CLAIMS

1. A method for authenticating and authorizing a transaction involving a terminal provider of a product or a service and a mobile application of a user mobile device wherein:

- during a registration process of the mobile application to a server:
- operating the server to generates a set of transaction unpredictable numbers,
- operating the server to send said generated set of transaction unpredictable numbers to the mobile application,
- during the authentication and authorization of the transaction:
- operating the mobile application to select a stored unused transaction unpredictable number, said selected unused transaction unpredictable number allowing to identify said transaction,
- operating the mobile application to elaborate a transaction authorization request message from the selected transaction unpredictable number,
- operating the mobile application to encode the authorization request into a simplex communication data,
- operating the terminal provider to receive and decode the simplex communication data,
- operating the terminal provider to send to the server, the decoded simplex communication data for authentication and authorization of the transaction,
- operating the server to verify a match of a transaction unpredictable number between the content of the decoded transaction authorization request message and the server transaction unpredictable number database,
- if the verification is successful, operating the server to add the matched transaction unpredictable number to the authorization request message,
- operating the server to send the transaction authorization request to an issuer,
- operating the server to receives from the issuer receiving the transaction authorization result indicating whether or not said transaction is authenticated and authorized,
- operating the server to forward the transaction authorization result to the terminal provider.

2. The method according to the previous claim, wherein to receive the simplex communication data, a scanner terminal of the provider scans the encoded authorization request.

3. The method according to any previous claims, wherein the simplex communication data is an image code such a QR code or a barcode, this image code being displayed on the user mobile device to be scanned by the provider and sent to the server.

4. The method according to claims 1 or 2, wherein the simplex communication data is a modulated sound, a modulated vibration or a NFC tag message.

5. The method according to any previous claims, wherein when the selected transaction unpredictable number is added to the elaborated transaction authorization request message :

- comparing the received selected transaction unpredictable number to the recovered transaction unpredictable number,
- if the comparison is successful, adding the recovered transaction unpredictable number to the authorization request and sending it to the issuer.

6. The method according to any previous claims wherein the unused transaction unpredictable number is selected according to a pre-determined sequence and wherein the transaction unpredictable number is recovered by the server according to a unique identifier of the user and the pre-determined sequence.

7. The method according to claims 1 to 5, wherein the transaction unpredictable number is recovered by the server from an unique identifier of the user, an index associated to the selected transaction unpredictable number which is added to the authorization request and the pre-determined sequence.

8. The method according to claims 1 to 5, wherein the unused transaction unpredictable number is selected randomly and wherein an index is associated to said selected transaction unpredictable number and wherein the transaction unpredictable number is recovered by the server from a unique identifier of the user and the index associated to the selected transaction unpredictable number.

9. The method according to any previous claims, wherein the transaction unpredictable number is marked as used in the storage after the selection step and the recovery step.

10. The method according to the previous claim, wherein when the transaction unpredictable numbers stored in the mobile payment application are all marked as used then a new set of transaction unpredictable numbers is generated by the server and sent to the mobile application for storage.

11. The method according to any previous claims, wherein the transmission of the generated set of transaction unpredictable numbers from the server to the mobile payment application is protected:

- by applying an encryption algorithm which involves key(s) shared between the server and the mobile payment application, and/or
- by applying an integrity algorithm which involves key(s) shared between the server and the mobile payment application.

12. The method according to any previous claims, wherein the mobile application and the set of transaction unpredictable numbers are stored into a secure element of the mobile device.

13. The method according to any previous claims, wherein the server and the issuer are the same entity.

14. The method according to the previous claims, wherein the transaction authorization request message comprises a transaction cryptogram generated from an amount of the transaction inputted by the user on the mobile device, the selected transaction unpredictable number, user's financial data, various keys and data elements defined by the transaction standard.

15. The method according to any previous claims, wherein the mobile device is a cellular or wireless phone, a tablet, a smartphone, a personal digital assistance (PDA), a pager, a portable computers.

