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 comprising one or more data records,

wherein the processor is configured to:

generate, after entry of the contactless card into a communication field of a client device, an activation link based on the one or more data records, the one or more data records comprising a dynamically generated phone number associated with a server and one or more unique identifiers, and

transmit the activation link to the client device, the activation link comprising the dynamically generated phone number and one or more encrypted payloads, the

activation link being configured to initiate a phone call, via the client device, to the dynamically generated phone number, to transmit the one or more encrypted payloads to the server for validation.

[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 an activation link from a contactless card, wherein the activation link is received via a telephone call to a phone number associated with the server, the activation link comprising an encrypted payload associated with one or more data elements stored on the contactless card,

validate the encrypted payload, and

after validating the encrypted payload, activating the contactless card.

[0007c] According to another aspect of the present invention, there is provided a method of activating a contactless card, the method comprising the steps of:

dynamically generating, by a processor of the contactless card, an activation link after entry of the contactless card into a communication field of a client device, the activation link comprising a phone number associated with a server and an encrypted payload;

initiating, via the client device upon receipt of the activation link, a phone call to the server;

transmitting, upon establishing a connection with the server, the activation link comprising the encrypted payload to the server for validation; and

transmitting, upon validation of the encrypted payload by the server, one or more instructions to 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.

CLAIMS

1. A contactless card, comprising:

a processor; and

a memory comprising one or more data records,

wherein the processor is configured to:

generate, after entry of the contactless card into a communication field of a client device, an activation link based on the one or more data records, the one or more data records comprising a dynamically generated phone number associated with a server and one or more unique identifiers, and

transmit the activation link to the client device, the activation link comprising the dynamically generated phone number and one or more encrypted payloads, the activation link being configured to initiate a phone call, via the client device, to the dynamically generated phone number, to transmit the one or more encrypted payloads to the server for validation.

2. The contactless card of claim 1, wherein the activation link further comprises:

one or more characters following the phone number, wherein the encrypted payload follows the one or more characters.

3. The contactless card of claim 2, wherein the one or more characters comprise one or more pauses associated with the 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 one or more encrypted payloads comprise the one or more unique identifiers stored in the memory of the contactless card.

8. The contactless card of claim 7, wherein:

the one or more unique identifiers correspond to 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, an activation link after entry of the contactless card into a communication field of a client device, the activation link comprising a phone number associated with a server and an encrypted payload;

initiating, via the client device upon receipt of the activation link, a phone call to the server;

transmitting, upon establishing a connection with the server, the activation link comprising the encrypted payload to the server for validation; and

transmitting, upon validation of the encrypted payload by the server, one or more instructions to the contactless card.

11. The method of claim 10, wherein:

the one or more instructions sent by the server indicate activation of the contactless card.

12. The method of claim 10, comprising:

receiving, by the processor, an instruction to stop the dynamic generation of the activation link; and

responsive to the instruction, stopping, by the processor, dynamic generation of the activation link.

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

14. The method of claim 13, further comprising:

triggering, by the server, upon unsuccessful decryption of the encrypted payload, one or more processes based on one or more parameters associated with the contactless card,

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.

15. The method of claim 10, wherein:

the activation link further comprises one or more comma characters following the phone number, and

a number of comma characters identifies a duration of time for establishing a phone connection and transmitting the encrypted payload.

16. The method of claim 12, wherein the encrypted payload comprises 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 an activation link from a contactless card, wherein the activation link is received via a telephone call to a phone number associated with the server, the activation link comprising an encrypted payload associated with one or more data elements stored on the contactless card,

validate the encrypted payload, and

after validating the encrypted payload, activate the contactless card.

18. The server of claim 17, wherein the phone number associated with the server is dynamically generated.

19. The server of claim 18, 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.