over the previous technology (e.g., magnetic strip cards) for in-person purchases, account access still 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 system, comprising: a contactless card having a processor and memory, the memory of the contactless card containing a card key and transmission data; and an application comprising instructions for execution on a receiving device having a processor and memory, the memory of the receiving device containing an application key; wherein, after entry into a communication field of the receiving device, the contactless card is configured to: generate a diversified card key by diversifying the card key with a counter value, encrypt the transmission data using a cryptographic algorithm and the diversified card key to yield encrypted transmission data, and transmit the encrypted transmission data to the application; and wherein the application is configured to: decrypt the encrypted transmission data using ~~the cryptographic algorithm~~a unique card identified, the counter value and the application key~~;~~, authenticate a user identity ~~associated with a user;~~ ,

based on a verification of the decrypted transmission data, and after authenticating the user identity, perform authorize an action relating to the user.

~~**[0007b]** Another aspect of the present disclosure provides a non-transitory computer-readable medium containing instructions for execution by the processor, wherein, upon execution by the processor, the instructions configure the processor to perform procedures comprising: receiving, from a contactless card, encrypted transmission data; decrypting, using a cryptographic algorithm and an application key, the transmission data; authenticating a user identity associated with the user; and after authenticating the user identity, performing an action relating to the user.~~

[0007~~c~~b] Another aspect of the present disclosure provides a method, comprising: generating, by a contactless card storing a card key and a counter value, a diversified card key by diversifying the card key with the counter value; encrypting, by ~~a~~ the contactless card using the diversified card key, transmission data ~~using a cryptographic algorithm and a diversified key to yield~~ stored on the contactless card to generate encrypted transmission data; transmitting, by the contactless card, the encrypted transmission data to an application ~~comprising instructions for execution on a receiving~~executing on a client device; receiving, by the application, the encrypted transmission data from the contactless card; decrypting, by the application, the encrypted transmission data using the ~~cryptographic algorithm~~counter value and an application key; authenticating a user identity ~~associated with a user~~, based on a verification of the decrypted transmission data; and after authenticating the user identity, perform an action relating to the user.

[0007c] Another aspect of the present disclosure provides a contactless card communicatively coupled, via near field communication, to an application executing on a receiving device, the contactless card being configured to: encrypt transmission data using a cryptographic algorithm and a diversified key to yield encrypted transmission data,

wherein the transmission data, the cryptographic algorithm and the diversified key are stored onto a memory of the contactless card; and transmit the encrypted transmission data to the application, the application being configured to decrypt and authenticate the encrypted transmission data, to authorize an action to be performed using the receiving device.

[0008] There is also disclosed a system for secure communication comprising: a transmitting device having a processor and memory, the memory of the transmitting device containing a diversified master key, transmission data and a counter value; an application comprising instructions for execution on a receiving device having a processor and memory, the memory of the receiving device containing a master key; wherein the transmitting device is configured to: generate a diversified key using the diversified master key, one or more cryptographic algorithms, and the counter value, generate a cryptographic result including the counter value using the 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 application; wherein

CLAIMS

1. A system, comprising:

a contactless card having a processor and memory, the memory of the contactless card containing a card key and transmission data; and

an application comprising instructions for execution on a receiving device having a processor and memory, the memory of the receiving device containing an application key;

wherein, after entry into a communication field of the receiving device, the contactless card is configured to:

generate a diversified card key by diversifying the card key with a counter value,

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

transmit the encrypted transmission data to the application; and

wherein the application is configured to:

decrypt the encrypted transmission data using ~~the cryptographic algorithm~~ a unique card identifier, the counter value and the application key~~;~~,

authenticate a user identity ~~associated with a user~~, based on a verification of the decrypted transmission data~~;~~, and

after authenticating the user identity, ~~perform~~ authorize an action relating to the user.

2. The system of claim 1, wherein the user identity is associated with ~~at least one~~ data identifying one or more user benefits, the data selected from the group of a rank, a category, and a points system.

3. The system of claim 2, wherein:

the action comprises providing access to ~~an~~ a customer service agent with an enhanced authorization based on the association, and

the enhanced authorization includes at least one selected from the group of an authorization to refund or waive a charge, an authorization to renew or modify a contract, and an authorization to provide free or reduced shipping.

4. The system of claim 3, wherein the enhanced authorization includes at least one selected from the group of an authorization to refund or waive a charge, an authorization to renew or modify a contract, an authorization to provide free or reduced shipping, and an authorization to provide an additional service.

5. The system of claim 1, wherein the action comprises routing a call to a first available operator based on a transaction history associated with the user identity.

6. The system of claim 1, wherein the action comprises at least one selected from the group of accessing financial information and accessing medical information.

7. The system of claim 1, wherein the action comprises at least one selected from the group of providing access~~ing~~ to a physical space, ~~accessing~~ a locker, and ~~accessing~~ a vehicle.