CLAIMS

1. A method for authenticating a transaction involving a terminal provider of a product or a service and a mobile application of a user mobile device wherein:

- operating the mobile device to receive and store a generated set of transaction unpredictable numbers on a server,

during the authentication of the transaction:

- operating the mobile application to select according to a pre-determined sequence of selection an transaction unpredictable number from the stored set of transaction unpredictable numbers and to associate said selected transaction unpredictable number to said transaction,

- the mobile application computes from at least the selected transaction unpredictable number associated to the transaction a cryptogram of transaction authorization request,

- operating the mobile application to encode the cryptogram into an payment code, said payment code being sent from the mobile application to the terminal provider for payment,

- said terminal provider comprising means configured to decode the received payment code and send it to the server for authentication, the transaction unpredictable number of the decoded payment code is compared to a set of transaction unpredictable numbers previously stored in the server database, if the comparison is successful the transaction is authenticated.

2. The method according to the previous claim, wherein during the authentication of the transaction unpredictable number the method comprises the following step:

- from the decoded payment code, the server recovers a transaction unpredictable number from the set of transaction unpredictable numbers previously stored in its database,

- the recovered transaction unpredictable number is compared to the received selected transaction unpredictable number in the decoded cryptogram,

- if the comparison is successful, adding the recovered transaction unpredictable number to the cryptogram and sending it from the server to an issuer for authorization of the transaction.

3. The method according to any previous claims, wherein the payment code is an image code such a QR code or a barcode, this image code being displayed on the user mobile device to be scanned by the terminal provider and sent to the server.

4. The method according to claims 1 or 2, wherein the payment code is a modulated sound, a modulated vibration or a NFC tag message.

5. The method according to claims 2 to 4, wherein the transaction unpredictable number is selected according to a pre-determined sequence and wherein the transaction unpredictable number is recovered by the server according to a unique identifier of the user added to the cryptogram authorization request and the pre-determined sequence.

6. The method according to claims 2 to 5, wherein the transaction unpredictable number is recovered by the server from an unique identifier of the user, an index associated to the selected transaction unpredictable number which are added to the cryptogram authorization request and the pre-determined sequence.

7. The method according to claims 2 to 5, wherein the transaction unpredictable number is selected randomly and wherein an index is associated to said selected transaction unpredictable number and wherein a transaction unpredictable number is recovered by the server from a unique identifier of the user and the index associated to the selected transaction unpredictable number added to the cryptogram authorization request.

8. The method according to any previous claims, wherein the transaction unpredictable number is marked as used in the storage after the selection step and the recovery step.

9. The method according to any the previous claim, wherein when the transaction unpredictable numbers stored in the mobile payment application are all marked as used then a new set of transaction unpredictable numbers is generated by the server and sent to the mobile application for storage.

10. The method according to any previous claims, wherein the transmission of the generated set of transaction unpredictable numbers from the server to the mobile payment application is protected:

- by applying an encryption algorithm which involves key(s) shared between the server and the mobile payment application, and/or
- by applying an integrity algorithm which involves key(s) shared between the server and the mobile payment application.

11. The method according to any previous claims, wherein the mobile application and the set of transaction unpredictable numbers are stored into a secure element of the mobile device.

12. The method according to any previous claims, wherein the server and the issuer are the same entity.

13. The method according to any previous claims, wherein the transaction is a financial transaction which being conform to EMV transaction standard, Mifare transaction standard or Calypso transaction standard.

14. The method according to the previous claim, wherein the cryptogram transaction authorization request message is generated from an amount of the transaction inputted by the user on the mobile device, the selected transaction unpredictable number, user's financial data, various keys and data elements defined by the transaction standard.

15. The method according to any previous claims, wherein the mobile device is a cellular or wireless phone, a tablet, a smartphone, a personal digital assistance (PDA), a pager, a portable computers.

16. System for authenticating and authorizing a transaction involving a terminal provider of a product or a service and a mobile application of a user mobile device according to any of the previous claims.