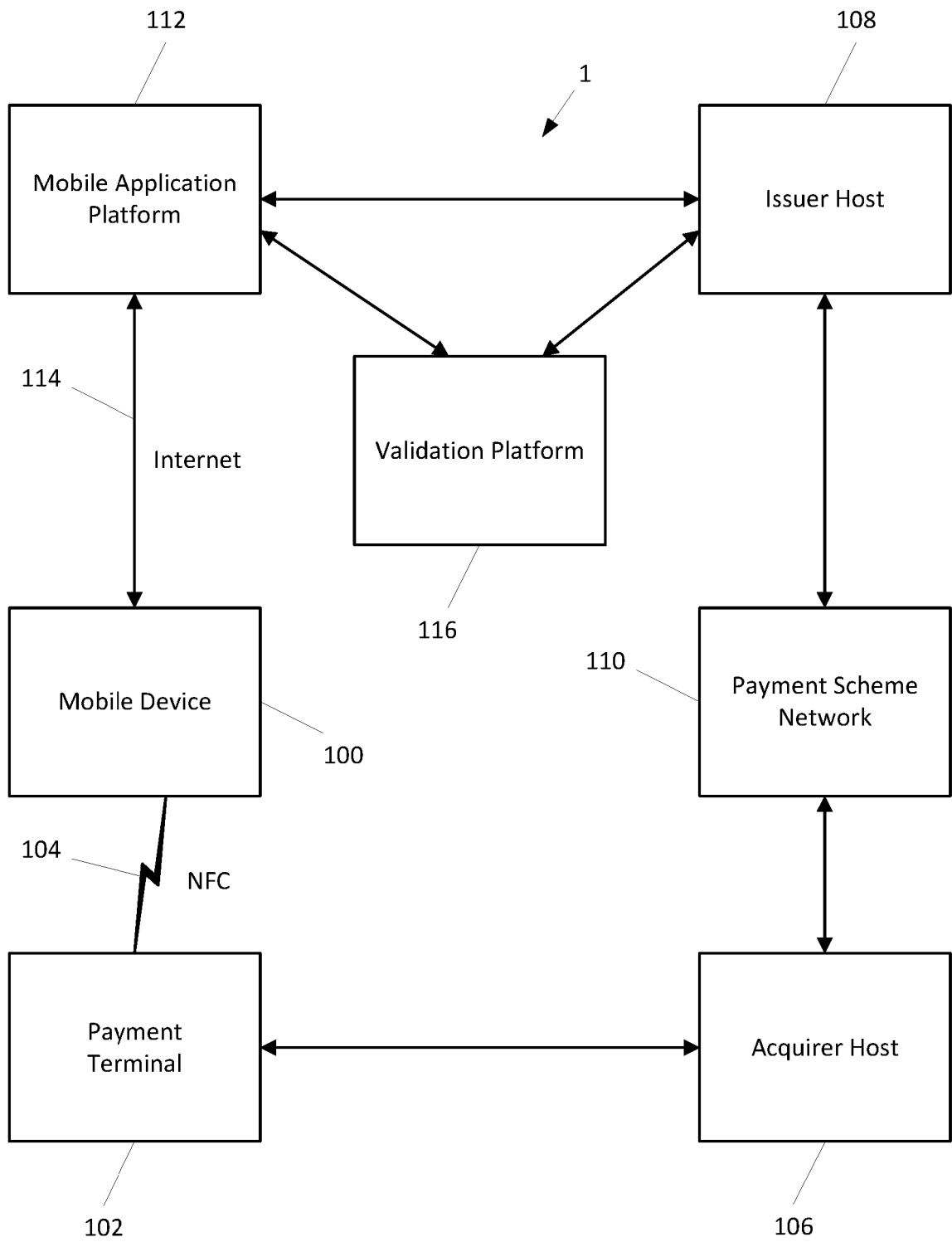


FIG. 1

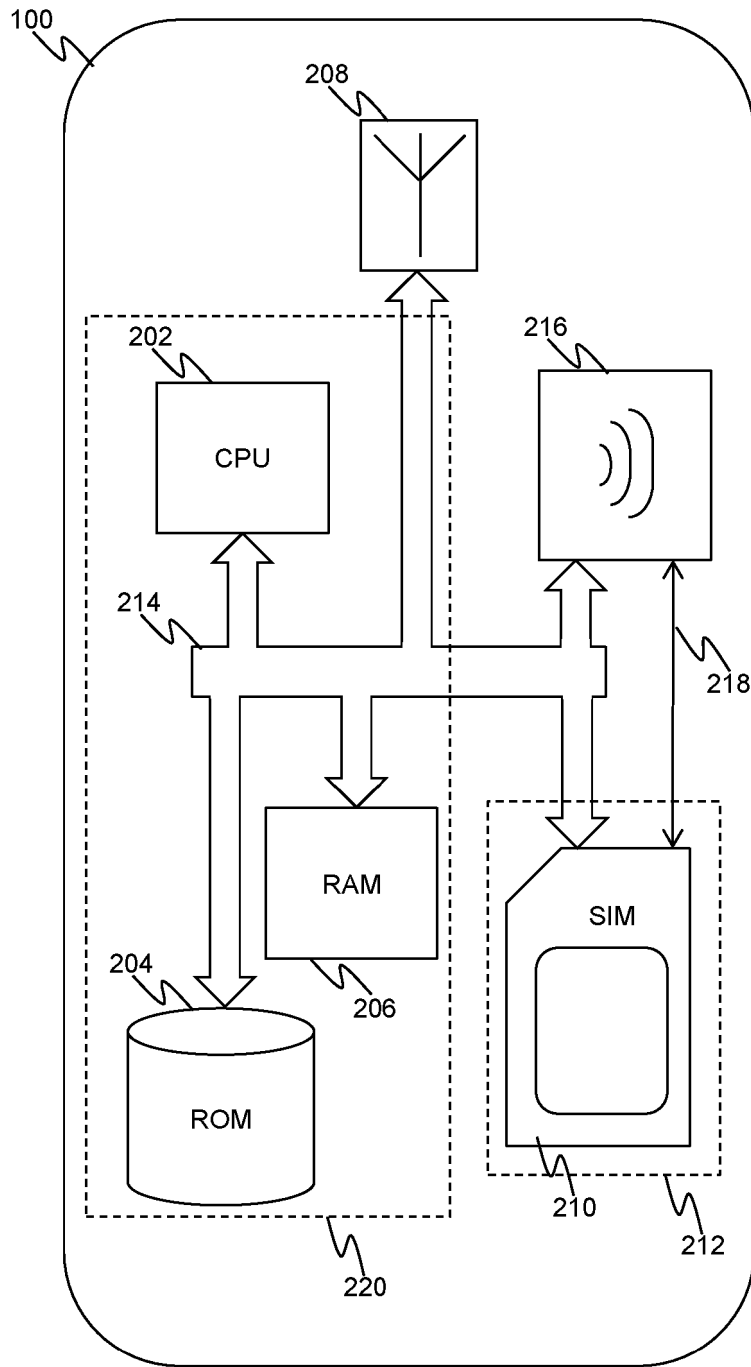


Figure 2

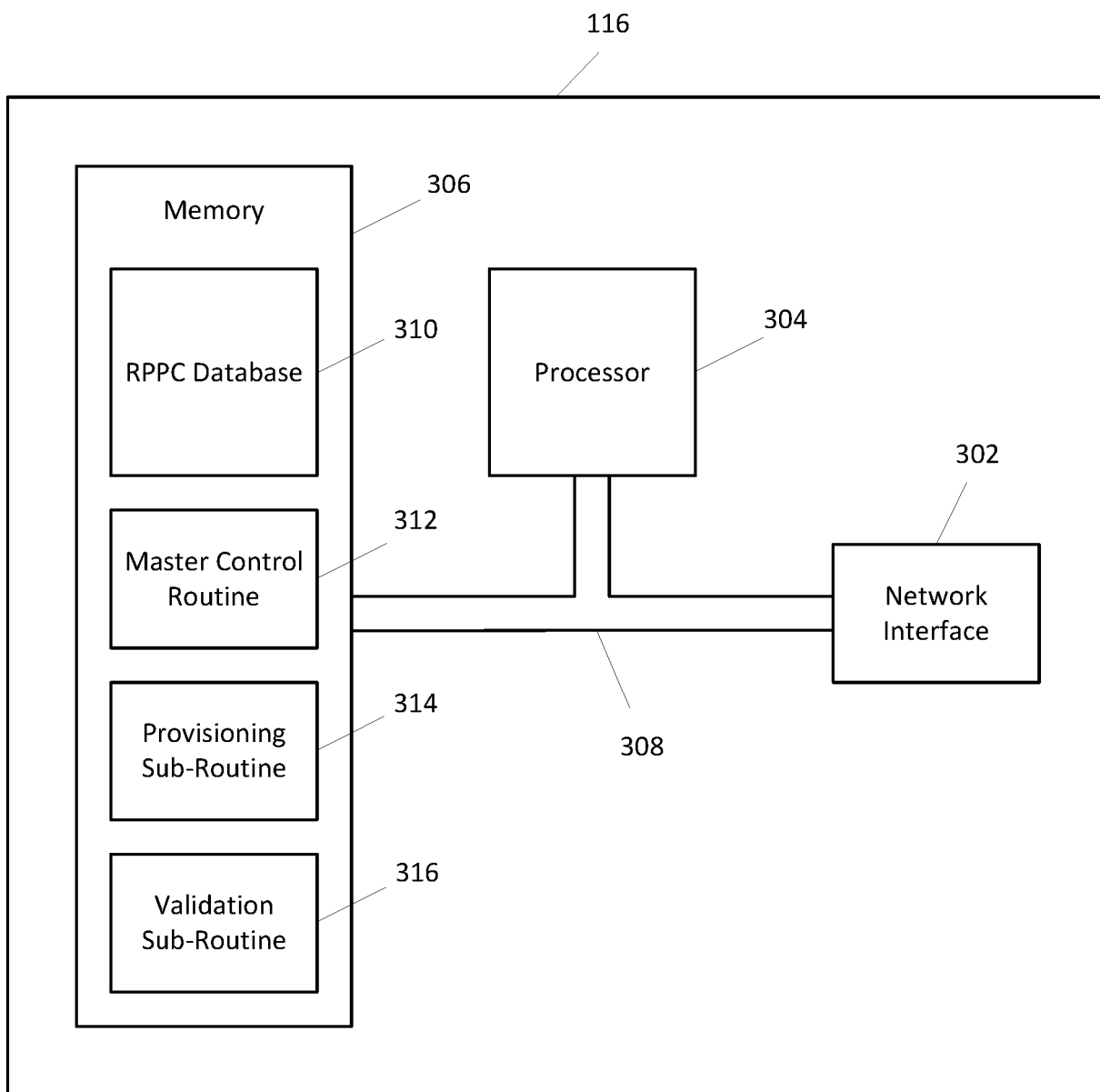


FIG. 3

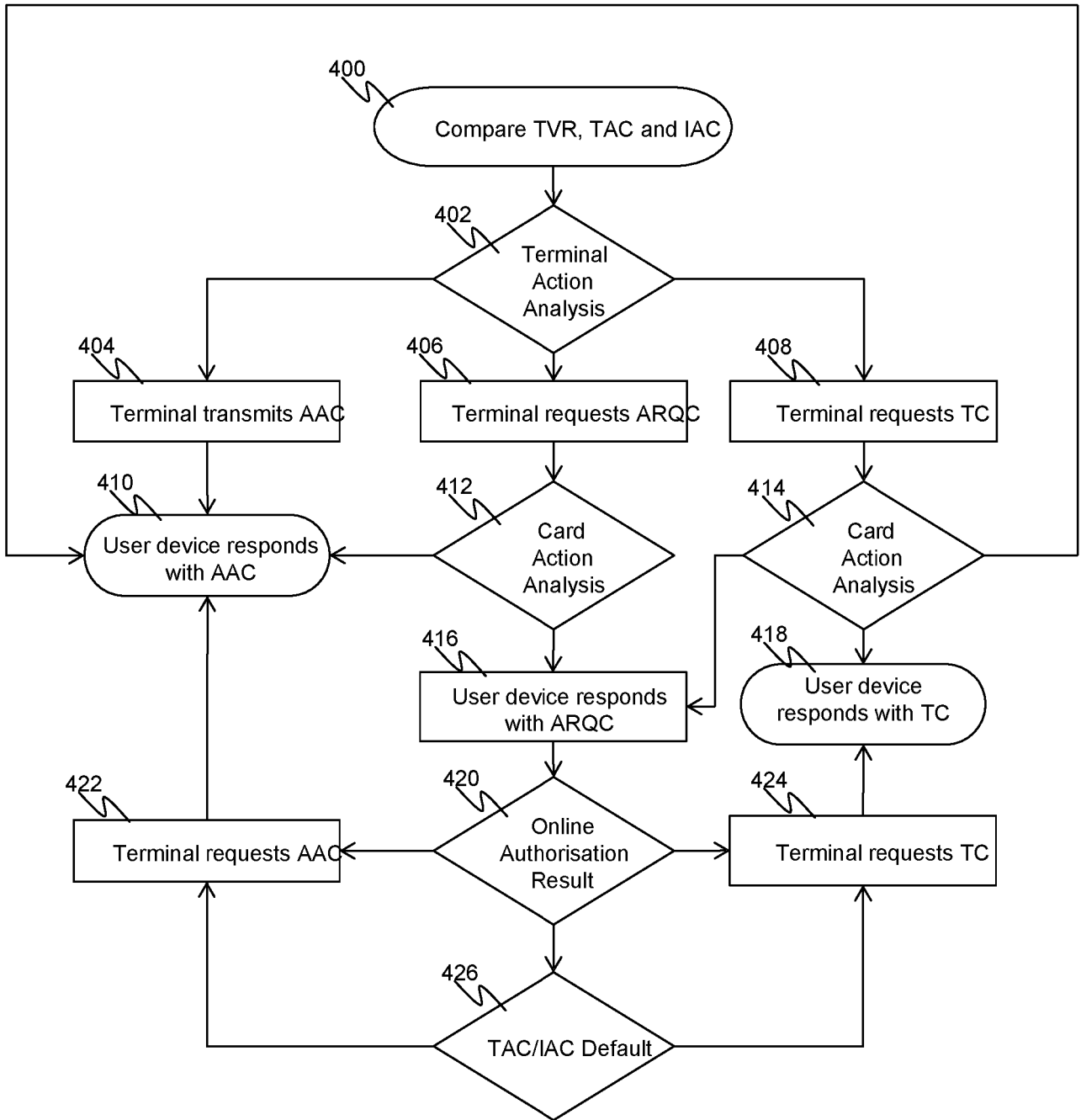


Figure4

Transaction Authorisation

Field of the Invention

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

Background

10 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 payment card may include a magnetic stripe containing information such as data relating to the account holder and an account from where the
15 funds for the transaction may be drawn. Such a magnetic stripe payment card is typically swiped through a magnetic card reader which reads data necessary for enacting the transaction. In another example, some payment cards are embedded with a semiconductor device (a “chip”) storing the above information and an interface is provided on the card for interacting with a card reader. This interface typically
20 takes the form of physical conductive pads.