8. The system of claim 1, wherein:

the receiving device ~~comprises~~ is communicatively coupled to a server, and

the contactless card is configured to transmit the encrypted transmission data to the server for validation via the application ~~via one or more intermediary devices~~.

9. The system of claim 1, wherein the application is further configured to record information comprising at least one selected from the group of time of authentication, location of authentication, ~~type of contactless card,~~ type of receiving device, ~~movement of one or more entries into a~~ type of one or more gestures performed with the contactless card within a short-range wireless communication field of the receiving device, and timing of the one or more ~~entries into a communication field~~gestures.

10. The system of claim 9, wherein the application is further configured to~~:~~

analyze the recorded information~~, and~~ to generate a user behavior profile.

11. The system of claim 10, wherein:

the application is further configured to:

determine a threshold of variation for the user behavior profile corresponding to acceptable behavior variation in a user's activity, and

~~the application is further configured to detect~~ set a variation threshold as an indicator of fraud based on the user behavior profile, and

the indicator of fraud includes behavior outside of the user behavior profile and beyond the threshold of variation.

12. A ~~non-transitory computer-readable medium containing instructions for execution by the processor, wherein, upon execution by the processor, the instructions configure the processor to perform procedures~~method comprising:

generating, by a contactless card storing a card key and a counter value, a diversified card key by diversifying the card key with the counter value;

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

transmitting, by the contactless card, the encrypted transmission data to an application executing on a client device;

receiving, ~~from a contactless card~~by the application, the encrypted transmission data from the contactless card;

decrypting, by the application, the encrypted transmission data using ~~a cryptographic algorithm~~the counter value and an application key~~, the transmission data~~;

authenticating a user identity ~~associated with the user~~, based on a verification of the decrypted transmission data; and

after authenticating the user identity, performing an action relating to the user.

13. The ~~non-transitory computer-readable medium~~method of claim 12, wherein the action comprises at least one selected from the group of providing access~~ing to~~ a physical space, ~~accessing~~ a locker, a safe, and ~~accessing~~ a vehicle.

14. The ~~non-transitory computer-readable medium~~method of claim 12, ~~wherein the procedures~~ further comprising~~e~~:

recording, by the application, information associated with user identity authentication behavior,

generating, by the application, a user behavior profile based on the recorded information,

determining, by the application, a threshold of variation for the user behavior profile, the threshold corresponding to acceptable behavior variation in the user behavior profile, and

detecting, by the application, an indicator of fraud based on ~~the user behavior profile and~~ the threshold of variation, wherein the indicator of fraud includes a behavior ~~outside of the user behavior profile and~~ beyond the threshold of variation.

15. The ~~non-transitory computer-readable medium~~method of claim 14, ~~wherein the procedures~~ further comprising generating, by the application, the user behavior profile and determining, by the application, the threshold of variation by applying a machine learning technique.

16. The ~~non-transitory computer-readable medium~~method of claim 14, wherein the recorded information includes ~~at least one prior authentication of the user identity and at least one location associated with the at least one prior authentication~~ a transaction history, associated with one or more previous authentications of the user identity.

17. A ~~method, comprising~~ contactless card communicatively coupled, via near field communication, to an application executing on a receiving device, the contactless card being configured to:

encrypt~~ing, by a contactless card,~~ transmission data using a cryptographic algorithm and a diversified key to yield encrypted transmission data, wherein the transmission data, the cryptographic algorithm and the diversified key are stored onto a memory of the contactless card; and

transmit~~ting, by the contactless card,~~ the encrypted transmission data to ~~an~~ the

application ~~comprising instructions for execution on a receiving device~~, the application being configured to decrypt and authenticate the encrypted transmission data, to authorize an action to be performed using the receiving device.~~;~~

~~decrypting the encrypted transmission data using the cryptographic algorithm and an application key;~~

~~authenticating a user identity associated with a user; and~~

~~after authenticating the user identity, perform an action relating to the user.~~

18. The ~~method~~ contactless card of claim 17, wherein:

the transmission data corresponds to user identity data, the user identity data being ~~is~~ associated with at least one selected from the group of a rank, a category, and a points system~~, and~~

~~the method further comprises providing access to an agent with an enhanced authorization based on the association~~.

~~19. The method of claim 18, wherein the at least one enhanced authorization includes at least one selected from the group of an authorization to refund or waive charges, an authorization to renew or modify a contract, an authorization to provide free or reduced shipping, and an authorization to provide additional services.~~

~~20.~~19. The ~~method~~ contactless card of claim 17, wherein:

the receiving device is equipped within a safe, and

the action comprises unlocking the safe.

20. The contactless card of claim 17, wherein the contactless card is further configured to generate the diversified key by diversifying a master key and a unique card identifier.