

In the claims

1. A data transmission system comprising:
 - a card having a processor and memory, the memory of the card containing a master key, transmission data and a counter value, wherein the card is an MSD compliant card;
 - a server having a processor and memory, the memory of the server containing the master key and the counter value;
 - a cellphone wherein the server is in data communication with the card through the cellphone;wherein the cellphone is configured to:
 - receive an input from a user and, based on the input, derive a key diversification value;
 - transmit the key diversification value to the card;
 - receive encrypted transmission data from the card; and
 - transmit the encrypted transmission data and the key diversification value to the server;wherein the card is configured to:
 - generate a diversified key using the master key, the counter value, the key diversification value and one or more cryptographic algorithms;
 - encrypt the transmission data using one or more cryptographic algorithms and the diversified key to yield the encrypted transmission data, and
 - transmit the encrypted transmission data to the cellphone; andwherein the server is configured to:
 - receive the encrypted transmission and the key diversification value from the

cellphone;

generate the diversified key based on the master key, the counter value and the key diversification value; and

decrypt the encrypted transmission data using one or more cryptographic algorithms and the diversified key; and

transmit a communication to a second server to authenticate a transaction.

2. The data transmission system of claim 1, wherein the card is a contactless card in compliance with the following standards: ISO/IEC 7810, ISO/IEC 7811, ISO/IEC 7812, ISO/IEC 7813, ISO 8583, and ISO/IEC 4909.

3. The data transmission system of claim 1, wherein the transmission data includes an account number.

4. The data transmission system of claim 1, wherein the input is an alphanumeric code provided by the user through a touchscreen of the cellphone.

5. The data transmission system of claim 1, wherein the input is a fingerprint scanned at the cellphone.

6. The data transmission system of claim 5, wherein the cellphone stores a plurality of key diversification values in association with a plurality of fingerprints.

7. The data transmission system of claim 6, wherein the cellphone is configured to transmit to the card and the server the key diversification value associated with the fingerprint scanned at the cellphone.

8. The data transmission system of claim 1, wherein the input is a photo of the user.

9. The data transmission system of claim 8, wherein the cellphone is configured to transmit the photo to the server.

10. The data transmission system of claim 9, wherein the server is configured to conduct a facial recognition technique to match the photo to a photo of the user stored in the server.
11. The data transmission system of claim 10, wherein the server is configured to generate the key diversification value based on the photo.
12. The data transmission system of claim 11, wherein the server is configured to transmit the key diversification value to the cellphone.
13. A data transmission system comprising:
 - a card having a processor and memory, the memory of the card containing a master key, transmission data and a counter value, wherein the card is an MSD compliant card;
 - a server having a processor and memory, the memory of the server containing the master key and the counter value;
 - a cellphone wherein the server is in data communication with the card through the cellphone;wherein the cellphone is configured to:
 - receive a first input from a user and, based on the first input, derive a key diversification value;
 - receive a second input from the user and, based on the second input, derive an algorithm selection value;
 - transmit the key diversification value and the algorithm selection value to the card;
 - receive encrypted transmission data from the card; and
 - transmit the encrypted transmission data, the key diversification value and the algorithm selection value to the server;

wherein the card is configured to:

generate a diversified key using the master key, the counter value, the key diversification value and a cryptographic algorithm selected using the algorithm selection value;

encrypt the transmission data using the cryptographic algorithm and the diversified key to yield the encrypted transmission data; and

transmit the encrypted transmission data to the cellphone; and

wherein the server is configured to:

receive the encrypted transmission, the key diversification value and the algorithm selection value from the cellphone;

generate the diversified key based on the master key, the counter value and the key diversification value using the cryptographic algorithm; and

decrypt the encrypted transmission data using the cryptographic algorithm and the diversified key; and

transmit a communication to a second server to authenticate a transaction.

14. The data transmission system of claim 13, wherein the card is a contactless card in compliance with the following standards: ISO/IEC 7810, ISO/IEC 7811, ISO/IEC 7812, ISO/IEC 7813, ISO 8583, and ISO/IEC 4909.

15. The data transmission system of claim 13, wherein the first input is a fingerprint scanned at the cellphone and the second input is an alphanumeric value entered on a touchscreen of the cellphone.

16. The data transmission system of claim 15, wherein the cellphone stores a plurality of key diversification values in association with a plurality of fingerprints.

17. The data transmission system of claim 16, wherein the cellphone is configured to transmit to the card and the server:

the key diversification value associated with the fingerprint scanned at the cellphone;

and

the alphanumeric value as the algorithm selection value.

18. The data transmission system of claim 13, wherein the first input is a photo of the user.

19. The data transmission system of claim 18, wherein the cellphone is configured to transmit the photo to the server.

20. The data transmission system of claim 19, wherein the server is configured to generate the key diversification value based on the photo.