Transactions using financial instruments may involve verification (authentication) of the user. For example, the user may be required to provide a signature. Alternatively, the user may be required to input a Personal Identification Number (PIN) on the terminal when prompted. The PIN may be sent to a server, in
25 encrypted form, for verification in a technique referred to as online PIN verification. Alternatively, 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 in a technique that is often referred to as offline PIN verification.
30 Each of the above verification 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.

A so-called contactless payment transaction method has been developed. 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.

For contactless payment transactions, it is difficult to secure the communication between the contactless payment device and the contactless payment terminal. However, the protocols for communicating between the contactless payment device and the contactless payment terminal have limited flexibility for implementing new data security techniques. If the contactless payment device includes functionality for accessing the Internet, as is present for example in many mobile phones, then various online data security techniques have been proposed. However, a disadvantage of data security techniques that require an Internet connection at the time of a transaction is that an Internet connection is not always available when a transaction takes place.

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. Dependent claims prescribe further detailed implementations of various embodiments.

In accordance with a first aspect, there is provided a method of authorising a transaction, the method comprising a user device receiving a shared secret and a shared secret identifier, receiving transaction data from a transaction terminal, calculating a one-way hash of data comprising the shared secret to generate a hash value, generating authentication data comprising the hash value and the shared secret identifier, and transmitting the authentication data to the transaction terminal. The receiving of the shared secret and the shared secret identifier need not occur during the transaction process. Accordingly, the shared secret can be supplied to the user device in advance of a transaction, and therefore a transaction can be performed offline, i.e. without an Internet connection, without needing to transmit the shared secret from the transaction terminal to the user device. The transmission of the authentication data can be achieved using the data formats available in existing contactless transaction protocols.

The method may comprise the user device receiving a plurality of shared secrets and a plurality of shared secret identifiers, each shared secret identifier corresponding to a respective shared secret, wherein the authentication data comprises the shared secret identifier corresponding to the shared secret used in the calculation of the hash value. In this way, a plurality of transactions may be performed without requiring an Internet connection.

The user device may receive the shared secret and the shared secret identifier via a first communication link, and transmit the authentication data via a second communication link different from the first communication link. The first communication link may communicate data using the Internet Protocol, and the second communication link may communicate data using a Near Field Communication protocol.

The method may further comprise verifying the identity of the user of the user device, with the data used to calculate the hash value further comprising information relating to the identity verification. The verifying of the identity of the user may comprise using a Fast Identity Online technique.

The transaction may comprise a contactless payment transaction, in which case the payment terminal comprises a contactless payment terminal and the user device comprises a contactless payment device.

In accordance with a second aspect, there is provided a method of validating a transaction, the method comprising a validation platform provisioning a user device with a shared secret and a shared secret identifier, receiving authentication data for a transaction, the authentication data identifying the user and comprising a transaction hash value and a transaction shared secret identifier, verifying that the transaction shared secret identifier corresponds to a valid shared secret; calculating a verification hash value by calculating a one-way hash of data comprising the shared secret corresponding to the transaction shared secret identifier; and comparing the transaction hash value and the verification hash value to determine if the transaction is valid. By provisioning a shared secret identifier in conjunction with a corresponding shared secret, the validation platform is able to identify the shared secret used to calculate the transaction hash value without the provision of the shared secret forming part of the transaction process at the time of the transaction. Accordingly, the shared secret can be provided to the user device in advance of a transaction, and therefore a transaction can be performed offline, i.e. without an Internet connection, without needing to transmit the shared secret from the transaction terminal to the user device.

The validation platform may provide the user device with a plurality of shared secrets and a plurality of shared secret identifiers, each shared secret identifier corresponding to a respective shared secret. In this way, a plurality of transactions may be performed without requiring an Internet connection.

Following receipt of authentication data including a shared secret identifier, the validation platform may invalidate the shared secret corresponding to the shared secret identifier for future transactions. In this way, protection against replay attacks is provided.

The data used to calculate the verification hash value may further comprise information relating to the identification of the user.

According to a third aspect of the invention, there is provided an apparatus comprising a first interface for receiving a shared secret and a shared secret identifier from a remote device via a first communication system and a second interface for receiving transaction data from a transaction terminal via a second communication system, the apparatus being arranged to calculate a one-way hash of data comprising the shared secret to generate a hash value, generate authentication data comprising the

hash value and the shared secret identifier, and transmit the authentication data to the transaction terminal.

