

SERVER AND METHOD FOR FACILITATING AN UN-AUTHENTICATABLE TRANSACTION

FIELD OF INVENTION

[1] The present invention relates broadly, but not exclusively, to servers and methods for facilitating un-authenticatable transactions.

BACKGROUND

[2] Initiating and settling transactions between a user and a recipient are taking place in various situations. On the other hand, the mode under which transactions are initiated and settled is shifting from cash payment to cashless payment. Recently, mobile devices (or user devices) are commonly used for initiating and settling transactions such as generating a transaction request and making payment for purchases made at physical stores or for transportation services. There are several ways to use mobile devices for initiating and settling transactions. In an example, a combination of QR codes (2D barcodes) and a QR code scanning function of mobile devices is increasingly used for initiating and settling transactions. QR codes are typically used to transfer information, such as a Uniform Resource Locator (URL). For example, a QR code scanner may be used to scan a QR code shown in advertisements in a public space to obtain a URL for further information of the advertisements. However, information obtained / transferred via QR codes may not be limited to a URL. Information required for initiating and settling transactions may also be transferred via QR codes.

[3] In a conventional way for initiating and settling transactions using QR codes, a QR code scanning function is required to be activated. For example, an online banking application installed in a mobile device, which requires a stable Internet connection between the mobile device and a server to function, has to be first activated before the application may be used.

[4] Typically, a transaction has to be first authenticated before the user who initiates the transaction may proceed to use the QR code scanning function in the online banking application. That is, the user has to provide the necessary information to prove that he is the true holder (or owner) of an account indicated in the corresponding

request of the transaction. In order to carry out authentication of the transaction, inputs from the user may have to be compared to a password, typically set at registration, corresponding to the account. That is, the authentication of the transaction may require a stable Internet connection for sending the inputs of the user. Practically speaking, a stable Internet connection may not always be available but the user and the recipient may want to initiate and settle transactions using the QR code even if the mobile device of the user is not in a stable Internet connection. If the authentication fails to complete due to unstable Internet connection, the user's experience for the transactions becomes quite unsatisfactory, which is undesirable for all parties involved in the transactions.

[5] The QR code scanning function in the online banking application may be used for scanning QR codes prepared by an acquirer server for a recipient of the transactions. To do so, an issuer institute is required to prepare the online banking application with the QR code scanning function and the acquirer server is required to prepare the QR codes for the recipient. Further, the issuer institute has to incorporate, into the online banking application, a function to handle QR code specific data element in order to accept data scanned by the QR code scanning function.

[6] A need therefore exists to provide methods and systems for facilitating an un-authenticatable transaction that addresses one or more of the above-mentioned problems.

SUMMARY

[7] According to a first aspect of the present invention, there is provided a server for facilitating an un-authenticatable transaction for an Internet connection capable user device when the user device is not in Internet connection with the server, the server comprising: at least one processor; and at least one memory including computer program code, the at least one memory and the computer program code configured to, with the at least one processor, cause the server at least to: receive, from the user device, a token and a transaction request, the token being one that was generated when the user device was in Internet connection with the server and the transaction request indicating an account, a user account and a recipient account to be used for the un-authenticatable transaction; verify if the token corresponds to one that has been registered for the account; and send,

to an issuer server, an authorization to transfer the amount indicated in the transaction request from the user account in response to the verification of the token.

[8] According to a second aspect of the present invention, there is provided a method for facilitating an un-authenticatable transaction for an Internet connection capable user device when the user device is not in Internet connection with the server, comprising receiving, from the user device, a token and a transaction request, the token being one that was generated when the user device was in Internet connection with the server and the transaction request indicating an account, a user account and a recipient account to be used for the un-authenticatable transaction; verifying if the token corresponds to one that has been registered for the account; and sending, to an issuer server, an authorization to transfer the amount indicated in the transaction request from the user account in response to the verification of the token.

BRIEF DESCRIPTION OF THE DRAWINGS

[9] Embodiments of the invention will be better understood and readily apparent to one of ordinary skill in the art from the following written description, which provides examples only, and in conjunction with the drawings in which:

[10] Figure 1A shows a block diagram of facilitating an un-authenticatable transaction according to various embodiments;

[11] Figure 1B shows a block diagram of how a payment network server shown in Figure 1A may be used for facilitating an un-authenticatable transaction according to various embodiments;

[12] Figure 2A shows a flow diagram illustrating a method for facilitating an un-authenticatable transaction according to various embodiments;

[13] Figure 2B shows a flow diagram illustrating a method for generating a QR code for use in an un-authenticatable transaction request according to various embodiments;

[14] Figure 3 shows an exemplary transaction flow illustrating a transaction flow between a merchant and a consumer from a point of view of the merchant and the consumer according to various embodiments;

[15] Figure 4 shows an exemplary flow of existing registration procedures for merchant and an exemplary flow of registration procedures for merchant according to various embodiments;

[16] Figure 5 shows an exemplary flow for facilitating an un-authenticatable transaction between a customer and a merchant involving a server managed by an exemplary financial institutes such as a payment network server, a clearing centre, a service centre and an acquirer according to various embodiments; and

[17] Figure 6 shows an exemplary system for facilitating an un-authenticatable transaction according to various embodiments.

DETAILED DESCRIPTION

Overview

[18] Various embodiments provide servers and method for facilitating an un-authenticatable transaction.

[19] One solution is to facilitate un-authenticatable transactions, in a secure manner, between the user and the recipient where the user is not in a stable Internet connection for authentication of the transactions. To facilitate the un-authenticatable transactions in a secure manner, a token is obtained from a payment network server using a mobile device with Internet connection prior to the un-authenticatable transactions. The token is generated in response to authenticating that the user is an owner of a user account. The generated token is also saved in a database operationally coupled with the payment network server which is accessible via a different communication protocol when Internet connection is not present. The different communication protocol may include telephone network communication. By presenting the token using a communication protocol different than Internet connection, a user can show that he is the owner of the user account, which allows the transaction to be authorized. That is, the user and the recipient can perform transactions without the stable Internet connection, which significantly enhances experiences of the user and the recipient.

