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.

[1] 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.

[2] 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

[3] According to a first aspect of the present disclosure, 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 determine a time period based on a time at which the token was generated and a time at which the transaction request is received; 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 and the determined time period. 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.

[4] According to a second aspect of the present disclosure, 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 determining a time period based on a time at which the token was generated and a time at which the transaction request is received; 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 and the determined time period. The method comprises 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

BRIEF DESCRIPTION OF THE DRAWINGS

[5] 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:

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

[7] 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;

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

[9] 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;

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

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:

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.

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:

generate a QR code indicating the recipient 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:

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.

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:

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.

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:

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.

8. 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 determining a time period based on a time at which the token was generated and a time at which the transaction request is received; 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 and the determined time period, the method 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.

9. The method in accordance with claim 8, 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.

10. The method in accordance with claim 8, 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.

11. The method in accordance with claim 8, further comprising:

generating a QR code indicating the recipient account.

12. The method in accordance with claim 8, 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.

13. The method in accordance with claim 8, 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.

14. The method in accordance with claim 8, 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.