may rely on log-in credentials (e.g., username and password) to confirm a cardholder's identity. However, if the log-in credentials are compromised, another person could have access to the user's account.

[0006] These and other deficiencies exist. Accordingly, there is a need to provide users with an appropriate solution that overcomes these deficiencies to provide data security, authentication, and verification for contactless cards. Further, there is a need for both an improved method of activating a card and an improved authentication for account access.

SUMMARY

[0007] Aspects of the disclosed technology include systems and methods for cryptographic authentication of contactless cards. Various embodiments describe systems and methods for implementing and managing cryptographic authentication of contactless cards.

[0007a] An aspect of the present disclosure provides a contactless card, comprising a processor and a memory, the memory containing transmission data, a diversified key, a counter, a first applet and a second applet, wherein the first applet is configured to: generate a cryptographic result using one or more cryptographic algorithms and the diversified key, wherein the cryptographic result includes the counter, encrypt the transmission data using the one or more cryptographic algorithms and the diversified key to yield encrypted transmission data, transmit, over a communication field established between the first applet and a client application comprising instructions for execution on a client device, the cryptographic result and the encrypted transmission data to the client application, create, in response to a message received from the client application, a communication path to the second applet, the message being generated by the client application in response to a decryption of the encrypted transmission data and validation of the cryptographic result received from the first applet, and deactivate the second applet via the communication path, wherein the second applet is precluded from communication external to the contactless card.

[0007b] Another aspect of the present disclosure provides a method, comprising: generating, by a first applet stored on a contactless card, a cryptographic result including a counter value using one or more cryptographic algorithms and a diversified key, the counter value and the diversified key being stored on the contactless card; encrypting transmission data, stored on the contactless card, using the diversified key to yield encrypted transmission data; transmitting, via a communication field, the cryptographic result and the encrypted transmission data to a client application executing on a client device; creating, by the first applet, a communication path to a second applet stored on the contactless card, wherein the communication path is created in response to a message received from the client application, the message being generated by the client application in response to a decryption of the encrypted transmission data and validation of the cryptographic result received from the first applet; and deactivating, by the first applet via the communication path, the second applet, wherein the second applet is precluded from communication external to the contactless card.

[0007c] Another aspect of the present disclosure provides a non-transitory computer-readable medium containing instructions for execution by a processor, wherein, upon execution, the processor is configured to perform procedures comprising: generating, by a first applet stored on a contactless card, a cryptographic result including a counter value using one or more cryptographic algorithms and a diversified key, the counter value and the diversified key being stored on the contactless card; encrypting transmission data, stored on the contactless card, using the diversified key to yield encrypted transmission data; transmitting, via a communication field, the cryptographic result and the encrypted transmission data to a client application executing on a client device; creating, by the first applet, a communication path to a second applet stored on the contactless card, wherein the communication path is created in response to a message received from the client application, the message being generated by the

client application in response to a decryption of the encrypted transmission data and validation of the cryptographic result received from the first applet, and deactivating, by the first applet via the communication path, the second applet, wherein the second applet is precluded from communication external to the contactless card.

[0008] There is also disclosed a card locking system comprising: a contactless card including one or more processors, and a memory, wherein the memory comprises a diversified master key, transmission data, first and second applets, and a counter; a client application comprising instructions for execution on a client device including a processor and a memory, the memory containing a master key, wherein the contactless card is configured to: generate a diversified key using the diversified master key, one or more cryptographic algorithms, and the counter, generate a cryptographic result including the counter using one or more cryptographic algorithms and the diversified key, encrypt the transmission data using the one or more cryptographic algorithms and the diversified key to yield encrypted transmission data, and transmit the cryptographic result and encrypted transmission data to the client application; and wherein the application is configured to: generate an authentication diversified key based on the master key and a unique identifier,

CLAIMS

1. A contactless card, comprising:

a processor; and

a memory, the memory containing transmission data, a diversified key, a counter, a first applet and a second applet,

wherein the first applet is configured to:

generate a cryptographic result using one or more cryptographic algorithms and the diversified key, wherein the cryptographic result includes the counter,

encrypt the transmission data using the one or more cryptographic algorithms and the diversified key to yield encrypted transmission data,

transmit, over a communication field established between the first applet and a client application comprising instructions for execution on a client device, the cryptographic result and the encrypted transmission data to the client application,

create, in response to a message received from the client application, a communication path to the second applet, the message being generated by the client application in response to a decryption of the encrypted transmission data and validation of the cryptographic result received from the first applet, and

deactivate the second applet via the communication path, wherein the second applet is precluded from communication external to the contactless card.