According to a fourth aspect of the present invention, there is provided an apparatus arranged to provision a remote user device with a shared secret and a shared secret identifier, the apparatus being further arranged to receive authentication data for a transaction, the authentication data identifying the user and comprising a transaction hash value and a transaction shared secret identifier, verify that the transaction shared secret identifier corresponds to a valid shared secret, calculate a verification hash value by calculating a one-way hash of data comprising the shared secret corresponding to the transaction shared secret identifier; and compare the transaction hash value and the verification hash value to determine if the transaction is valid.

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

Figure 3 schematically illustrates a validation platform for use in an embodiment; and

Figure 4 shows a process flow of an authentication process performed by a user device and a payment terminal according to an embodiment.

Detailed Description of Illustrative Embodiments

Figure 1 illustrates a transaction system 1 in which embodiments may be implemented. In particular, the transaction system of Figure 1 is a payment transaction system in which a mobile device 100 can perform a contactless payment transaction with a contactless payment terminal 102 over a first communication link 104 using Near Field Communication (NFC). The NFC communication protocol is standardised in ISO/IEC 18092.

In the transaction system 1, the contactless payment terminal 102 is a Point of Sales (PoS) terminal located in a business premises, for example a shop, restaurant, cinema, station or other location, and is arranged to process payment transactions on behalf of the business or other entity associated with the PoS terminal.

5 The contactless payment terminal 102 is able to maintain or establish a data connection with an acquirer host 106 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. The communication between the contactless
10 payment terminal 102 and the acquirer host is typically via a leased line.

 An issuer host 108 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 mobile device 100.

 Each of the acquirer host 106 and the issuer host 108 is capable of
15 communicating with a payment scheme network 110. The payment scheme network 110 is a server system of computing devices which may be associated with a financial services organisation, for example.

 In the transaction system 1, the operating system of the mobile device 100 supports Host Card Emulation or the like that permits cloud-based payment
20 transactions using a mobile application (not shown in Figure 1) stored by the mobile device 100. The mobile application in the transaction system 1 is not stored in a secure element within the mobile device (such as an ISIM) card, and therefore sensitive account information such as the Primary Account Number (PAN) is stored in servers linked to the mobile application to provide security for the sensitive account
25 information. The mobile application is able to communicate with a mobile application platform 112 using a second communication link 114 using the Internet Protocol when the mobile device 100 is online (i.e. when an Internet connection exists). The mobile application platform 112 is able to communicate with the issuer host 108.

30 As shown in Figure 1, the mobile application platform 112 is also able to communicate with a validation platform 116. A communication link also exists between the validation platform 116 and the issuer host 108.

Although the mobile application platform 112 and the issuer host 108 are shown separately in Figure 1, the mobile application platform 112 could be hosted by one or more servers of the issuer host 108. Similarly, although the validation platform 116 is shown separately from the issuer host 108, the validation platform 116 could be hosted by one or more servers of the issuer host 108.

As will be described in detail hereafter, the validation platform 116 provisions, via the mobile application platform 112, the mobile application within the mobile device 100 with an indexed list of shared secrets (which will hereinafter be referred to as a Relying Party Provisioned Challenges or RPPCs) in which each shared secret is associated with a corresponding shared secret identifier. An RPPC is known only within the validation platform 116 and within the mobile application of the mobile device 100. An RPPC is used when forming an application cryptogram for a transaction. After the transaction has been completed, the validation platform 116 marks the RPPC used for that transaction as no longer being valid.

Figure 2 illustrates exemplary components of a user device according to embodiments of the present invention wherein the user device comprises a mobile telephony device.

User device 100 comprises conventional computational hardware including a processing portion 202, read only memory 204, random access memory 206, and other standard hardware such as an input/output controller, display controller etc. (not shown). User device 200 also comprises specific mobile telephony hardware including telephony antenna 208, and SIM card 210. The SIM card 210 constitutes a secure processing environment on the user device, also known as secure element 212, and incorporates additional security measures such as tamper resistance. The components described above are accessible to processing portion 202 via an internal communication structure, such as system bus 214. The operation and interaction of these components is well known in the art and therefore will not be covered in further detail here.

User device 100 also includes short range wireless communications hardware, including short range wireless antenna 216, which can be used to make contactless communication with the PoS terminal 102, and may be an NFC antenna.

Typically, where short range wireless antennas have hitherto been provided in known mobile telephony devices, they have been controlled by the SIM 210, via a

dedicated communication channel 218, separate to system bus 214. The dedicated communication channel 218 may, for example, use the Single Wire Protocol for communication. According to embodiments of the present invention, the short range wireless antenna is accessible from an area outside of secure element 212, hereafter
5 known as the standard application environment 220, for example via the system bus 214. This feature is presently available, for example, in the host card emulation functionality of the Android operating system.

Standard application environment 220 also comprises the payment application deployed on device 100. The payment application may be installed on the standard
10 application environment at the time of manufacture of the device, or under the supervision of the issuing bank. Alternatively the payment application may be installed by the end user of the device. An end user may install the application by downloading the installation files to the user device, for example via the internet. Alternatively a user may install the application by downloading the installation files
15 first to another device, such as a personal computer, and then sideloading the files onto to the user device, for example via a USB connection. Alternatively still, a user may obtain the installation files by accessing an application portal on the user device, such as the Apple[®] AppStore[™], or the Android Market[™], which facilitate an integrated download and installation of application files. The download of installation
20 files facilitated by an application portal may be provided via an available internet connection, or over-the-air provisioning (OTAP).

