CLIENT DEVICE AUTHENTICATION USING CONTACTLESS LEGACY MAGNETIC STRIPE DATA

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to U.S. Patent Application No. 16/590,536 filed October 2, 2019.

BACKGROUND

[0002] Data security and transaction integrity are of critical importance to businesses and consumers. This need continues to grow as electronic transactions constitute an increasingly large share of commercial activity. Contactless cards can be an invaluable resource in providing data security and transaction integrity. While the growing use of chip-based financial cards (e.g., EMV cards) provides certain secure features over the legacy magnetic stripe cards (MSD), the majority of contactless-accepting merchants still utilize MSD cards and MSD technology. Therefore, many card issuers still choose to support both MSD cards and EMV cards.

SUMMARY

[0003] Because many card issuers still choose to support MSD cards in this country, technologies that facilitate transaction security and user authentication for these cards are desirable. In particular, it is important to enhance card security for contactless legacy magnetic stripe cards when it comes to interactions with cellphones or similar client devices. Example interactions can include activation, authentication or step-up authentication using mobile devices, cellphones and tablets.

[0003a] According to one aspect, there is provided a contactless card, comprising a memory storing a card key, transmission data, and a counter value; and a processor, wherein the contactless card is an MSD compliant contactless card, and wherein the contactless card is configured to generate a diversified key using the card key, the counter value,

and a cryptographic algorithm, encrypt the transmission data using the cryptographic algorithm and the diversified key to yield the encrypted transmission data, and transmit the encrypted transmission data.

[0003b] According to another aspect, there is provided a method performed by an MSD compliant contactless card comprising a processor and a memory storing a card key, transmission data, and a counter value, the method comprising generating a diversified key using the card key, the counter value, and a cryptographic algorithm, encrypting the transmission data using the cryptographic algorithm and the diversified key to yield the encrypted transmission data, and transmitting the encrypted transmission data.

[0003c] According to another aspect, there is provided a non-transitory, computer-readable medium containing instructions for execution by an MSD compliant contactless card comprising a processor and a memory storing a card key, transmission data, and a counter value, wherein, upon execution the instructions configure the contactless card to perform procedures comprising: generating a diversified key using the card key, the counter value, and a cryptographic algorithm, encrypting the transmission data using the cryptographic algorithm and the diversified key to yield the encrypted transmission data, and transmitting the encrypted transmission data.

[0004] In an example embodiment, a secure data transmission system including an MSD compliant card ("card"), a cellphone and a server are disclosed. The cellphone can receive

~~In the claims~~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; and~~

~~wherein 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.~~

1. A contactless card, comprising:

a memory storing a card key, transmission data, and a counter value; and

a processor,

wherein the contactless card is an MSD compliant contactless card, and

wherein the contactless card is configured to:

generate a diversified key using the card key, the counter value, and a cryptographic algorithm,

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

transmit the encrypted transmission data.

2. The contactless card of claim 1, wherein:

the memory further stores a key diversification value, and

the contactless card is further configured to generate the diversified key using the key diversification value, the card key, the counter value, and the cryptographic algorithm.

3. The contactless card of claim 2, wherein the contactless card is further configured to receive the key diversification value from at least one selected from the group of a client device and a server.

4. The contactless card of claim 2, wherein the key diversification value includes a biometric input.

5. The contactless card of claim 4, wherein the biometric input comprises at least one selected from the group of data associated with a photo and data associated with a fingerprint.

6. The contactless card of claim 2, wherein the key diversification value comprises an alphanumeric code.

7. The contactless card of claim 1, wherein the transmission data includes an account number.

8. The contactless card of claim 1, wherein the contactless card is further to select the cryptographic algorithm based on an algorithm selection value.

9. The contactless card of claim 8, wherein the memory further stores the algorithm selection value.

10. The contactless card of claim 9, wherein the algorithm selection value is the counter value.

11. The contactless card of claim 8, wherein the contactless card is configured to receive the algorithm selection value from at least one selected from the group of a client device and a server.

12. The contactless card of claim 8, wherein:

the contactless card further includes an input pad, and

the contactless card is further configured to receive the algorithm selection value via the input pad.

13. A method performed by an MSD compliant contactless card comprising a processor and a memory storing a card key, transmission data, and a counter value, the method comprising:

generating a diversified key using the card key, the counter value, and a cryptographic algorithm,

encrypting the transmission data using the cryptographic algorithm and the diversified key to yield the encrypted transmission data, and

transmitting the encrypted transmission data.

14. The method of claim 13, further comprising generating the diversified key using a key diversification value, the card key, the counter value, and the cryptographic algorithm.

15. The method of claim 14, wherein generating the diversified key using the card key, the counter value, and the cryptographic algorithm comprises encrypting the counter value using the card key and the cryptographic algorithm.

16. The method of claim 14, wherein the key diversification value comprises at least one selected from the group of a random nonce generated each time a new diversified key is needed, a portion of the counter value, a one-time passcode, and a cryptographic hash of data stored in the memory.

17. The method of claim 14, wherein the method further comprises:

receiving a user input, and

storing the user input as the key diversification value.

18. A non-transitory, computer-readable medium containing instructions for execution by an MSD compliant contactless card comprising a processor and a memory storing a card key, transmission data, and a counter value, wherein, upon execution the instructions configure the contactless card to perform procedures comprising:

generating a diversified key using the card key, the counter value, and a cryptographic algorithm,

encrypting the transmission data using the cryptographic algorithm and the diversified key to yield the encrypted transmission data, and

transmitting the encrypted transmission data.

19. The non-transitory, computer-readable medium of claim 18, the procedures further comprising generating the diversified key using a key diversification value, the card key, the counter value, and the cryptographic algorithm.

20. The non-transitory, computer-readable medium of claim 19, wherein generating the diversified key using the card key, the counter value, and the cryptographic algorithm comprises encrypting the counter value using the card key and the cryptographic algorithm.