CLAIMS

1. A method for performing secure online transaction between an integrated circuit card, a communications device and a server, comprising:

(a) in the integrated circuit card, generating a dynamic encryption key for transaction data, and transmitting the dynamic encryption key to the communications device via near field communication;

(b) in the communications device, encrypting the transaction data using the dynamic encryption key;

(c) in the integrated circuit card, signing the transaction data to obtain transaction signature and sending the transaction signature to the communications device via near field communication; and

(d) transmitting the encrypted transaction data and transaction signature from the communications device to the server via a communications means for decryption of the encrypted transaction data and authentication of the transaction signature by the server,

wherein a tag is assigned to the dynamic encryption key in step (a) for identification during decryption of the encrypted transaction data.

2. A method for performing secure online transaction between an integrated circuit card, a communications device and a server, comprising:

(a) in the integrated circuit card, signing transaction data to obtain transaction signature and sending the transaction signature to the communications device via near field communication;

(b) in the integrated circuit card, generating a dynamic encryption key for the transaction data, and transmitting the dynamic encryption key to a communications device via near field communication;

(c) in the communications device, encrypting the transaction data using the dynamic encryption key; and

(d) transmitting the encrypted transaction data and transaction signature from the communications device to the server via a communications means for decryption of the encrypted transaction data and authentication of the transaction signature by the server,

wherein a tag is assigned to the dynamic encryption key in step (b) for identification

during decryption of the encrypted transaction data.

3. The method according to claim 1 or 2, wherein the integrated circuit card and the communications device communicate via near field communication without any intermediary hardware device.

4. The method according to claim 3, wherein the intermediary hardware device is a dedicated card reading device provided by a merchant or service provider which is authenticated and compatible with the integrated circuit card.

5. The method according to any preceding claim , wherein the step of generating a dynamic encryption key comprises:

(a) executing an application for the online transaction by the communications device;

(b) requesting the integrated circuit card to generate an application cryptogram (AQ) and setting all fields of the transaction data to a prescribed value by the communications device; and

(c) generating the application cryptogram (ACi), an integrated circuit card verification result (CVRi) and an application transaction counter (ATC) by the integrated circuit card and transmitting the generated AC_{i5} CVRi and ATC to the communications device, wherein the generated ACi is the encryption key used for encrypting the transaction data.

6. The method according to claim 5, wherein the step of signing of the transaction data comprises:

(a) processing the transaction data by dividing at least one field of the transaction data into n groups by the communications device if the data length thereof is greater than a prescribed size, with the prescribed size being one group; if the data length is not an integer multiple of a prescribed number, adding data pre-determined by the server to the remaining data length that is not divided into one or more groups, to make up the prescribed size to form a group;

(b) populating the one or more fields of the transaction data according to the

grouping of the step (a) by the communications device and requesting the integrated circuit card to generate an application cryptogram (AC_2); and

(c) repeating the step (b) until all the transaction data is communicated to the integrated circuit card, and the integrated circuit card generates the application cryptogram AC_2 to AC_{n+i}, verification result CVR_2 to CVR_{n+i} and corresponding application transaction counters and transmits the same to the communications device to complete the signing of the transaction data.

7. The method according to claim 6, wherein the step of transmitting the encrypted transaction data and signature comprising transmitting the encrypted transaction data, the application cryptogram (AC_2 to AC_{n+i}), the application transaction counter (ATC) and all the verification results (CVRi to CVR_{n+i}) from the communications device to the server via the communications means.