Figure 3 shows exemplary components of the validation platform 116. As shown, the validation platform 116 includes a network interface 302, a processor 304 and memory 306 interconnected by bus system 308. The memory 306 stores data
25 including an RPPC database 310, and program code including a Master Control routine 312, a Provisioning sub-routine 314 and a Validation sub-routine 316.

The RPPC database 310 stores for each user device 100 a table of RPPC codes. Each RPPC code is associated with an index number, an expiry date and a status, which may be valid or invalid.

30 The Provisioning sub-routine 314 is initiated by the Master Control routine 312 to provide new RPPC codes to a user device 100. The execution of the Provisioning sub-routine 314 may be initiated in response to receipt of a request by the user device 100. The Provisioning sub-routine 314 forwards at least one new

RPPC code to the user device 100, together with an index number for each RPPC code forwarded and the expiry date. The Provisioning sub-routine also stores each forwarded RPPC code and corresponding index number and expiry date in the table in the RPPC database 310 for that user device 100, and sets the status of each forwarded RPPC code to valid.

As will be discussed in more detail hereafter, the Validation sub-routine 316 is initiated by the Master Control routine 312 to validate an application cryptogram received from the issuer host 108. After the use of a valid RPPC in a transaction, the status of the RPPC in the table for the user device 100 is set to invalid in order to prevent reuse of the RPPC. In this way, possible “replay” attacks, in which bogus transaction data is prepared using an RPPC that has been already used for a previous transaction are prevented.

Before the transaction is completed, the payment terminal 102 must ensure that the presented user device 100 is both genuine, and authorised to complete the transaction. Authentication of payment devices and authorisation of transactions are handled according to transaction protocols, which ensure the interoperability of a range of payment devices and payment terminals.

The transaction system 1 of Figure 1 uses the EMV (Europay®, Mastercard®, Visa®) transaction protocols, as defined for example in the EMV Contactless Specifications for Payment Systems, which are publicly available and published by EMVCo LLC. These protocols are referred to herein as simply “EMV”.

EMV provides methods that support dynamic signature generation, of which Dynamic Data Authentication (DDA) is the simplest. Additionally, EMV provides a method called Fast DDA (fDDA) which is optimised for contactless transactions, and a method called Combined Data Authentication (CDA), which combines DDA with the subsequent step of Application Cryptogram Generation (described below), in order to allow both operations to be completed in parallel.

EMV provides for transaction authorisation through the generation of application cryptograms. Depending on which options are used from the various EMV specifications, there are several mechanisms available for application cryptogram generation. Throughout the transaction processing, the success or failure of certain checks and actions, such as those described above in relation to offline data authentication, can be recorded in a Terminal Verification Results (TVR) data.

The TVR data is reviewed during Terminal Action Analysis, and on the basis of its contents, the terminal makes a preliminary decision about whether the transaction should be approved offline, authorised online, or declined. Approval offline comprises the terminal deciding that the transaction can take place without seeking express permission from the Issuing Bank. Online authorisation comprises sending details of the transaction to the Issuing Bank for authorisation before approving the transaction. In some circumstances, the terminal will decline the transaction offline, before seeking authorisation from the Issuing Bank.

The decision of the appropriate course of action for the terminal to take is made on the basis of Terminal Action Codes (TAC) and Issuer Action Codes (IAC). TACs are programmed into the terminal by the acquiring bank, and define the circumstances under which a transaction should be approved offline, authorised online, or declined. IACs are deployed into the payment application by the issuing bank, and also define a set of circumstances under which a transaction should be approved offline, authorised online, or declined. The terminal uses both the TACs and the IACs in order to make a preliminary decision on how to process the transaction.

Figure 4 illustrates an exemplary Application Cryptogram Generation command flow diagram according to the EMV transaction protocols.

The flow begins at step 400 by comparing the contents of the TVR to the TACs stored at the payment terminal 102 and the IACs retrieved from the payment application on the user device 100. On the basis of the comparison, the payment terminal 100 makes a preliminary decision about whether the transaction should be approved offline, authorised online, or declined in step 402.

Depending on the result of the decision made at step 402, the terminal requests a specific type of Application Cryptogram to be generated by sending a GENERATE AC command to the user device 100. If the payment terminal 102 decides to decline the transaction offline, the GENERATE AC command requests Application Authentication Cryptogram (AAC) in step 404. If the payment terminal 102 decides to attempt to authorise the transaction online, the GENERATE AC command requests an Authorisation Request Cryptogram (ARQC) in step 406. If the payment terminal 102 decides to approve the transaction offline, the GENERATE AC command requests a Transaction Certificate (TC) in step 408.

In response to the GENERATE AC command issued by the payment terminal 102, the user device 100 may perform its own risk management in the form of “Card Action Analysis”. Card action analysis is performed on the basis of parameters determined by the issuer and stored on the user device 100. The result of the Card
5 Action Analysis can only elect an authorisation method the same as determined by the payment terminal 102 or stricter.