[20] In an example, the user intends to pay \$100 to the recipient in the basement or somewhere with unstable Internet connection. Before the user moves to basement or somewhere with unstable Internet connection and loses a stable Internet connection, the user device sends a request to the payment network server to generate a token which enables an un-authenticatable transaction to be performed in the basement or somewhere with unstable Internet connection. In response to the request from the user device, the token is generated by the payment network server and forwarded to the user device. The token is also saved in a memory operationally coupled with the payment network server. Once the token is generated and saved in the memory operationally coupled with the user device and in the memory operationally coupled with the payment network server, the user device is ready for the un-authenticatable transaction.

[21] Once the user device is ready for the un-authenticatable transaction, the user may proceed to the place with unstable Internet connection. To receive the payment, the recipient displays a QR code indicating a recipient account. The user activates the QR code scanner function in the application installed in the user device and scans the QR code displayed by the recipient. The amount \$100 can be input by the recipient or the user. In the event that the recipient input the amount, the recipient may use a recipient device to input the amount and generate the QR code indicating the amount. In the event that the user inputs the amount, the user may input the amount after scanning the QR code displayed by the recipient. Once the user device obtains the amount, the recipient account and the user account, the user device generates a transaction request. As the stable Internet connection is not available, the transaction cannot be authenticated. Therefore, the generated transaction request may also be considered as a request for an un-authenticatable transaction. However, even if a stable Internet connection is not available for the user device, a token as discussed in the previous paragraph enables the un-authenticatable transaction in the place with unstable Internet connection. The token saved in the memory operationally coupled to the user device is retrieved and sent by other communication means such as a telephone line communication together with the request for the un-authenticatable transaction proving that the user is the owner of the user account so that the un-authenticatable transaction can be authorized without compromising security of the transaction. In an example, the token may be sent from the user device to the payment network server via the recipient device using other communication means such as Near Field Communication (NFC) or Virtual Private Network (VPN). In other words, it can be appreciated that the token may be sent when there is no stable Internet

connection. As it is not necessary to wait for the user device to be in a stable Internet connection, the token and the transaction request can be sent to the payment network server immediately after the user has scanned the QR code of the recipient and entered the amount to be transferred and the token has been retrieved from the user device using a communication means such as a telephone line communication. For example, the user device can send the token and the transaction request to the payment network server when the user device and the recipient device are in connection, even when there is no stable Internet connection. Once the token is verified (e.g. the token sent with the request matches that corresponding to the user), an authorization for the transaction is sent to the issuer server and an acquirer server and the user and the recipient will be notified that \$100 is successfully transferred from the user account to the recipient account. Therefore, the recipient can confirm the payment has been received from the user before the user leaves from the recipient's place, even when there is no stable Internet connection.

[22] The following disclosure thus provides advantages, such as facilitating un-authenticatable transactions between the user and the recipient without compromising security. That is, the user and the recipient are able to initiate and settle the transactions utilizing the mobile device in an environment where the stable Internet connection is not available. If the transactions utilizing the mobile device can be used without limitation of the stable Internet connection requirement, the transactions can be taken place in a basement or rural area with insufficient network infrastructure. The expansion of available area for transactions utilizing the mobile device will significantly increase satisfaction of the user and the recipient. As a result, the transactions between the user and the recipient are also expected to increase.

Terms Description (in Addition to Plain and Dictionary Meaning of Terms)

[23] Unless context dictates otherwise, the following terms will be given the meaning provided here:

The term “authenticatable transaction” includes a transaction initiated based on information (e.g. account information and/or user information) that has to be first compared to those corresponding to an account indicated to be used. This process may be referred to as “authentication” of the transaction. An authenticatable transaction typically has to go through the authentication

process before an amount corresponding to the transaction may be transferred.

The term “authorization” includes receiving an instruction permitting a transfer of an amount from one account (typically a user account) to another account (typically a recipient account). The amount typically is one that is indicated in a transaction request. Typically, an authorization is sent by an entity that approves the transaction or indicates the transaction to be one that is initiated by the true holder of the account. The instruction may be in accordance with Application Programming Interface (API) compatible with each of the entities managing the accounts.

The term “un-authenticatable transaction” includes a transaction based on information (e.g. account information and/or user information) that may not have to be first compared to these corresponding to an account indicated to be used. The un-authenticatable transaction is typically initiated by a transaction request, along with a token. The un-authenticatable transaction typically does not have to go through the authentication process before the amount corresponding to the transaction may be transferred.

The term “Internet connection capable device” includes a device with at least one module for Internet connection such as 3G network module or Wi-Fi network module.

The term “user device” refers to a device which is capable of managing the user account. The user device may be a mobile device which includes any device for portable use including a mobile phone, a tablet computer, a wearable device such as a smart watch etc.

The term “recipient device” refers to a device which is capable of managing the recipient account. The recipient device may be a mobile device which includes any device for portable use including a mobile phone, a tablet computer, a wearable device such as a smart watch etc. Alternatively, the recipient device may be a point of sales (POS) system.

The term “one or more databases” refers to any databases located within a computing system or remote server such as a computer in a financial

institute or cloud server. The database or databases may each be a cloud database running on a cloud computing platform.

Exemplary Embodiments

[24] Embodiments of the present invention will be described, by way of example only, with reference to the drawings. Like reference numerals and characters in the drawings refer to like elements or equivalents.

