What is claimed is:

1. A method of conducting a secure transaction between a merchant and a customer, the method including:

initiating a first secure monitored session between a merchant terminal and a transaction server;

wherein the first secure monitored session refers to a mutually authenticated connection in which sensitive data is encrypted;

during the first secure monitored session, capturing a customer primary account number (PAN) at the merchant terminal, the customer primary account number being associated with a customer account at a financial institution;

wherein the PAN represents a debit or credit card number, a tokenized version thereof, or an encrypted version thereof that is associated with the customer account at the financial institution;

sending a request for a transaction from the merchant terminal to the transaction server, the request including the customer PAN and a transaction amount;

generating, at the transaction server, a transaction identifier (TRANS-ID) that is unique to the transaction and a timestamp (TIMESTAMP1) corresponding to a time when the transaction was requested or initiated, and sending TRANS-ID and TIMESTAMP1 to the merchant terminal;

encoding the TRANS-ID and TIMESTAMP1 in a visual representation for presentation on a display;

allowing capture of the visual representation by a camera on a customer device;

in response to the capture of the visual representation on the customer device, launching a customer app on the customer device, wherein the customer app is configured to:

initiate a second secure monitored session between the customer device and the transaction server, wherein the second secure monitored session refers to a mutually authenticated connection which provides a safe window in which a PIN number associated with the customer PAN is entered;

control the customer device to present the customer with a user interface to enter the PIN number associated with the customer PAN;

generate a PIN block for the PIN number using a random primary account number downloaded from the server and transmit the PIN block to the transaction server for verification;

obtaining, at the transaction server, a verification or rejection of the transaction from the financial institution associated with the customer account; and

transmitting the verification or rejection of the transaction to the merchant terminal to complete the transaction.

2. The method according to claim 1 wherein the merchant terminal is authorized to communicate with the transaction server via a merchant app that is stored on the merchant terminal using a first unique random number (MA-RAND1) as a temporary merchant identifier in an onboarding process between the merchant terminal and the transaction server.

3. The method according to claim 2 wherein the step of initiating the first secure monitored session includes:

i) creating, at the merchant app, a second unique random number (MA-RAND2);

ii) generating a session key (MA-SESSION-KEY) using MA-RAND2 and a seed value for the merchant app version as key parameters;

iii) calculating a key check value (KCV) of MA-SESSION-KEY;

iv) sending MA-RAND1 XOR MA-RAND2 and KCV from the merchant app to the transaction server, where XOR represents a bitwise exclusive OR function;

v) calculating MA-SESSION-KEY at the transaction server and verifying the KCV against the KCV received from the merchant app;

vi) sending white box cryptography tables from the transaction server to the merchant app, wherein the white box cryptography tables are encrypted using MA-SESSION-KEY, wherein the white box cryptography tables represent bytes used to source a white box cryptography session;

vii) decrypting, at the merchant app, the white box cryptography tables using MA-SESSION-KEY and replacing the current white box cryptography tables with the new decrypted tables;

viii) replacing MA-RAND1 with MA-RAND2; and

ix) repeating steps vi) to viii) at predefined time intervals during the first secure monitored session.

4. The method according to claim 3 wherein the MA-SESSION-KEY is generated by applying a one way function to both MA-RAND2 and the seed value.

5. The method according to claim 3 or claim 4 wherein, if KCV calculated at the transaction server mismatches KCV received from the merchant app, the transaction server replaces MA-RAND1 with an alternate unique random number (MA-RAND1-BAK).

6. The method according to claim 5 wherein , if the KCV calculated at the transaction server mismatches with the KCV received from the merchant app, then an error condition is raised.

7. The method according to claim 6 wherein, after a predefined number of error conditions, the merchant app requests that the server generate an alternative first random number MA-RAND1.

8. The method according to any one of claims 3 to 7 wherein the white box cryptography tables include an embedded single use key.

9. The method according to claim 8 wherein the single use key is an AES-256 Symmetric single use key.

10. The method according to any one of claims 3 to 9 wherein the white box cryptography tables are replaced at time intervals in the range of 1 to 5 seconds.

11. The method according to claim 10 wherein the white box cryptography tables are replaced at time intervals of every 2 seconds.

12. The method according to any one of claims 2 to 11 wherein, during the first secure monitored session, the merchant app executes a check routine to check for signs of tampering by examining the integrity of the operating system, memory and/or stored code and files of the merchant terminal.

13. The method according to claim 12 wherein the merchant app executes within a Trusted Execution Environment of the merchant terminal.

14. The method according to claim 12 or claim 13 wherein, during the first secure monitored session, the merchant app reports data from the check routine at least once per second to the transaction server and the transaction server compares the reported data to expected results of the merchant app and the device type it is executing on.