If the payment terminal 102 decides to reject the transaction offline by requesting an AAC as per step 404, the user device 100 must respond with an AAC in step 410. Any other response from the user device 100 will cause the transaction
10 processing to fail.

If the payment terminal 102 decides to attempt to send the transaction online for authorisation by the issuing bank by requesting an ARQC as per step 406, as a result of the Card Action Analysis in step 412 the user device 100 may decide to respond with an ARQC in step 414 as requested, or elect to decline the transaction
15 offline by responding with an AAC in step 410. A response from the user device 100 comprising a TC will cause the transaction processing to fail.

If the payment terminal 102 decides to allow the transaction offline by requesting a TC as per step 408, as a result of the Card Action Analysis in step 414 the user device may decide to respond with a TC in step 418 as requested, elect to
20 send the transaction online for authorisation by the issuing bank by responding with an ARQC in step 416, or elect to decline the transaction by responding with an AAC in step 410.

If the user device 100 responds with an ARQC, the payment terminal 102 attempts to send this to the issuing bank for authorisation in step 420. If the result of
25 the online authorisation procedure is to reject the transaction, the payment terminal 102 requests an AAC in step 422 by sending a second GENERATE AC command, and the AAC is returned by the user device in step 410. If the result of the online authorisation procedure is to authorise the transaction, the payment terminal 102 requests a TC in step 424 by sending a second GENERATE AC command, and the
30 AAC is returned by the user device 100 in step 416.

Alternatively, if the online authorisation procedure cannot be completed, the terminal reverts to a default method as defined in the TAC/IAC, by sending a second GENERATE AC command which either requests an AAC as per step 422, which is

returned by the user device 100 in step 410, or a TC in step 424, which is returned by the user device 100 in step 418.

Once the user device 100 has responded with either an AAC or a TC as per steps 410 or 418 respectively, the Application Cryptogram Generation command flow is completed.

In order to respond to a GENERATE AC command issued by the terminal, the user device 100 must produce an Application Cryptogram. An Application Cryptogram is produced on the basis of data sent to the user device 100 in the data field of the GENERATE AC command. The data to be used is specified in a Card Risk Management Data Object List (CDOL), which is stored in the user device 100. The user device 100 stores two CDOLs, one for use with the first GENERATE AC command issued in a given transaction, and the other to be used if a second GENERATE AC command is issued.

The Application Cryptogram is generated by applying a hash algorithm to a data set specified by a CDOL to generate a hash value. A hash algorithm is a one-way mathematical operation that is used to generate a fixed size result on the basis of a large or variably sized data input. The result depends on the entire data input, and it is computationally difficult to determine input data that would produce a given result. EMV recommends the use of the Secure Hash Algorithm (SHA-1) as standardised in ISO/IEC 10118-3.

In addition to the Application Cryptogram, in this embodiment the user device 100 also generates a supplementary hash value by applying a hash algorithm to a further data set including an RPPC, and optionally also the result of a user verification process (such as password or PIN entry, a biometric test or a technique such as FIDO) and possibly also verification data associated with the user verification process. The supplementary hash value is included together with the RPPC index corresponding to the RPPC used to generate the supplementary hash value in the ARQC data. The supplementary hash value is sufficiently small that the supplementary hash value and the RPPC index can be included in available space within the EMV message conveying the ARQC data.

When the issuer host 108 receives the ARQC data, the supplementary hash value and the RPPC index are forwarded to the validation platform 116, which determines from the RPPC index the corresponding RPPC, checks that the

corresponding RPPC is valid for that user device 100, and then calculates a validation hash value using the set of data used to generate the supplementary hash value in the ARQC data, and then compares the validation hash value with the supplementary hash value in the ARQC data. If the validation hash value matches the supplementary hash value, then the validation platform 116 sends a message to the issuer host 108 indicating that the user device 100 is authenticated. If the validation hash value does not match the supplementary hash value, then the validation platform 116 sends a message to the issuer host 108 indicating that the user device 116 is not authenticated. Whether or not the validation hash value matches the supplementary hash value in the ARQC data, the validation platform 116 then marks the RPPC value invalid for future transactions.

In use, 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 user device 100.

Once the contactless payment terminal 102 has been appropriately configured, the user (e.g. customer at a retail establishment) performs a user verification process on the user device 100 and then brings the contactless user device 100 into proximity with the contactless payment terminal 102. This results, for example, in the contactless payment terminal 102 sending a request to the contactless user device 100 to provide data for enacting the payment transaction. In response, the user device 100 retrieves and sends the requested data to the contactless payment terminal 102. 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. Messages sent by the user device 100 may be in protected form. For example, it may comprise a cryptogram, for example an EMV compliant Authorisation ReQuest Cryptogram (ARQC).