[25] Figure 1A shows a block diagram of facilitating an un-authenticatable transaction according to various embodiments. In an example, the transaction is performed by at least a user device 102, a payment network server 104, an issuer server 106, an acquirer server 108, a user account 110 and a recipient account 112. In an example, the user device 102 may send, to the payment network server 104, a request for generating a token. The user device 102 may be configured to receive the requested token so that the user device 102 can send a request for the un-authenticatable transaction together with the received token to be verified by the payment network server 104. The received token is saved in a database, corresponding to the account indicated in the request requesting the token. The token saved in the database is retrievable, together with time stamp information indicating when the token is generated. In response to a verification of the token, an authorization may be sent to the issuer server 106 to transfer an amount indicated, in the un-authenticatable transaction, from the user account 110. After transferring the amount from the user account 110, the payment network server 104 may send an authorization to the acquirer server 108 to transfer the amount to the recipient account 112.

[26] In an example, the user device 102 may be a mobile phone, a wearable device or any other devices relating to the user account 110. The user device 102 may be configured to communicate with the payment network server 104. In an example, the user device 102 may be operationally coupled with a camera for scanning a QR code to obtain information such as the recipient account and an amount to be transferred. The user device 102 may be an Internet connection capable device including modules for Internet connection such as 3G communication or Wi-Fi communication.

[27] In an example, the payment network server 104 may be a server operationally coupled to the issuer server 106, the acquirer server 108 and the user device 102. The payment network server 104 may be configured to communicate with the user device 102 so that the payment network server 104 can facilitate an un-authenticatable transaction between the user account 110 and the recipient account 112. In various embodiments, the payment network server 104 may have at least two separate functions. First one is generating a token (or a single use key) in response to a request from the user device 102 which is performed when the user device 102 is in a stable Internet connection with the payment network server 104. Second one is facilitating the un-authenticatable transaction using the generated token, which is performed when the user device 102 is not in a stable Internet connection with the payment network server 104.

[28] With regard to generating a token in response to receiving a request from the user device 102, the payment network server 104 may be the one that receives, from the user device 102, a request for generating the token. The request for generating the token may include information of the account which is used in the un-authenticatable transaction such as account holder information. The request may also include information of the user, i.e. information of the person who is requesting to generate the token. The request may also include information of the user device 102 such as a serial number of the user device 102 to identify the device that was used to send the request. The payment network server 104 may be operationally coupled to the issuer server 106 and forward information included in the request for generating the token to the issuer server 106 and request to verify that the user is the account holder of the account. Once the issuer server 106 verifies that the user is the account holder of the account, the token may be generated by the payment network server 104 as requested by the user. The token may include the information of the account which will be used in the un-authenticatable transaction. The token may also include information of the user device 102 which is used to send the request for generating the token to limit the usage of the token to the user device 102. The token may further include time stamp information indicating when the token was generated so that a token generated before a specific time period can be expired. The generated token may be saved in a memory operationally coupled to the payment network server 104. The generated token may also be sent to the user device 102. The token itself may not be shown to the user in an explicit manner. In an example, an application of the user device 102 may send a request to generate a token to the payment network

server 104 and receive the generated token from the payment network server 104 and save the generated token in an internal memory of the user device 102 in an encrypted manner. In an example, a token indicator which indicates a presence of the token may be generated and saved in the internal memory of the user device 102 so that the presence of the token is indicated without decrypting the encryption of the token. The token may be tied to the user device 102 to prevent other people from using the token in other devices. If the user may need the token to be used in the other device, the user may be required to send, to the payment network server 104, a request for generating another token separately. These processes may be performed when the user device 102 is in a stable Internet connection with the payment network server 104.

[29] With regard to facilitating an un-authenticatable transaction using the generated token, the payment network server 104 may be the one that receives, from the user device 102, an un-authenticatable transaction request together with the token generated in the payment network server 104. The payment network server 104 may check whether or not the user device 102 sending the un-authenticatable transaction request correspond to the user device 102 which is used to send the request to generate the token based on information of the user device 102 indicated in the token. Furthermore, the payment network server 104 may check information of the time stamp and determine whether or not the token is acceptable in view of a time period when the token was generated for example the payment network server 104 may reject a token which was generated before a specific time period. Once the token received from the user device 102 is considered as valid in view of the user device information and the time stamp information, the payment network server 104 may compare the token received from the user device 102 with the token generated and saved in the memory operationally coupled with the payment network server. Once the payment network server 104 confirms that the token received from the user device 102 is identical with the token generated and saved in the memory operationally coupled with the payment network server 104, the un-authenticatable transaction request received together with the token may be considered valid and the account indicated in the token may be used for the un-authenticatable transaction request. These processes may be performed when the user device 102 is not in a stable Internet connection with the payment network server 104.

[30] In an example, the payment network server 104 may be configured to communicate with the recipient device 114 so that the payment network server 104 may generate the QR code indicating the recipient account in response to receipt of a request from the recipient device 114. However, if a recipient displays a static QR code printed on a sheet, the recipient device 114 may not be required for facilitating the un-authenticatable transactions.

[31] In an example, the issuer server 106 may be a server linked with an issuer institute of the user account 110. The issuer server 106 may be operationally coupled to the user account 110 so that the issuer server 106 can facilitate transactions relating to the user account 110. The issuer server 106 may also be operationally coupled to the payment network server 104.

[32] In an example, the acquirer server 108 may be a server linked with an acquirer institute of the recipient account 112. The acquirer server 108 may be operationally coupled to the recipient account 112 so that the acquirer server 108 can facilitate transactions relating to the recipient account 112. The acquirer server 108 may also be operationally coupled to the issuer server 106 and the payment network server 104.

[33] Figure 1B shows a block diagram of facilitating an un-authenticatable transaction according to various embodiments. In an example, the transaction is performed by at least a user device 102, a payment network server 104, an issuer server 106 and an acquirer server 108.