15. The method according to any one of the preceding claims wherein the visual representation includes a QR code.

16. The method according to any one of claims 1 to 14 wherein the visual representation includes a barcode.

17. The method according to any one of the preceding claims wherein the merchant terminal is a personal mobile device.

18. The method according to claim 17 wherein the personal mobile device is a smartphone or tablet computer.

19. The method according to any one of claims 2 to 18 wherein the step of initiating a second secure monitored session between the customer device and the transaction server includes:

    a) creating a unique random number (CA-RAND) at the customer app;

    b) generating a session key (CA-SESSION-KEY) using CA-RAND and a second seed value for the customer app version as key parameters;

    c) calculating a second key check value (KCV2) of CA-SESSION-KEY at the customer app and sending KCV2 and a hash of a function result combining TRANS-ID and TIMESTAMP1 XOR CA-RAND to the transaction server;

    d) calculating the CA-SESSION-KEY at the transaction server and verifying KCV2 against the KCV2 obtained from the customer app;

e) sending white box cryptography tables, a second transaction timestamp (TIMESTAMP2) and a random PAN from the transaction server to the customer app, wherein the white box cryptography tables are encrypted using the CA-SESSION-KEY, wherein the white box cryptography tables represent bytes used to source a white box cryptography session;

f) replacing TRANS-ID with CA-RAND and TIMESTAMP1 with TIMESTAMP2 at the transaction server;

g) decrypting, at the customer app, the white box cryptography tables using CA-SESSION-KEY and replacing the current white box cryptography tables with the new decrypted tables;

h) replacing TRANS-ID with CA-RAND and TIMESTAMP1 with TIMESTAMP2 at the customer app;

i) repeating steps f) to h) at predetermined time intervals during the second secure monitored session.

20. The method according to claim 19 wherein the CA-SESSION-KEY is calculated at the transaction server by extracting CA-RAND from a hash of a function result combining TRANS-ID and TIMESTAMP1 XOR CA-RAND.

21. The method according to claim 19 or claim 20 wherein the CA-SESSION-KEY is generated by applying a one way function to CA-RAND and the second seed value.

22. The method according to any one of claims 19 to 21 wherein, if KCV2 calculated at the transaction server mismatches the KCV2 received from the customer app, the transaction server replaces TRANS-ID and TIMESTAMP1 with replacement values.

23. The method according to any one of claims 19 to 22 wherein the white box cryptography tables are replaced at time intervals in the range of 1 to 5 seconds.

24. The method according to claim 23 wherein the white box cryptography tables are replaced at time intervals of every 2 seconds.

25. The method according to claim 19 wherein the white box cryptography tables are deleted upon ending the first and/or second secure monitored sessions.

26. The method according to any one of claims 19 to 25 wherein, during the second secure monitored session, the customer app executes a check routine to check for signs of tampering by examining the integrity of the operating system, memory and/or stored code and files of the customer device.

27. The method according to claim 26 wherein the customer app executes within a Trusted Execution Environment of the customer device.

28. The method according to claim 26 or claim 27 wherein, during the second secure monitored session, the customer app reports data from the check routine at least once per second to the transaction server and the transaction server compares the reported data to expected results of the customer app and the device type it is executing on.

29. A computer system configured to perform a method according to any one of the preceding claims.

30. A non-transient carrier medium having instructions stored thereon such that, when executed on a computer, the computer is configured to perform a method according to any one of claims 1 to 28.

31. A method of conducting a secure transaction between a customer mobile device and a merchant terminal, the method including:

    in response to a request received by the merchant terminal, processing, by a processor of the customer mobile device, a digital representation captured by a camera of the customer mobile device, the image including an encoded transaction identifier (TRANS-ID) and a timestamp (TIMESTAMP1) corresponding to a time when the transaction was requested or initiated, wherein (TRANS-ID) is unique to the transaction and based on a customer primary account number (PAN) and a transaction amount;

    wherein the PAN represents a debit or credit card number, a tokenized version thereof, or an encrypted version thereof that is associated with the customer account at the financial institution;

    initiating a secure monitored session between the customer mobile device and a transaction server;

wherein the secure monitored session refers to a mutually authenticated connection which provides a safe window in which a PIN number associated with the customer PAN is entered;

controlling a user interface on the customer mobile device to present a customer with an interface to enter the PIN number associated with a customer primary account number (PAN) of the customer;

upon receipt of the PIN number at the interface, generating a PIN block for the PIN number and transmitting the PIN block to the transaction server for verification for obtaining a verification or rejection of the transaction from a financial institution associated with the customer account.

32. The method according to claim 31, further comprising receiving a verification or rejection of the transaction at the customer mobile device and display the verification or rejection to the customer on a display of the customer mobile device.

33. A server configured to facilitate a method of conducting a secure transaction between a customer mobile device and a merchant terminal, the method including:

conducting a first secure monitored session with the merchant terminal, wherein during the first secure monitored session, a customer primary account number (PAN) is captured at the merchant terminal, the customer PAN being associated with a customer account at a financial institution;

wherein the first secure monitored session refers to a mutually authenticated connection in which sensitive data is encrypted;

wherein the PAN represents a debit or credit card number, a tokenized version thereof, or an encrypted version thereof that is associated with the customer account at the financial institution;

receiving a request for a transaction from the merchant terminal, the request including the customer PAN and a transaction amount;

generating a transaction identifier (TRANS-ID) that is unique to the transaction and a timestamp (TIMESTAMP1) corresponding to a time when the transaction was requested or initiated, and sending TRANS-ID and TIMESTAMP1 to the merchant

terminal, wherein TRANS-ID and TIMESTAMP1 are encoded in a visual representation and presented on a display for capture by a camera on the customer device;

conducting a second secure monitored session with the customer device, wherein the second secure monitored session refers to a mutually authenticated connection which provides a safe window in which a PIN number associated with the customer PAN is entered, wherein during the second secure monitored session, the customer device is controlled to:

present the customer with a user interface to enter the PIN number associated with the customer PAN; and

generate a PIN block for the PIN number using a random primary account number downloaded from the server and transmit the PIN block to the server for verification;

receiving the PIN block and obtaining a verification or rejection of the transaction from a financial institution associated with the customer account; and

transmitting the verification or rejection of the transaction to the merchant terminal to complete the transaction.