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] There are disclosed 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] According to a first aspect of the present invention, there is provided a contactless card, comprising:

a processor; and

a memory containing one or more applets and data,

wherein the processor is configured to transmit, after entry of the contactless card into a communication field, the data,

wherein the data comprises one or more information elements configured to activate the contactless card, and

wherein the one or more information elements including a first information element comprising a dynamically generated phone number.

[0007b] According to a second aspect of the present invention, there is provided a server, comprising:

a processor; and

a memory,

wherein the processor is configured to:

receive one or more information elements from a contactless card, wherein:

the one or more information elements are configured to activate the contactless card, and

the one or more information elements include a first information element comprising a dynamically generated phone number,

validate the one or more information elements, and

after validating the one or more information elements, activating the contactless card.

[0008] There is disclosed a card activation system comprising: a contactless card including one or more processors and memory, wherein the memory contains one or more applets; a client application comprising instructions for execution on a client device including one or more processors and memory; and one or more servers, wherein the contactless card is configured to transmit a first set of information is transmitted to the client application upon entry of the contactless card into a communication field, the first set of information comprising one or more links configured to activate the contactless card, wherein the client application is configured to receive the first set of information from the contactless card and transmit to the one or more servers for validation, and wherein, upon the validation of the first set of information, the contactless card is activated.

[0009] There is disclosed a method of activating a contactless card, the method comprising the steps of: entering, by the contactless card, into a communication field; transmitting, by one or more applets contained in a memory of the contactless card, a first set of information to a client application comprising instructions for execution on a client device via the communication field, the first set of information comprising one or more links configured to activate the contactless card; transmitting, by the client application, the first set of information to one or more servers; performing, by one or more servers, one or more cryptographic operations to validate the first set of information; and activating, upon the validation of the first set of information, the contactless card.

[0010] Embodiments of the present disclosure provide a contactless card comprising: a processor; a memory, wherein the memory contains one or more applets and a first set of information, wherein, upon entry of the contactless card into a communication field, the one or more applets are configured to transmit the first set of information, wherein the first set of information comprises one or more links configured to activate the contactless card, the one or more links including a first information element and a second information element, and wherein the first information element comprises a phone number and the second information element comprises an encrypted payload.

[0011] 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.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] FIG. 1A is a diagram of a data transmission system according to an example embodiment.

CLAIMS

1. A contactless card, comprising:

a processor; and

a memory containing one or more applets and data,

wherein the processor is configured to transmit, after entry of the contactless card into a communication field, the data,

wherein the data comprises one or more information elements configured to activate the contactless card, and

wherein the one or more information elements including a first information element comprising a dynamically generated phone number.

2. The contactless card of claim 1, wherein the one or more information elements further comprise:

a second information element comprising one or more characters, and

a third information element comprising one or more encrypted payloads.

3. The contactless card of claim 2, wherein the one or more characters comprise one or more pauses associated with a phone call.

4. The contactless card of claim 2, wherein the one or more encrypted payloads include instructions for downloading an application compatible with the contactless card.

5. The contactless card of claim 2, wherein the one or more encrypted payloads include instructions for at least one selected from the group of (i) transferring a balance or other

amounts between one or more accounts associated with a user of the contactless card, (ii) resetting a personal identification number (PIN) associated with the user, the contactless card, or an account associated with the user, (iii) linking an account associated with the user that is not an account with an entity issuing the contactless card, (iv) approving or causing a transfer of a balance from one or more accounts to or from an account associated with the contactless card, and (v) requesting, from the entity issuing the contactless card, a card replacement.

6. The contactless card of claim 2, wherein the one or more encrypted payloads include instructions for at least one selected from the group of (i) requesting or causing an automated clearing house (ACH) payment to occur, (ii) approving or causing a wire transfer to occur from or to an account associated with a user of the contactless card, (iii) registering, verifying the registration of, or authenticating the user to allow, an account or contactless card associated with the user to be attached to a payment service associated with a device, and (iv) request an account activity including at least one selected from the group of a debt limit increase for a credit account, a request for an expedited transaction, and a request to dispute a transaction.

7. The contactless card of claim 1, wherein the contactless card is configured to initiate a phone call using the dynamically generated phone number after entry into a communication field.

8. The contactless card of claim 1, wherein:

the memory further contains an identification token, and

the processor is further configured to transmit the identification token with the data.

9. The contactless card of claim 1, wherein the contactless card is configured to stop the dynamic generation of the phone number upon receipt of an instruction.

10. A method of activating a contactless card, the method comprising the steps of:

dynamically generating, by a processor of the contactless card, a first set of information after entry of the contactless card into a communication field, the first set of information comprising one or more information elements configured to activate the contactless card;

transmitting, by processor, the first set of information to one or more servers for validation;

receiving, by the processor, an instruction to stop the dynamic generation the first set of information; and

responsive to the instruction, stopping, by the processor, dynamically generating the first set of information.

11. The method of claim 10, wherein:

the instruction is sent by the one or more servers upon validation of the first set of data, and

the instruction indicates activation of the contactless card.

12. The method of claim 10, wherein the one or more information elements comprise:

a first information element comprising a phone number,

a second information element comprising one or more characters, wherein the one or more characters comprise one or more pauses associated with a phone call, and

a third information element comprising one or more encrypted payloads.

13. The method of claim 12, further comprising decrypting, by the one or more servers, the one or more encrypted payloads with one or more keys.

14. The method of claim 13, further comprising triggering, by the one or more servers, upon unsuccessful decryption of the third information element, one or more processes based on one or more parameters associated with the contactless card.

15. The method of claim 14, wherein the one or more processes includes at least one selected from the group of routing a phone call to a desired recipient and prompting input of one or more parameters associated with the contactless card.

16. The method of claim 12, wherein the one or more encrypted payloads include instructions for downloading an application compatible with the contactless card.

17. A server, comprising:

a processor; and

a memory,

wherein the processor is configured to:

receive one or more information elements from a contactless card, wherein:

the one or more information elements are configured to activate the contactless card, and

the one or more information elements include a first information element comprising a dynamically generated phone number,

validate the one or more information elements, and

after validating the one or more information elements, activating the contactless card.

18. The server of claim 17, wherein the processor is further configured to receive the first set of information via a telephone call at the dynamically generated number.

19. The server of claim 17, wherein the processor is further configured to transmit, to the contactless card, an instruction to stop the dynamic generation of the phone number.

20. The server of claim 17, wherein, upon a determination of an incorrect phone number, the processor is further configured to:

flag the incorrect phone number, and

store the incorrect phone number in a database.