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

Claims

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.