[34] In an example, the payment network server 104 may include at least one processor 122 and at least one memory 124 including computer program code. The at least one processor 122 and the at least one memory 124 may be configured to operationally coupled. Details of an example of the payment network server 104 will be explained with reference to Figure 6.

[35] The payment network server 104 may be configured to receive a transaction request and the token from the user device 102 directly or indirectly. The token may be the one that was generated when the user device 102 was in Internet connection with the payment network server 104. The token may be generated based on the user account 110 relating to the user device 102 and a time stamp of the request for the token from the user device 102. The transaction

request may indicate the amount, the user account 110, the recipient account 112 to be used for the un-authenticatable transaction.

[36] In an example, a transaction request may be labelled (or added a flag) by the payment network server 104 via the user device 102 in view of whether the transaction request is authenticatable or un-authenticatable. When the user device 102 is in a stable Internet connection with the payment network server 104, the transaction request from the user device 102 can be authenticated and a flag is raised to indicate that the transaction request is an authenticatable transaction request by the payment network server 104 via the user device 102. On the other hands, when the user device 102 is not in a stable Internet connection with the payment network server 104, the transaction request from the user device 102 cannot be authenticated by the payment network server 104 and it is not possible to raise a flag for the transaction request as an authenticatable transaction request. Thus, the transaction request remains un-authenticatable and it is labelled as an un-authenticatable transaction request by the user device 102. In other words, the transaction request may be an un-authenticatable transaction request by default until it is authenticated by the payment network server 104 using a stable Internet connection.

[37] When the payment network server 104 receives a transaction request, the payment network server 104 may check whether the received transaction request is an authenticatable transaction request or an un-authenticatable transaction request. In an example, the transaction request may include information, such as a flag or a label, regarding whether or not the transaction request is authenticatable. By checking the information of the transaction request, the payment network server 104 may determine whether the received transaction request is an authenticatable transaction request or an un-authenticatable transaction request. If the transaction is an un-authenticatable transaction, the payment network server 104 may further check whether any token to verify the un-authenticatable transaction is received. When the payment network server 104 receives the token, the payment network server 104 may be configured to verify if the token corresponds to one that has been registered for the user account 110 based on information included in the token, such as account holder information, user device information and time stamp information. In an example, the token was encrypted and saved in the user device 102 and only a specific application is configured to be able to decrypt the token saved in the user device 102 using a key stored in the specific application to avoid

access from other applications. The key for decrypting the token may be generated when the token was encrypted in the user device 102. In an example, the user device 102 may determine whether or not a stable Internet connection for authenticating a transaction is available in response that the user initiates a transaction using the user device, for example by activating a relevant application of the user device 102. The user device 102, more specifically an application of the user device 102, may make a threshold number of attempts for Internet connection to determine whether or not the stable Internet connection is available. If it is determined that the stable Internet connection is not available (for example, the user device 102 fails to establish a stable Internet connection after making the threshold number of times), the user device 102 may check whether a token for an un-authenticatable transaction is saved in the user device 102. In an example, there is a token indicator that indicates a presence of such a token and the user device 102 may check the token indicator to determine the presence of such a token. By using the token indicator, it may be possible to determine the presence of such a token without decrypting the token. In an example, once the presence of such a token is determined, the token for the un-authenticatable transaction is decrypted and information such as a time stamp thereof is checked. Once it is confirmed that the token can be used for the un-authenticatable transaction, the user may be notified that the un-authenticatable transaction is available for the user device 102.

[38] In an example, the payment network server 104 may be configured to send, to the issuer server 106, an authorization to transfer the amount indicated in the transaction request from the user account 110 in response to the verification of the token.

[39] In an example, the payment network server 104 may receive, from the issuer server 106, a notification indicating that the amount was transferred from the user account 110. In an example, the payment network server 104 may send, to the acquirer server 108, an authorization to transfer the amount indicated in the transaction request to the recipient account 112 in response to the notification.

[40] In an example, the payment network server 104 may determine a time period based on a time at which the token was generated and a time at which the transaction request is received. The authorization may be sent to the issuer server

106 in response to the determined time period. If it is discovered that the token was generated a long time ago, a validity of the token may be reviewed.

[41] In an example, the payment network server 104 may verify if the user account 110 is one that is permitted to transfer the amount indicated in the transaction request. The authorization may be sent to the issuer server 106 in response to the verification of the user account 110. If it is discovered that the amount indicated in the transaction request exceeds a predetermined amount permitted for the user account 110, the authorization may not be sent to the issuer server 106 and the user device 102 may indicate that the amount to be transferred exceeded the permissible amount of the user account 110.

[42] In an example, the payment network server 104 may generate a QR code indicating the recipient account 112. The QR code may be a static QR code or a dynamic QR code. In an example, the static QR code may include the recipient account 112. In an example, the static QR code may be printed on a sheet and the recipient device 114 may not be required. The static QR code may not indicate an amount to be transferred and may be used for several types of transactions for the recipient account 112. In an example, the user device 102 may scan the static QR code and obtain the recipient account 112 and input an amount to be transferred from the user account 110 to the recipient account 112. The user device 102 may generate a transaction request including the user account 110, the recipient account 112 and the amount to be transferred and send the transaction request to the payment network server 104.

[43] In an example, the payment network server 104 may receive, from the recipient device 114, an input indicating the amount to be transferred. The payment network server 104 may generate a QR code in response to the receipt of the input from the recipient device 114. The payment network server 104 may send, to the recipient device 114, the generated QR code indicating the amount to be transferred. In an example, the user device 102 may scan a dynamic QR code displayed on the recipient device 114. The dynamic QR code may indicate the recipient account and an amount to be transferred. The user device 102 may obtain the recipient account 112 and the amount to be transferred and generate a transaction request including the user account 110, the recipient account 112 and the amount to be transferred and send the transaction request to the payment network server 104.

