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.

[0008] Disclosed herein is 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 the 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; 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; decrypt the encrypted transmission data and validate the received cryptographic result using the one or more cryptographic algorithms and the session key; wherein the application is configured to initiate, upon authentication of at least one user credential, one or more processes, the one or more processes comprising authenticating one or more electronically generated images associated with transportation ticketing information.

[0008a] According to a first aspect of the present disclosure, there is provided a contactless card, including: a processor; and a memory containing a card key, transmission data, and user preference information, wherein the processor is configured to: encrypt the transmission data using a cryptographic algorithm and the card key to yield encrypted transmission data, transmit the encrypted transmission data for decryption, perform one or more actions including retrieval, from the memory, of user preference information for an account associated with a user, and transmit a request for information based on the user preference information.

[0008b] According to a second aspect of the present disclosure, there is provided a method, including the steps of: encrypting, by a processor of a contactless card, transmission data using a cryptographic algorithm and a card key to yield encrypted transmission data; transmitting, by the processor, the encrypted transmission data for decryption; performing, by the processor, one or more actions including retrieval, from a memory of the contactless card, of user preference information for an account associated with a user; and transmitting, by the processor, a request for information based on the user preference information.

[0008c] According to a third aspect of the present disclosure, there is provided a system, including: a contactless card including a processor and a memory, wherein the memory contains a card key, transmission data, and user preference information; and a server, wherein, after entry into a communication field, the contactless card is configured to: encrypt the transmission data using a cryptographic algorithm and the card key to yield encrypted transmission data, transmit the encrypted transmission data for decryption, perform one or more actions including retrieval, from the memory, of user preference information for an account associated with a user, and transmit a request for information based on the user preference information to the server.

[0009] Disclosed herein is a method of securing one or more processes using a transmitting device and an application comprising instructions for execution on a receiving device, the method comprising the steps of: generating a diversified key using a diversified master key, one or more cryptographic algorithms, and a counter value, the transmitting device comprising a processor and memory, the memory of the transmitting device containing the diversified master key, transmission data, and the counter value; generating a cryptographic result including the counter value using the one or more cryptographic algorithms and the diversified key; encrypting the transmission data using the one or more cryptographic algorithms and the diversified key to

yield encrypted transmission data; transmitting the cryptographic result and encrypted transmission data to an application, the application comprising instructions for execution on a receiving device; generating an authentication diversified key based on the master key and a unique identifier; generating a session key based on the authentication diversified key and the cryptographic result; decrypting the encrypted transmission data and validating the received cryptographic result using the one or more cryptographic algorithms and the session key; and initiating, upon authentication of at least one user credential, one or more processes, the one or more processes comprising authenticating one or more electronically generated images associated with transportation ticketing information**[0010]** Further features of the disclosed design, and the advantages offered thereby, are explained in greater detail hereinafter with reference to specific example embodiments illustrated in the accompanying drawings, wherein like elements are indicated by like reference designators.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] FIG. 1A is a diagram of a data transmission system according to an example embodiment.

[0012] FIG. 1B is a diagram illustrating a sequence for providing authenticated access according to an example embodiment.

[0013] FIG. 2 is a diagram of a data transmission system according to an example embodiment.

[0014] FIG. 3 is a diagram of a system using a contactless card according to an example embodiment.

[0015] FIG. 4 is a flowchart illustrating a method of key diversification according to an example embodiment.

[0016] FIG. 5A is an illustration of a contactless card according to an example embodiment.

[0017] FIG. 5B is an illustration of a contact pad of the contactless card according to an example embodiment.

[0018] FIG. 6 is an illustration depicting a message to communicate with a device according to an example embodiment.

CLAIMS

1. A contactless card, comprising:

a processor; and

a memory containing a card key, transmission data, and user preference information, wherein the processor is configured to:

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

transmit the encrypted transmission data for decryption,

perform one or more actions including retrieval, from the memory, of user preference information for an account associated with a user, and

transmit a request for information based on the user preference information.

2. The contactless card of claim 1, wherein the request for information comprises a request for language information.

3. The contactless card of claim 2, wherein the request for language information comprises a request for a translation of text.

4. The contactless card of claim 3, wherein the translation of text comprises at least one selected from the group of translation of text from a non-English language to English and translation of text from English to a non-English language.

5. The contactless card of claim 1, wherein the request for information comprises a request for venue information.

6. The contactless card of claim 6, wherein the venue information is associated with at least one venue selected from the group of an airport lounge, a restaurant, a gas station, and a shop.

7. The contactless card of claim 6, wherein the venue information comprises directions to a venue.

8. The contactless card of claim 1, wherein the processor is further configured to perform the one more actions after the decryption of the transmission data.

9. The contactless card of claim 1, wherein at least one of the one or more actions includes converting a purchase amount from a first currency to a second currency.

10. The contactless card of claim 9, wherein converting a purchase amount from a first currency to a second currency comprises at least one selected from the group of converting a purchase amount from a non-U.S. dollar currency to U.S. dollars and converting U.S. dollars to a non-U.S. dollar currency.

11. The contactless card of claim 1, wherein the processor is configured to transmit the request for information to a server via a communication field generated by a client device.

12. A method, comprising the steps of:

encrypting, by a processor of a contactless card, transmission data using a cryptographic algorithm and a card key to yield encrypted transmission data;

transmitting, by the processor, the encrypted transmission data for decryption;

performing, by the processor, one or more actions including retrieval, from a memory of the contactless card, of user preference information for an account associated with a user; and

transmitting, by the processor, a request for information based on the user preference information.

13. The method of claim 12 wherein the request for information comprises a request for a translation of text from a first language to a second language.

14. The method of claim 12, wherein at least one of the one or more actions includes converting a purchase amount from a first currency to a second currency.

15. A system, comprising:

a contactless card comprising a processor and a memory, wherein the memory contains a card key, transmission data, and user preference information; and

a server,

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

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

transmit the encrypted transmission data for decryption,

perform one or more actions including retrieval, from the memory, of user preference information for an account associated with a user, and

transmit a request for information based on the user preference information to the server.

16. The system of claim 15, wherein the request for information comprises a request for a translation of text from a first language to a second language.

17. The system of claim 16, wherein the server is configured to host a form including the text in the first language and the second language.

18. The system of claim 15, wherein:

the request for information comprises a request for venue information, and

the venue information is associated with at least one venue selected from the group of an airport lounge, a restaurant, a gas station, and a shop.

19. The system of claim 18, wherein the venue information comprises directions to a venue.

20. The system of claim 15, wherein:

the communication field is generated by an application executing on a client device configured to transmit the request for information to the server, and

the client device comprises at least one selected from the group of a point-of-sale device, a kiosk, a terminal, a tablet, a mobile device, and a network-enabled computer.