On receipt of a 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 108. The contactless payment terminal 102 then sends an authorisation request message to acquirer host 106, the message including the information received from the contactless payment device 100. 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 106 forwards same to the payment scheme network 110. In the present embodiment, the payment scheme network 110 routes the message to the issuer host 108 (for example, based on an indicator of the issuer included in the message). The issuer host 108 receives the authorisation request message, cryptographically verifying same using the validation platform 116 where appropriate, and performs a determination process to determine whether to authorise the contactless payment transaction. The issuer host 108 then returns a result of the determination to the acquirer host 106, via the payment scheme network 110, in a message including 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 108 is routed to the contactless payment terminal 102 via the payment scheme network 110 and acquirer host 106. 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.

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. Further, the systems and methods applied above can be used in transactions other than payment transactions. For example, the systems and methods described above can be used in an electronic access system in which a terminal device
5 (analogous to a lock) authenticates a user device (analogous to a key) before providing access. Such an electronic access system may provide access to data. Alternatively, such an electronic access system may be used to open a door to a safe, or a room or the like.

As discussed previously, using a shared secret in the form of an RPPC as
10 discussed above can prevent replay attacks. In addition, relay attacks can be largely defeated if the data set used to calculate the hash value in the ARQC included some transaction specific data.

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

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
20 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 an electronic transaction, the method comprising a user device:
 - 5 receiving a shared secret and a shared secret identifier;
 - receiving transaction data from a transaction terminal;
 - calculating a one-way hash of data comprising the shared secret to generate a hash value;
 - generating authentication data comprising the hash value and the shared secret
 - 10 identifier; and
 - transmitting the authentication data to the transaction terminal.

2. A method according to claim 1, wherein the user device receives a plurality of shared secrets and a plurality of shared secret identifiers, each shared secret identifier
15 corresponding to a respective shared secret, and
wherein the authentication data comprises the shared secret identifier corresponding to the shared secret used in the calculation of the hash value.

3. A method according to claim 1 or 2, wherein the user device receives the
20 shared secret and the shared secret identifier via a first communication link, and
wherein the user device transmits the authentication data via a second communication link different from the first communication link.

4. A method according to claim 3, wherein the first communication link
25 communicates data using the Internet Protocol.

5. A method according to claim 3 or claim 4, wherein the second communication link is a wireless communication link.

- 30 6. A method according to claim 5, wherein the second communication link communicates data using a Near Field Communication protocol.

7. A method according to any preceding claim, further comprising verifying the identity of the user of the user device,
wherein the data used to calculate the hash value further comprises information relating to the identity verification.
- 5
8. A method according to claim 7, wherein the verifying of the identity of the user comprises using a Fast Identity Online technique.
9. A method according to any preceding claim, wherein the transaction
10 comprises a contactless payment transaction, the payment terminal comprises a contactless payment terminal and the user device comprises a contactless payment device.
10. A method of validating a transaction, the method comprising a validation
15 platform:
provisioning a user device with a shared secret and a shared secret identifier;
receiving authentication data for a transaction, the authentication data identifying the user and comprising a transaction hash value and a transaction shared secret identifier;
20 verifying that the transaction shared secret identifier corresponds to a valid shared secret;
calculating a verification hash value by calculating a one-way hash of data comprising the shared secret corresponding to the transaction shared secret identifier;
and
25 comparing the transaction hash value and the verification hash value to determine if the transaction is valid.
11. A method according to claim 10, wherein the validation platform provisions the user device with a plurality of shared secrets and a plurality of shared secret
30 identifiers, each shared secret identifier corresponding to a respective shared secret.
12. A method according to claim 10 or 11, wherein following receipt of authentication data including a shared secret identifier, the validation platform

invalidates the shared secret corresponding to the shared secret identifier for future transactions.

5 13. A method according to any of claims 10 to 12, wherein the data used to calculate the verification hash value further comprises information relating to the identification of the user.

14. A computer program comprising instructions for performing a method as claimed in any preceding claim.

10

15. Apparatus arranged to perform a method as claimed in any of claims 1 to 13.



Application No: GB1519676.9

Examiner: Mr Anthony Haslam

Claims searched: 1-15

Date of search: 22 April 2016

Patents Act 1977

Corrected Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance
X	1-15	WO 2013/151797 A1 (MASTERCARD INTERNATIONAL INC) See abstract and figures.
X	1-15	WO 2012/078964 A1 (ELECTRONIC PAYMENT EXCHANGE et al.) See abstract and figures.
X	1-15	US 2013/0173474 A1 (RANGANATHAN et al.) See abstract and figures.
X	1-15	Proxama, 2015, "EMV-TT A virtualised payment system", Proxama.com, [online], Available from: http://www.proxama.com/wp-content/uploads/2015/09/EMV-TT-A-VIRTUALISED-PAYMENT-SYSTEM.pdf [Accessed 22 April 2016].

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC^X :

--

Worldwide search of patent documents classified in the following areas of the IPC

G06Q

The following online and other databases have been used in the preparation of this search report

EPODOC, WPI, INTERNET

International Classification:

Subclass	Subgroup	Valid From
G06Q	0020/32	01/01/2012
G06Q	0020/38	01/01/2012



Subclass	Subgroup	Valid From
G06Q	0020/40	01/01/2012