[44] In an example, the payment network server 104 may connect to an application executing on the user device 102 to transfer the token and the transaction request when the user device 102 is in virtual private network (VPN) connection with the server. By using VPN, the token and the transaction request may be securely forwarded to the payment network server 104. Connection between the payment network server 104 and the user device 102 may be any network channels other than VPN.

[45] In an example, the payment network server 104 may determine a credibility score of the recipient account 112 based on a transaction history of the recipient account 112. For example, the transaction history of the recipient account 112 may be retrieved from the acquirer server 108 and the credibility score of the recipient account 112 may be calculated in view of reliability of the account such as rating from a user or a recipient who had experienced one or more transactions with the recipient account 112 in the past. The reliability of the account may also include a rate of success against failure in the past transactions. The authorization may be sent to the issuer server 106 in response to the determined credibility score of the recipient account 112. Although a user faces a recipient, the user does not know if the recipient is reliable enough to forward an amount of money. If the determined credibility score of the recipient account 112 is lower than a predetermined score, the recipient account 112 may be considered as unreliable and transferring the amount to the recipient account 112 may not be recommended. If the recipient account 112 is considered as unreliable, the authorization to the issuer server 106 may not be sent and the user device 102 may inform the user of the fact.

[46] In an example, the payment network server 104 may receive, from the user device 102, a request for the token when the user device 102 is in Internet connection with the server. The payment network server 104 may generate the token in response to the receipt of the request from the user device 102. The payment network server 104 may send, to the user device 102, the generated token for the un-authenticatable transaction. Even if the user device 102 is not in Internet connection with the payment network server 104, the user device 102 may send a transaction request and the token to the payment network server using a channel other than Internet connection and request for authorization of the transaction. The token may be single use key (SUK) or limited use key (LUK) which is verified by a token service provider such as the payment network server

104. In an example, the token may be configured to be expired after a specific time period to avoid usage of the token which is after a specific time period.

[47] Figure 2A shows a flow diagram 200 illustrating a method for facilitating an un-authenticatable transaction according to various embodiments. The method 200 includes at least the steps of:

- receiving, from a user device, a token and a transaction request, the token being one that was generated when the user device was in Internet connection with a server and the transaction request indicating an amount, a user account and a recipient account to be used for the un-authenticatable transaction; (step 202)
- verify if the user device corresponds to one that requested to generate the token (step 204);
- verifying if the token corresponds to one that has been registered for the user account; (step 206); and
- sending, to an issuer server, an authorization to transfer the amount indicated in the transaction request from the user account in response to the verification of the token (step 208).

[48] In step 202, the token and the transaction request may be received from the user device. The transaction request may indicate the amount, the user account and the recipient account to be used for the un-authenticatable transaction. The token may be generated when the user device was in Internet connection with the server. In an example, the user device may send a request to generate the token to a payment network server and the payment network server may generate the token in response to the request from the user device. In an example, the amount and the recipient account may be obtained by scanning the QR code. An exemplary flow relating to the QR code is explained with reference to Figure 2B.

[49] The transaction request and the token may be received separately or together. In an example, the token may be received and verified and then the transaction request may be received. In an example, the token may be received and a connection channel for the transaction request may be established after verification of the token. In an example the token and the transaction request may be received together and processed separately. The received transaction request

may be held until the token is verified. That is, the transaction request may not be processed until the token is first verified.

[50] In step 204, whether or not the user device corresponds to one that requested to generate the token may be verified. In an example, a token saved in an internal memory of the user device may be retrieved when the transaction request is sent to the payment network server. The token may be encrypted and require a key for decryption. The key may be operable with a relevant application of the user device. The token may include for example, the account holder information, the user device information and a time stamp of the generation of the token. If three tokens are requested for three separate devices, each requested token includes information for each separate device and distinguishable from each other. The token may be sent to the payment network server together with the transaction request. The payment network server may identify which device sent the transaction request and check whether the user device information in the token corresponds to the device which sent the transaction request.

[51] In step 206, whether or not the token corresponds to one that has been registered for the account may be verified. The token received from the user device may be compared with the token generated by the payment network server, which may be saved in a memory operationally coupled with the payment network server. In an example, information regarding the token received from the user device, for example, time stamp information indicating when the token was generated may be used for verification of the account.

[52] In step 208, the authorization may be sent to the issuer server to transfer the amount indicated in the transaction request from the user account in response to the verification of the token. In an example, the notification indicating that the amount was transferred from the user account may be received and the authorization may be sent to the acquirer server to transfer the amount indicated in the transaction request to the recipient account in response to the receipt of the notification.

[53] Figure 2B shows a flow diagram 220 illustrating a method for facilitating an un-authenticatable transaction according to various embodiments. More specifically, the flow diagram 220 shows a steps of generating QR code for use in the un-authenticatable transaction request.

[54] In step 222, an input indicating an amount to be transferred is received. In an example, the amount may be input by a keypad operationally coupled to a recipient device or a virtual keypad displayed on the recipient device. The recipient device may be configured to send the input to a payment network server.

[55] In step 224, a QR code may be generated in response to the receipt of the input. The QR code may indicate the amount to be transferred and the recipient account so that a user device can obtain the amount and the recipient account information by scanning the QR code.

[56] In step 226, the QR code indicating the amount to be transferred may be sent to a recipient device so that the recipient device can display the QR code to be scanned by the user device. The user device, by scanning the displayed QR code, can obtain the amount to be transferred and it is not necessary for the user to re-input the amount. For user's point of view, just checking the amount and confirming the information after scanning the QR code are sufficient to generate the transaction request.

[57] Figure 3 shows an exemplary transaction flow 300 illustrating a transaction flow between a merchant (or a recipient) and a consumer (or a user) according to various embodiments. The exemplary transaction flow 300 includes at least steps 302, 304, 306, 308, 310 and 312.

