WE CLAIM:

~~1. A method for establishing secure communication between a terminal device (105) and a target system (103), the method comprising:~~

~~receiving, by a communication verification system (101), a communication request (107) from the terminal device (105) for establishing communication between the terminal device (105) and the target system (103), wherein the communication request (107) is generated at the terminal device (105) when a user initiates a transaction at the terminal device (105);~~

~~verifying, by the communication verification system (101), the terminal device (105) and the target system (103) based on predetermined registration details (211), for validating the communication request (107);~~

~~signaling, by the communication verification system (101), the terminal device (105) for generating a unique Quick Response (QR) code (111), corresponding to the communication request (107), upon validating the communication request (107); and~~

~~establishing, by the communication verification system (101), the secure communication between the terminal device (105) and the target system (103) when the QR code (111) is processed by a predetermined verification interface configured in a user device (113), associated with the user.~~

~~2. The method as claimed in claim 1, wherein the communication request (107) comprises a transaction request, a unique transaction identifier and transaction-specific information.~~

~~3. The method as claimed in claim 1, wherein the predetermined registration details (211) comprises a terminal identifier, a target system (103) identifier, a Virtual Private Address (VPA) of the terminal device (105), and a target channel identifier.~~

~~4. The method as claimed in claim 1, wherein the unique QR code (111) generated by the terminal device (105) is displayed on a display interface (235) associated with the terminal device (105).~~

~~5. The method as claimed in claim 1, wherein processing the QR code (111) comprises:~~

Commented [SNP1]:
Method claims 1-7 have been omitted to overcome objection u/s 3(k).

~~scanning the QR code (111) through the predetermined verification interface configured in the user device (113);~~

~~decoding, through the predetermined verification interface, the QR code (111) for extracting information related to the transaction;~~

~~generating, using the predetermined verification interface, a transaction payload (115) corresponding to the information related to the transaction; and~~

~~transmitting, through the user device (113), the transaction payload (115) to the target system (103) for authorizing the transaction.~~

~~6. The method as claimed in claim 5, wherein the information related to the transaction comprises name of the user, a unique identifier of the user, a user specific VPA, and the predetermined registration details (211).~~

~~7. The method as claimed in claim 5, wherein authorizing the transaction comprises:~~

~~receiving, by the communication verification system (101), the information related to the transaction from the terminal device (105);~~

~~receiving, by the communication verification system (101), a transaction authorization message from the target system (103), wherein the transaction authorization message is generated at the target system (103) upon validating the transaction payload (115) received from the terminal device (105); and~~

~~comparing, by the communication verification system (101), the information related to the transaction with the transaction authorization message for authorizing the transaction between the terminal device (105) and the target system (103).~~

1. A communication verification system (101) for establishing secure communication between a terminal device (105) and a target system (103), the communication verification system (101) comprising:

a processor (203); and

a memory (205), communicatively coupled to the processor (203), wherein the memory (205) stores processor-executable instructions, which on execution cause the processor (203) to:

receive a communication request (107) from the terminal device (105) to establish communication between the terminal device (105) and the target system (103), wherein the communication request (107) is generated at the terminal device (105) when a user initiates a transaction at the terminal device (105);

verify the terminal device (105) and the target system (103) based on predetermined registration details (211) to validate the communication request (107);

signal the terminal device (105) to generate a unique Quick Response (QR) code (111), corresponding to the communication request (107), upon validating the communication request (107); and

establish the secure communication between the terminal device (105) and the target system (103) when the QR code (111) is processed by a predetermined verification interface configured in a user device (113), associated with the user.

2. The communication verification system (101) as claimed in claim ~~9~~1, wherein the communication request (107) comprises a transaction request, a unique transaction identifier and transaction-specific information.

3. The communication verification system (101) as claimed in claim ~~9~~1, wherein the predetermined registration details (211) comprises a terminal identifier, a target system (103) identifier, a Virtual Private Address (VPA) of the terminal device (105), and a target channel identifier.

4. The communication verification system (101) as claimed in claim ~~9~~1, wherein the processor (203) displays the unique QR code (111) generated by the terminal device (105) on a display interface (235) associated with the terminal device (105).

5. The communication verification system (101) as claimed in claim ~~9~~1, wherein to process the QR code (111), the processor (203) is configured to:

scan the QR code (111) through the predetermined verification interface configured in the user device (113);

decode, through the predetermined verification interface, the QR code (111) for extracting information related to the transaction;

generate, using the predetermined verification interface, a transaction payload (115) corresponding to the information related to the transaction; and

transmit, through the user device (113), the transaction payload (115) to the target system (103) for authorizing the transaction.

6. The communication verification system (101) as claimed in claim ~~1~~3~~5~~, wherein the ~~information related to the transaction~~ transaction payload (115) comprises name of the user, a unique identifier of the user, a user-specific VPA, and the predetermined registration details (211).

Commented [SNP2]:
Support:

Paragraph 2 on Page No. 8 of the complete specification.

7. The communication verification system (101) as claimed in claim ~~1~~3~~5~~, wherein to authorize the transaction, the processor (203) is configured to:

receive the information related to the transaction from the terminal device (105);

receive a transaction authorization message from the target system (103), wherein the transaction authorization message is generated at the target system (103) upon validating the transaction payload (115) received from the terminal device (105); and

compare the information related to the transaction with the transaction authorization message to authorize the transaction between the terminal device (105) and the target system (103).

~~8. A terminal device (105) comprising:~~

~~a data reception module (231) to receive a transaction initiation request from a user;~~

~~a communication request generation module (232) to generate a communication request (107) upon receiving the transaction initiation request;~~

~~a Quick Response (QR) code generator (233) for generating a unique QR code (111) corresponding to the communication request (107); and~~

~~a display interface (235) for displaying the QR code (111).~~