2. The contactless card of claim 1, wherein the communication path comprises a secure channel.

3. The contactless card of claim 1, wherein the first applet is configured to deactivate the second applet for a predetermined period of time.

4. The contactless card of claim 1, wherein the second applet is reactivated after entry of a contactless card into the communication field.

5. The contactless card of claim 1, wherein the first applet is further configured to deactivate the second applet based on exceeding a threshold.

6. The contactless card of claim 5, wherein the threshold comprises at least one selected from the group of user status, user history, account activity, account history, transaction limits, spending limits, time limits, location limits, good type limit, service type limit, merchant limit, and point of sale device type.

7. The contactless card of claim 1, wherein the first applet is further configured to set the contactless card to an inactive state.

8. The contactless card of claim 1, wherein the diversified key is generated using a diversified master key stored on the contactless card, one or more cryptographic algorithms, and the counter.

9. A method, comprising:

generating, by a first applet stored on a contactless card, a cryptographic result including a counter value using one or more cryptographic algorithms and a diversified key, the counter value and the diversified key being stored on the contactless card;

encrypting transmission data, stored on the contactless card, using the diversified key to yield encrypted transmission data;

transmitting, via a communication field, the cryptographic result and the encrypted transmission data to a client application executing on a client device;

creating, by the first applet, a communication path to a second applet stored on the contactless card, wherein the communication path is created in response to a message received from the client application, the message being generated by the client application in response to a decryption of the encrypted transmission data and validation of the cryptographic result received from the first applet; and

deactivating, by the first applet via the communication path, the second applet, wherein the second applet is precluded from communication external to the contactless card.

10. The method of claim 9, further comprising:

transmitting, by a server in response to the deactivation of the second applet, a message to a client device,

wherein the message is indicative of at least one selected from the group of location information, account information, and rewards points.

11. The method of claim 10, further comprising monitoring, by the server, a time period associated with the deactivation of the second applet.

12. The method of claim 10, further comprising, after entering the communication field of the client device, reactivating the second applet.

13. The method of claim 9, wherein:

the first applet is configured to deactivate the second applet based on exceeding a threshold, and

the threshold comprises at least one selected from the group of user status, user history, account activity, account history, transaction limits, spending limits, time limits, location limits, good type limit, service type limit, merchant limit, and point of sale device type.

14. The method of claim 9, wherein the communication path comprises a secure channel.

15. A non-transitory computer-readable medium containing instructions for execution by a processor, wherein, upon execution, the processor is configured to perform procedures comprising:

generating, by a first applet stored on a contactless card, a cryptographic result including a counter value using one or more cryptographic algorithms and a diversified key, the counter value and the diversified key being stored on the contactless card;

encrypting transmission data, stored on the contactless card, using the diversified key to yield encrypted transmission data;

transmitting, via a communication field, the cryptographic result and the encrypted transmission data to a client application executing on a client device;

creating, by the first applet, a communication path to a second applet stored on the contactless card, wherein the communication path is created in response to a message received from the client application, the message being generated by the client application in response to a decryption of the encrypted transmission data and validation of the cryptographic result received from the first applet, and

deactivating, by the first applet via the communication path, the second applet, wherein the second applet is precluded from communication external to the contactless card.

16. The non-transitory computer-readable medium of claim 15, wherein the communication path comprises a secure channel.

17. The non-transitory computer-readable medium of claim 15, wherein:

the first applet is configured to deactivate the second applet based on exceeding a threshold, and

the threshold comprises at least one selected from the group of user status, user history, account activity, account history, transaction limits, spending limits, time limits, location limits, good type limit, service type limit, merchant limit, and point of sale device type.

18. The non-transitory computer-readable medium of claim 15, wherein the first applet is configured to deactivate the second applet for a predetermined period of time.

19. The non-transitory computer-readable medium of claim 15, wherein the second applet is reactivated after entry of the contactless card into the communication field of the client device.

20. The non-transitory computer-readable medium of claim 15, wherein the first applet is further configured to set the contactless card to an inactive state.