[58] Step 302 may include pre-step 1 for the merchant and pre-step 2 for the consumer, both pre-step 1 and pre-step 2 may be required prior to initiating the un-authenticatable transactions. In pre-step 1, the merchant may register with payment network server to create a QR code so that the merchant can display the QR code to the consumer. In pre-step 2, the consumer may install a digital wallet application in the consumer's device and create a wallet account for the digital wallet application and add payment vehicle information (or account information) such as debit/credit card account for use in the wallet account.

[59] In step 304, the merchant may display QR code to the customer who intends to buy a product or a service from the merchant. In an example, the QR code may be printed on a paper and the paper may be placed on a table. In an example, the QR code may be shown on a screen of the merchant's device.

[60] In step 306, the consumer may login to a digital wallet using wallet account created in the pre-step 2. In an example, the digital wallet application installed in the consumer's device is opened and the consumer may login to the digital wallet. Internet connectivity may not be required for login to the digital wallet.

[61] In step 308, the consumer may scan QR code of the merchant using the digital wallet application on the consumer's device. Further, the consumer may select payment vehicle such as debit/credit card for use in the transaction. In an example, one or more registered payment vehicles may be listed in the digital wallet so that the consumer can select one of the registered payment vehicles.

[62] In step 310, the payment network server may receive a transaction request from the consumer's device. The transaction request may include at least payer account such as consumer's account, payee account such as merchant's account, issuer, acquirer and the amount to be paid. In an example, the payment network server may call internal gateway to arrange the issuer to debit the amount from the consumer's account and the acquirer to credit the amount to the merchant's account.

[63] In step 312, the consumer and the merchant may get confirmation that transaction is successful. If there are errors in transferring the amount, the error message indicating failure of the transferring the amount may be received by the consumer and/or the merchant.

[64] Figure 4 shows an exemplary flow of existing registration procedures 400 for merchant 420 and an exemplary flow of registration procedures 410 for merchant 420 according to various embodiments. In the existing registration procedures 400, a merchant (or a recipient) 420 may contact an acquirer institute 422 for QR code in step 402. In response, the acquirer institute 422 may integrate with Software Development Kit (SDK) for QR code and generate a QR code for the merchant 420 in step 404. In step 406, the merchant 420 may obtain the QR code and pay for maintenance fees.

[65] On the other hands, in an exemplary flow of registration procedures 410, the merchant 420 may create account for the payment network server 424 such as wallet account and add details of payment vehicle such as card details and acquirer details in step 412. In response, the payment network server 424 may

generate instant QR code online in step 404. As the payment network server 424 may create QR code for each of the acquirers, the merchant 420 may not be required to contact each acquirer for QR code.

[66] Figure 5 shows an exemplary flow 500 for facilitating an un-authenticatable transaction between a merchant (or a recipient) 522 and a customer (or a user) 520 according to various embodiments. In step 502, the merchant 522 may display QR code to the customer 520. The QR code may be static and printed on a paper. Alternatively, the QR code may be dynamic and displayed on a screen of the merchant's device.

[67] In step 504, the customer 520 may open a digital wallet application installed on the customer's device. The customer's device may be a smart phone or a wearable device such as smart watch. And then, the customer 520 may scan the QR code using the customer's device and select one of the payment vehicles which are registered prior to the transaction. Conventionally, the customer's device is required to connect to Internet to be authenticated and proceed with such a payment. However, Internet connection is not required for the payment according to the present embodiments because a single use key may enable to authorize the un-authenticatable transaction from the customer's device.

[68] In step 506, the payment network server 524 may receive and verify the single use key and authorize the un-authenticatable transaction request from the customer's device. The payment network server 524 may call issuer access control server (ACS) and the amount indicated in the un-authenticatable transaction request may be transferred in a real-time manner by the issuer server. After receiving confirmation from the issuer, the payment network server 524 may send payment authorization to acquirer server 530 via Statement update API which is provided by the acquirer server 530 to allow the payment network server to send a request to update the records of the acquirer server, in which the acquirer 530 may be authorized to perform the payment to the merchant. Conventionally, the acquirer server 530 does not disclose how to update its records and statement update requests received by the acquirer server 530 may not be consistent with a format of the acquirer server. Statement update API is the one which makes the format of statement update requests to be consistent with the format of the acquirer server 530 and facilitate the update of records in the acquirer server 530.

Thus, statement update API is based on information provided by the acquirer server.

[69] In step 508, the acquirer 530 may receive payment details and merchant account details in accordance with the Statement update API to update the records and validate the merchant account and credit the amount to the merchant. After crediting the amount to the merchant 522, the merchant 522 may be informed of the credit via Short Message Service (SMS) or E-mail. As acquirer 530 can credit the amount to the merchant 522 before receiving the amount from the issuer, the merchant 522 can receive the amount without waiting for the transaction between the acquirer 530 and the issuer.

[70] Step 510, 512, 514, 516 and 518 may be performed after the merchant 522 receives the amount indicated in the transaction request. In step 510, the acquirer 530 may prepare a message and send to a service centre 528. In step 512, the service centre 528 may receive the message and send the message to the clearing centre 526. In step 514, the clearing centre 526 may send a remittance request to the issuer. In step 516, the issuer may send the remittance to the acquirer 530. In step 518, the acquirer 530 may receive the funds. In existing flow, the merchant 522 can receive the amount after step 518. However, in the present embodiment, the merchant 522 can receive the amount at step 508.

[71] Some portions of the description which follows are explicitly or implicitly presented in terms of algorithms and functional or symbolic representations of operations on data within a computer memory. These algorithmic descriptions and functional or symbolic representations are the means used by those skilled in the data processing arts to convey most effectively the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities, such as electrical, magnetic or optical signals capable of being stored, transferred, combined, compared, and otherwise manipulated.

