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 a first applet and a second applet, wherein the first applet is configured to: create a communication path to the second applet, and deactivate the second applet via the communication path.

[0007b] Another aspect of the present disclosure provides a method, comprising: creating, by a first applet stored by a contactless card, a communication path to a second applet stored by the contactless card; and deactivating, by the first applet via the communication path, the second applet.

[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: creating, by a first applet, a communication path to a second applet, and deactivating, by the first applet via the communication path, the second applet.

[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,

generate a session key based on the authentication diversified key and the cryptographic result, and decrypt the encrypted transmission data and validate the cryptographic result using the one or more cryptographic algorithms and the session key, wherein the counter is independently updated by the contactless card and the client application for each transmission between the contactless card and the application, wherein the first applet is configured to establish a communication path to the second applet based on receipt of a message from the client application, and wherein the second applet is deactivated by the first applet via the communication path.

[0009] There is also disclosed a method for locking a contactless card including a processor and a memory containing a master key, an identification number, a first applet, a second applet, and a counter, comprising: generating a card key using the master key and the identification number; generating a first session key using the card key and a first portion of the counter and a second session key using the card key and a second portion of the counter, wherein the first portion of the counter is different than the second portion of the counter; generating a cryptographic result including the counter using one or more cryptographic algorithms and the card key; generating a cryptogram using the first session key, the cryptogram including the cryptographic result and the identification number; encrypting the cryptogram using the second session key; transmitting the encrypted cryptogram and the cryptographic result; receiving a deactivation instruction to deactivate the contactless card; creating a communication path to the second applet; and deactivating the second applet via the communication path.

[0010] There is also disclosed a contactless card comprising: a processor and a memory, wherein the memory comprises first and second applets and a

CLAIMS

1. A contactless card, comprising:

a processor; and

a memory, the memory containing a first applet and a second applet,

wherein the first applet is configured to:

create a communication path to the second applet, and

deactivate the second applet via the communication path.

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 further configured to deactivate the second applet in response to a message.

4. The contactless card of claim 3, wherein the first applet is further configured to receive the message from an application executing on a receiving device.

5. The contactless card of claim 4, wherein:

the receiving device comprises a server, and

the message is received by the first applet via a client device.

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

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

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

9. The contactless card of claim 6, 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.

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

11. A method, comprising:

creating, by a first applet stored by a contactless card, a communication path to a second applet stored by the contactless card; and

deactivating, by the first applet via the communication path, the second applet.

12. The method of claim 11, further comprising:

receiving, by the first applet, a message,

wherein the first applet is further configured to deactivate the second applet based on the message.

13. The method of claim 11, 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.

14. The method of claim 13, further comprising monitoring, by the server, a time period associated with the deactivation of the second applet.

15. The method of claim 13, further comprising, after entering a communication field of the client device, reactivating the second applet.

16. The method of claim 11, 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.

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

creating, by a first applet, a communication path to a second applet, and

deactivating, by the first applet via the communication path, the second applet.

18. The non-transitory computer-readable medium of claim 17, wherein the communication path comprises a secure channel.

19. The non-transitory computer-readable medium of claim 17, wherein the procedures further comprise:

receiving, by the first applet, a message,

wherein the first applet is further configured to deactivate the second applet based on the message.

20. The non-transitory computer-readable medium of claim 17,

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.