

WHAT IS CLAIMED IS:

1. A computer-implemented method comprising:

generating a mobile-One Time Password (m-OTP) with a mobile application configured on a cardholder's device without using a network connection, the m-OTP generated based on at least one algorithm;

receiving, by an acquirer system, a transaction message from a merchant system, the transaction message comprising the m-OTP, transaction information for authorization, and an identifier differentiating the transaction message from other types of transaction messages not including the m-OTP;

transmitting, by the acquirer system, the transaction message to a directory server, the transaction message comprising the m-OTP and the transaction information for authorization;

receiving, by the directory server, the transaction message comprising the transaction information for authorization, from the acquirer system, wherein the transaction message comprises at least the m-OTP, wherein the m-OTP was submitted into the merchant system, and wherein the merchant system provided the transaction message to the acquirer system for completing a transaction;

differentiating, by the directory server, the transaction message from a plurality of transaction messages based on the identifier;

after differentiating the transaction message from the plurality of transaction messages, transmitting, by the directory server, the transaction message to an issuer system;

authenticating, by the issuer system, the cardholder based on the m-OTP retrieved from the transaction message and a second m-OTP generated by the issuer system using the at least one algorithm, wherein the mobile application is an issuer mobile application associated with the issuer system;

authorizing, by the issuer system, the transaction in response to authenticating the cardholder by matching the m-OTP generated by the mobile application and the second m-OTP generated by the issuer system using the at least one algorithm;

receiving, by the directory server, a response message comprising a result of authorization of the transaction message from the issuer system, the

response message configured to display a message on a merchant checkout page hosted by the merchant system; and

providing, by the directory server, the response message to the merchant system via the acquirer system.

2. The method as claimed in claim 1, wherein the identifier is inserted in one of a Message Type Identifier (MTI), a bitmap, or data elements of the transaction message.

3. The method as claimed in claim 1, wherein the m-OTP is a time-based password.

4. The method as claimed in claim 1, wherein the transaction message is formatted according to ISO8583 standard.

5. The method as claimed in claim 1, wherein the transaction information comprises at least one of a primary account number of the cardholder, a processing code, a transaction amount, a transaction date and time, an acquirer system identification code, a currency code, an issuer system identification code, a mode of authentication comprising the m-OTP, generated by the issuer system, a static password, and biometric pattern information.

6. The method as claimed in claim 1, wherein the response message is generated based on authenticating the m-OTP and authorizing the transaction message.

7. The method as claimed in claim 1, wherein the transaction message includes a payer authentication request (PAREq) message.

8. A computer program product for authorizing transactions, the computer program product comprising at least one non-transitory computer-readable medium including one or more instructions that when executed by at least one processor, causes the at least one processor to:

generate a mobile-One Time Password (m-OTP) with a mobile application configured on a cardholder's device without using a network connection, the m-OTP generated based on at least one algorithm;

receive, by an acquirer system, a transaction message from a merchant system, the transaction message comprising transaction information for authorization, the m-OTP, and an identifier differentiating the transaction message from other types of transaction messages not including the m-OTP;

transmit, by the acquirer system, the transaction message to a directory server, the transaction message comprising the m-OTP and the transaction information for authorization;

receive, by the directory server, the transaction message comprising the transaction information for authorization, from the acquirer system, wherein the transaction message comprises at least the m-OTP, and wherein the merchant system provided the transaction message by the acquirer system for completing a transaction;

differentiate, by the directory server, the transaction message from a plurality of transaction messages based on the identifier;

after differentiating the transaction message from the plurality of transaction messages, transmit, by the directory server, the transaction message to an issuer system;

authenticate, by the issuer system, the cardholder based on the m-OTP retrieved from the transaction message and a second m-OTP generated by the issuer system using the at least one algorithm, wherein the mobile application is an issuer mobile application associated with the issuer system;

authorize, by the issuer system, the transaction in response to authenticating the cardholder by matching the m-OTP generated by the mobile application and the second m-OTP generated by the issuer system using the at least one algorithm;

receive, by the directory server, a response message comprising a result of authorization of the transaction message from the issuer system, the response message configured to display a message on a merchant checkout page hosted by the merchant system; and

provide, by the directory server, the response message to the merchant system via the acquirer system.

9. The directory server as claimed in claim 8, wherein the at least one processor is configured to send the transaction message to the issuer system formatted according to ISO8583.

10. The directory server as claimed in claim 8, wherein the at least one processor receives the transaction message comprising the identifier inserted in one of a Message Type Identifier (MTI), a bitmap, or data elements.

11. The directory server as claimed in claim 8, wherein the at least one processor receives the response message generated based on authenticating the m-OTP and authorizing the transaction message.

12. The directory server as claimed in claim 8, wherein the transaction message includes a payer authentication request (PAREq) message.

13. A computer-implemented method of authorizing transactions, comprising:

receiving, by a merchant system, a mobile-One Time Password (m-OTP) as input for initiating a transaction, wherein the m-OTP was generated by an issuer mobile application, which is installed in a cardholder's device, without using a network connection, the m-OTP generated based on at least one algorithm;

generating, by the merchant system, a transaction message comprising an identifier and the m-OTP, wherein the identifier indicates that the transaction message comprises the m-OTP and is differentiated from other types of transaction messages that do not comprise an m-OTP;

providing, by the merchant system, the transaction message comprising the m-OTP to an acquirer system, wherein the acquirer system includes an authentication request in the transaction message and provides the transaction message to a directory server;

differentiating, by the directory server, the transaction message from a plurality of transactions based on the identifier;

after differentiating the transaction message from the plurality of transaction messages, transmitting, by the directory server, the transaction message to an issuer system, wherein the issuer system authenticates a cardholder based on the m-OTP retrieved from the transaction message and a second m-OTP generated by the issuer system using the at least one algorithm, wherein the transaction is authorized in response to authenticating the cardholder by matching the m-OTP generated by the mobile application and the second m-OTP generated by the issuer system using the at least one algorithm, and wherein a response message comprising a result of authorization is generated by the issuer system;

receiving, by the merchant system, the response message from the directory server via the acquirer system; and

displaying, by the merchant system, a message on a merchant checkout page hosted by the merchant system, wherein the response message is configured to display the message on the merchant checkout page hosted by the merchant system.

14. The method as claimed in claim 13, wherein the transaction message is formatted according to ISO8583 standard, and wherein the transaction message includes a payer authentication request (PAREq) message.

15. The method as claimed in claim 13, wherein the identifier is inserted in one of a Message Type Identifier (MTI), a bitmap, or data elements of a transaction message format.

16. The method as claimed in claim 13, wherein the m-OTP is a time-based password.