[72] Unless specifically stated otherwise, and as apparent from the following, it will be appreciated that throughout the present specification, discussions utilizing terms such as “receiving”, “verifying”, “sending”, “determining”, “generating” or the like, refer to the action and processes of a computer system, or similar electronic device, that manipulates and transforms data represented as physical quantities within the

computer system into other data similarly represented as physical quantities within the computer system or other information storage, transmission or display devices.

[73] Figure 6 depicts an exemplary computing device 600, hereinafter interchangeably referred to as a computer system 600 or as a server 600, where one or more such computing devices 600 may be used to implement the server 104 shown in Figure 1B. The following description of the computing device 600 is provided by way of example only and is not intended to be limiting.

[74] As shown in Figure 6, the example computing device 600 includes a processor 604 for executing software routines. Although a single processor is shown for the sake of clarity, the computing device 600 may also include a multi-processor system. The processor 604 is connected to a communication infrastructure 606 for communication with other components of the computing device 600. The communication infrastructure 606 may include, for example, a communications bus, cross-bar, or network.

[75] The computing device 600 further includes a main memory 608, such as a random access memory (RAM), and a secondary memory 610. The secondary memory 610 may include, for example, a storage drive 612, which may be a hard disk drive, a solid state drive or a hybrid drive and/or a removable storage drive 614, which may include a magnetic tape drive, an optical disk drive, a solid state storage drive (such as a USB flash drive, a flash memory device, a solid state drive or a memory card), or the like. The removable storage drive 614 reads from and/or writes to a removable storage medium 644 in a well-known manner. The removable storage medium 644 may include magnetic tape, optical disk, non-volatile memory storage medium, or the like, which is read by and written to by removable storage drive 614. As will be appreciated by persons skilled in the relevant art(s), the removable storage medium 644 includes a computer readable storage medium having stored therein computer executable program code instructions and/or data.

[76] The computing device 600 also includes at least one communication interface 624. The communication interface 624 allows software and data to be transferred between computing device 600 and external devices via a communication path 626. In various embodiments of the inventions, the communication interface 624 permits data to be transferred between the computing device 600 and a data communication network, such as a public data or private data communication network. The communication interface 624 may be used to exchange data between different

computing devices 600 which such computing devices 600 form part an interconnected computer network. Examples of a communication interface 624 can include a modem, a network interface (such as an Ethernet card), a communication port (such as a serial, parallel, printer, GPIB, IEEE 1394, RJ45, USB), an antenna with associated circuitry and the like. The communication interface 624 may be wired or may be wireless. Software and data transferred via the communication interface 624 are in the form of signals which can be electronic, electromagnetic, optical or other signals capable of being received by communication interface 624. These signals are provided to the communication interface via the communication path 626.

[77] As shown in Figure 6, the computing device 600 further includes a display interface 602 which performs operations for rendering images to an associated display 630 and an audio interface 632 for performing operations for playing audio content via associated speaker(s) 634.

[78] As used herein, the term "computer program product" (or computer readable medium, which may be a non-transitory computer readable medium) may refer, in part, to removable storage medium 644, removable storage unit 622, a hard disk installed in storage drive 612, or a carrier wave carrying software over communication path 626 (wireless link or cable) to communication interface 624. Computer readable storage media (or computer readable media) refers to any non-transitory, non-volatile tangible storage medium that provides recorded instructions and/or data to the computing device 600 for execution and/or processing. Examples of such storage media include magnetic tape, CD-ROM, DVD, Blu-ray™ Disc, a hard disk drive, a ROM or integrated circuit, a solid state storage drive (such as a USB flash drive, a flash memory device, a solid state drive or a memory card), a hybrid drive, a magneto-optical disk, or a computer readable card such as a PCMCIA card and the like, whether or not such devices are internal or external of the computing device 600. Examples of transitory or non-tangible computer readable transmission media that may also participate in the provision of software, application programs, instructions and/or data to the computing device 600 include radio or infra-red transmission channels as well as a network connection to another computer or networked device, and the Internet or Intranets including e-mail transmissions and information recorded on Websites and the like.

[79] The computer programs (also called computer program code) are stored in main memory 608 and/or secondary memory 610. Computer programs can also be received via the communication interface 624. Such computer programs, when

executed, enable the computing device 600 to perform one or more features of embodiments discussed herein. In various embodiments, the computer programs, when executed, enable the processor 604 to perform features of the above-described embodiments. Accordingly, such computer programs represent controllers of the computer system 600.

[80] It is to be understood that the embodiment of Figure 6 is presented merely by way of example. Therefore, in some embodiments one or more features of the computing device 600 may be omitted. Also, in some embodiments, one or more features of the computing device 600 may be combined together. Additionally, in some embodiments, one or more features of the computing device 600 may be split into one or more component parts. The main memory 608 and/or the secondary memory 610 may serve(s) as the memory for the server 104 of Figure. 1B; while the processor 504 may serve as the processor of the server 104 of Figure. 1B.

[81] The present specification also discloses servers for performing the operations of the methods. Such servers may be specially constructed for the required purposes, or may comprise a computer or other device selectively activated or reconfigured by a computer program stored in the computer. The algorithms and displays presented herein are not inherently related to any particular computer or other apparatus. Various machines may be used with programs in accordance with the teachings herein. Alternatively, the construction of more specialized apparatus to perform the required method steps may be appropriate. The structure of a computer will appear from the description below.

[82] In addition, the present specification also implicitly discloses a computer program, in that it would be apparent to the person skilled in the art that the individual steps of the method described herein may be put into effect by computer code. The computer program is not intended to be limited to any particular programming language and implementation thereof. It will be appreciated that a variety of programming languages and coding thereof may be used to implement the teachings of the disclosure contained herein. Moreover, the computer program is not intended to be limited to any particular control flow. There are many other variants of the computer program, which can use different control flows without departing from the spirit or scope of the invention.