8. The method according to claim 7, wherein the step of decrypting the encrypted transaction data by the server comprising:

a. deriving a key and an application interchange profile (AIP) corresponding to the integrated circuit card from a database having information relating to the integrated circuit card holder;

b. calculating the ACi according to the received ATC and CVRi, the key and the AIP derived from the step (a) above, and the prescribed value of the transaction data;

c. decrypting the encrypted transaction data by using the calculated AQ and a prescribed algorithm;

d. dividing the at least one field of the transaction data into n groups if the data length thereof is greater than a prescribed size, with the prescribed size being one group; if the data length is not an integer multiple of a prescribed number, adding data pre-determined by the communications device to the remaining data length that is not divided into one or more groups, to make up the prescribed number to form a group;

e. adding one to the ATC, and calculating an application cryptogram data using each group in the step (d), the AIP and CVR_n, and comparing the

calculated application cryptogram data with AC_n; and

f. repeating the step (e) until all the calculated application cryptogram is compared with all AC_n+i,

wherein when the values compared are identical, the authenticity is verified and the integrity of the online transaction is preserved.

9. The method according to any of claims 5 to 8, wherein the application cryptogram is an eight-byte application cryptogram.

10. The method according to any preceding claim, wherein the one or more fields of the transaction data comprises a transaction type, an authorized amount, an unpredictable number and an account number.

11. The method according to any preceding claim, wherein the communications device is a mobile computing device.

12. The method according to claim 10, wherein the mobile computing device is one of a mobile phone, tablet, laptop and personal digital assistant.

13. The method according to any one of claims 6 to 12, wherein the communications means is one of the Internet, an intranet, a dedicated network and any network suitable for connecting the communications device and the server.

14. The method according to any one of claims 6 to 13, wherein the prescribed size is four bytes.

15. The method according to any one of claims 6 to 14, wherein the integer multiple is an integer multiple of four.

16. The method according to any preceding claim, wherein the tag is in the form an ordinal.

17. The method according to any of claims 1 to 15, wherein the tag is in the form of a

timestamp.

18. A system for performing secure online transaction comprising:

(a) an integrated circuit card;

(b) a communications device; and

(c) a server,

wherein the integrated circuit card and the communications device communicate via near field communication without any intermediary hardware device; and the communications device and the server

communicate via a communications means; and

wherein the integrated circuit card is operable to generate a dynamic encryption key for transaction data; the communications device is operable to encrypt the transaction data using the encryption key; the integrated circuit card is further operable to sign the transaction data to obtain transaction signature and send the transaction signature to the communications device; and transmit the encrypted transaction data and transaction signature from the communications device to the server via the communications means; the server further operates to decrypt the encrypted transaction data and authenticate the transaction signature in which a tag is assigned to the dynamic encryption key for identification during decryption of the encrypted transaction data.

19. A system for performing secure online transaction according to claim 18 wherein the intermediary hardware device is a dedicated card reading device provided by a merchant or service provider which is authenticated and compatible with the integrated circuit card.

20. A server for use in a system for performing secure online transaction wherein the server is operable to receive an encrypted transaction data and transaction signature from a communications device; and is further operable to decrypt the encrypted transaction data and authenticate the transaction signature; the server further comprises:

(a) means for deriving a key and an application interchange profile (AIP) corresponding to an integrated circuit card from a database having

information relating to the integrated circuit card holder;

(b) means for calculating an application ciphertext (ACi) according to an application transaction counter (ATC) and an integrated circuit card verification result (CVRi), the key and the AIP derived from the step (a) above, and a prescribed value of the transaction data;

(c) means for decrypting the encrypted transaction data by using the calculated AC and a prescribed algorithm;

(d) means for dividing the at least one field of the transaction data into n groups if the data length thereof is greater than a prescribed size, with the prescribed size being one group; if the data length is not an integer multiple of a prescribed number, adding data pre-determined by the communications device to the remaining data length that is not divided into one or more groups, to make up the prescribed number to form a group;

(e) means for adding one to the ATC, and calculating an application cryptogram data using each group in the step (d), the AIP and CVR_n, and comparing the calculated application cryptogram data with AC_n; and

(f) means for repeating the step (e) until all the calculated application cryptogram is compared with all AC_{n+i},

wherein when the values compared are identical, the authenticity is verified and the integrity of the online transaction is preserved.