Claims:

1. A transaction authorization method, comprising:

generating, by a server, a master authentication code based on an authorization request for a transaction, wherein a user initiates the transaction from an account by using a transaction application of a plurality of transaction applications installed on a user-computing device;

splitting, by the server, the master authentication code into a first authentication code and a second authentication code, such that when a logical operation is performed between the first authentication code and the second authentication code, the master authentication code is obtained, the logical operation being an XOR operation, an XNOR operation, or an inversion operation;

communicating, by the server, the first authentication code to the transaction application and the second authentication code to the user by way of registered contact information linked to the account, wherein the second authentication code is accessible to another transaction application of the plurality of transaction applications at the user-computing device;

receiving, by the server, a response code from a corresponding at least one of the plurality of transaction applications, the at least one of the plurality of transaction applications comprising the transaction application, wherein the transaction application generates the response code based on the first authentication code and the second authentication code;

determining, by the server, whether the master authentication code itself matches the response code generated by and received from the transaction application; and

processing, by the server, the transaction based on a match between the response code and the master authentication code.

2. The transaction authorization method of claim 1, further comprising receiving, by the server, the authorization request from the transaction application installed on the user-computing device.

3. The transaction authorization method of claim 1, wherein the master authentication code is a Quick Response code (QR CODE), and wherein the first authentication code is a first portion of the QR CODE and the second authentication code is a second portion of the QR CODE.

4. The transaction authorization method of claim 1, wherein the registered contact information includes at least one of a registered contact number or a registered email address of the user.

5. The transaction authorization method of claim 1, wherein the user submits the second authentication code to the transaction application.

6. The transaction authorization method of claim 1, wherein the transaction application retrieves the second authentication code by accessing a message repository of the user-computing device.

7. The transaction authorization method of claim 1, wherein at least one of the first authentication code or the second authentication code includes position information, and wherein the transaction application generates the response code by merging the first authentication code and the second authentication code based on the position information.

8. The transaction authorization method of claim 1, wherein determining whether the master authentication code itself matches the response code comprises comparing, by the server, the response code with the master authentication code for processing the transaction.

9. The transaction authorization method of claim 1, further comprising declining, by the server, the transaction based on a mismatch between the response code and the master authentication code.

10. A transaction authorization system, comprising:

a server comprising:

a memory configured to store a plurality of authorization requests for a plurality of transactions; and

a processor that communicates with the memory, wherein the processor is configured to:

generate a master authentication code based on an authorization request for a transaction of the plurality of transactions, wherein a user initiates the

transaction from an account by using a transaction application of a plurality of transaction applications installed on a user-computing device;

split the master authentication code into a first authentication code and a second authentication code, such that when a logical operation is performed between the first authentication code and the second authentication code, the master authentication code is obtained, the logical operation being an XOR operation, an XNOR operation, or an inversion operation;

communicate the first authentication code to the transaction application and the second authentication code to the user by way of registered contact information linked to the account, wherein the second authentication code is accessible to another transaction application of the plurality of transaction applications at the user-computing device;

receive a response code from a corresponding at least one of the plurality of transaction applications, the at least one of the plurality of transaction applications comprising the transaction application, wherein the transaction application generates the response code based on the first authentication code and the second authentication code;

determine whether the master authentication code itself matches the response code generated by and received from the transaction application; and

process the transaction based on a match between the response code and the master authentication code.

11. The transaction authorization system of claim 10, wherein the processor is further configured to receive the authorization request from the transaction application installed on the user-computing device.

12. The transaction authorization system of claim 10, wherein the master authentication code is a Quick Response code (QR CODE), and wherein the first authentication code is a first portion of the QR CODE and the second authentication code is a second portion of the QR CODE.

13. The transaction authorization system of claim 10, wherein the registered contact information includes at least one of a registered contact number or a registered email address of the user.

14. The transaction authorization system of claim 10, wherein the user submits the second authentication code to the transaction application.

15. The transaction authorization system of claim 10, wherein the transaction application retrieves the second authentication code by accessing a message repository of the user-computing device.

16. The transaction authorization system of claim 10, wherein at least one of the first authentication code or the second authentication code includes position information, and wherein the transaction application generates the response code by merging the first authentication code and the second authentication code based on the position information.

17. The transaction authorization system of claim 10, wherein the processor is further configured to compare the response code with the master authentication code for processing the transaction.

18. The transaction authorization system of claim 10, wherein the processor is further configured to decline the transaction based on a mismatch between the response code and the master authentication code.

19. A method for conducting transactions, the method comprising:

transmitting, by a transaction application of a plurality of transaction applications installed on a user-computing device, an authorization request for a transaction to a server, wherein a user initiates the transaction from an account by using the transaction application, and wherein the server generates a master authentication code based on the authorization request;

receiving, by the transaction application, a first authentication code from the server, wherein the server splits the master authentication code into the first authentication code and a second authentication code, such that when a logical operation is performed between the first authentication code and the second authentication code, the master authentication code is

obtained, the logical operation being an XOR operation, an XNOR operation, or an inversion operation;

receiving, by the transaction application, the second authentication code from the user, wherein the server communicates the second authentication code to the user by way of registered contact information linked to the account, wherein the second authentication code is accessible to another transaction application of the plurality of transaction applications at the user-computing device;

generating, by the transaction application, a response code based on the first authentication code and the second authentication code, wherein any other transaction application of the plurality of transaction applications that has unauthorized access to the second authentication code cannot generate a response code that matches the master authentication code without receiving the first authentication code from the server; and

transmitting, by the transaction application, the response code to the server for processing the transaction including whether the master authentication code itself matches the response code, wherein the server processes the transaction based on a match between the response code and the master authentication code.