[83] Furthermore, one or more of the steps of the computer program may be performed in parallel rather than sequentially. Such a computer program may be stored on any computer readable medium. The computer readable medium may include storage devices such as magnetic or optical disks, memory chips, or other storage devices suitable for interfacing with a computer. The computer readable medium may also include a hard-wired medium such as exemplified in the Internet system, or wireless medium such as exemplified in the GSM mobile telephone system. The computer program when loaded and executed on such a computer effectively results in a server that implements the steps of the preferred method.

[84] It will be appreciated by a person skilled in the art that numerous variations and/or modifications may be made to the present invention as shown in the specific embodiments without departing from the spirit or scope of the invention as broadly described. The present embodiments are, therefore, to be considered in all respects to be illustrative and not restrictive.

CLAIMS

What is claimed is:

1. A server for facilitating an un-authenticatable transaction for an Internet connection capable user device when the user device is not in Internet connection with the server, the server comprising:

at least one processor; and

at least one memory including computer program code,

the at least one memory and the computer program code configured to, with the at least one processor, cause the server at least to:

receive, from the user device, a token and a transaction request, the token being one that was generated when the user device was in Internet connection with the server and the transaction request indicating an amount, a user account and a recipient account to be used for the un-authenticatable transaction;

verify if the token corresponds to one that has been registered for the user account; and

send, to an issuer server, an authorization to transfer the amount indicated in the transaction request from the user account in response to the verification of the token.

2. The server in accordance with claim 1, wherein the at least one memory and the computer program code configured to, with the at least one processor, cause the server further to:

receive, from the issuer server, a notification indicating that the amount was transferred from the user account; and

send, to an acquirer server, an authorization to transfer the amount indicated in the transaction request to the recipient account in response to the notification.

3. The server in accordance with claim 1, wherein the at least one memory and the computer program code configured to, with the at least one processor, cause the server further to:

determine a time period based on a time at which the token was generated and a time at which the transaction request is received,

wherein the authorization is sent to the issuer server in response to the determined time period.

4. The server in accordance with claim 1, wherein the at least one memory and the computer program code configured to, with the at least one processor, cause the server further to:

verify if the user account is one that is permitted to transfer the amount indicated in the transaction request,
wherein the authorization is sent to the issuer server in response to the verification of the user account.

5. The server in accordance with claim 1, wherein the at least one memory and the computer program code configured to, with the at least one processor, cause the server further to:

generate a QR code indicating the recipient account.

6. The server in accordance with claim 1, wherein the at least one memory and the computer program code configured to, with the at least one processor, cause the server further to:

receive, from a recipient device, an input indicating the amount to be transferred;
generate a QR code in response to the receipt of the input from the recipient device; and
send, to the recipient device, the generated QR code indicating the amount to be transferred.

7. The server in accordance with claim 1, wherein the at least one memory and the computer program code configured to, with the at least one processor, cause the server further to:

connect to an application executing on the user device to transfer the token and the transaction request when the user device is in virtual private network (VPN) communication with the server.

8. The server in accordance with claim 1, wherein the at least one memory and the computer program code configured to, with the at least one processor, cause the server further to:

determine a credibility score of the recipient account based on a transaction history of the recipient account,

wherein the authorization is sent to the issuer server in response to the determined credibility score of the recipient account.

9. The server in accordance with claim 1, wherein the at least one memory and the computer program code configured to, with the at least one processor, cause the server further to:

receive, from the user device, a request for the token when the user device is in Internet connection with the server;

generate the token in response to the receipt of the request from the user device; and

send, to the user device, the generated token for the un-authenticatable transaction.

10. A method for facilitating an un-authenticatable transaction for an Internet connection capable user device when the user device is not in Internet connection with a server, comprising:

receiving, from the user device, a token and a transaction request, the token being one that was generated when the user device was in Internet connection with the server and the transaction request indicating an amount, a user account and a recipient account to be used for the un-authenticatable transaction;

verifying if the token corresponds to one that has been registered for the user account; and

sending, to an issuer server, an authorization to transfer the amount indicated in the transaction request from the user account in response to the verification of the token.

11. The method in accordance with claim 10, further comprising:

receiving, from the issuer server, a notification indicating that the amount was transferred from the user account; and

sending, to an acquirer server, an authorization to transfer the amount indicated in the transaction request to the recipient account in response to the notification.

12. The method in accordance with claim 10, further comprising:

determining a time period based on a time at which the token was generated and a time at which the transaction request is received,

wherein the authorization is sent to the issuer server in response to the determined time period.

13. The method in accordance with claim 10, further comprising:
verifying if the user account is one that is permitted to transfer the amount indicated in the transaction request,
wherein the authorization is sent to the issuer server in response to the verification of the user account.
14. The method in accordance with claim 10, further comprising:
generating a QR code indicating the recipient account.
15. The method in accordance with claim 10, further comprising:
receiving, from a recipient device, an input indicating the amount to be transferred;
generating a QR code in response to the receipt of the input from the recipient device; and
sending, to the recipient device, the generated QR code indicating the amount to be transferred.
16. The method in accordance with claim 10, further comprising:
connecting to an application executing on the user device to transfer the token and the transaction request when the user device is in virtual private network (VPN) communication with the server.
17. The method in accordance with claim 10, further comprising:
determining a credibility score of the recipient account based on a transaction history of the recipient account,
wherein the authorization is sent to the issuer server in response to the determined credibility score of the recipient account.
18. The method in accordance with claim 10, further comprising:
receiving, from the user device, a request for the token when the user device is in Internet connection with the server;
generating the token in response to the receipt of the request from the user device;

sending, to the user device, the generated token for the un-authenticatable transaction.