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] According to a first aspect, there is provided a contactless card, comprising: a processor; and a memory, the memory containing an applet and activation information, wherein the activation information comprises a link including an email address, an email field, and an encrypted payload, and wherein the applet is configured to, after an entry into a communication field: dynamically generate the email address, and transmit the activation information for validation.

[0007b] According to a second aspect, there is provided a method of activating a contactless card, the method comprising the steps of: dynamically generating, by an applet contained in a memory of the contactless card, an email address after entry of the contactless card into a communication field; transmitting, by the applet, activation information for validation, wherein the activation information comprises a link including the email address, an email field,

and an encrypted payload; and disabling, after activation of the contactless card, dynamic generation of the email address by the applet.

[0007c] According to a third aspect, there is provided a server, comprising: a processor; and a memory, wherein the processor is configured to: receive activation information comprising a link including an email address, an email field, and an encrypted payload, wherein the activation information is associated with a contactless card, validate the activation information, activate the contactless card, and transmit a notification regarding activation of the contactless card.

[0008] Embodiments of the present disclosure provide 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 one or more applets of the contactless card are configured to transmit a first set of information to the client application after 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 via an email program, wherein the client application is configured to receive the first set of information from the one or more applets of the contactless card and transmit to the one or more servers for validation, and wherein, upon the validation of the first set of information by the one or more servers, the contactless card is activated.

CLAIMS

What is claimed is:

1. A contactless card, comprising:

a processor; and

a memory, the memory containing an applet and activation information,

wherein the activation information comprises a link including an email address, an email field, and an encrypted payload, and

wherein the applet is configured to, after an entry into a communication field:

dynamically generate the email address, and

transmit the activation information for validation.

2. The contactless card of claim 1, wherein the email address precedes the email field.

3. The contactless card of claim 1, wherein the email field comprises a token.

4. The contactless card of claim 1, wherein the activation information comprises a uniform resource locator that is dynamically generated to activate the contactless card.

5. The contactless card of claim 1, wherein the activation information comprises a card verification value configured to activate the contactless card.

6. The contactless card of claim 1, wherein the encrypted payload comprises a one-time password.

7. The contactless card of claim 1, wherein the contactless card is configured to disable dynamic generation of the email address after activation of the contactless card.

8. The contactless card of claim 1, wherein the contactless card is configured to disable dynamic generation of the email address after an additional entry into the communication field.

9. The contactless card of claim 1, wherein the applet is further configured to transmit the activation for validation to a server via one or more intermediary devices.

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

dynamically generating, by an applet contained in a memory of the contactless card, an email address after entry of the contactless card into a communication field;

transmitting, by the applet, activation information for validation, wherein the activation information comprises a link including the email address, an email field, and an encrypted payload; and

disabling, after activation of the contactless card, dynamic generation of the email address by the applet.

11. The method of claim 10, wherein the encrypted payload comprises a limited use token.

12. The method of claim 10, wherein the email field comprises a token.

13. The method of claim 10, wherein the activation information comprises a uniform resource locator that is dynamically generated to activate the contactless card.

14. The method of claim 10, wherein the activation information comprises a card verification value configured to activate the contactless card.

15. The method of claim 10, wherein the encrypted payload comprises a one-time password.

16. The method of claim 10, wherein disabling the dynamic generation of the email address by the applet comprising transmitting, by a second applet, an instruction to the applet to halt the dynamic generation of the email address after an additional entry of the contactless card into a communication field.

17. A server, comprising:

a processor; and

a memory,

wherein the processor is configured to:

receive activation information comprising a link including an email address, an email field, and an encrypted payload, wherein the activation information is associated with a contactless card,

validate the activation information,

activate the contactless card, and

transmit a notification regarding activation of the contactless card.

18. The server of claim 17, wherein:

the email field comprises a “From” field, and

the processor is further configured to validate the activation information by validating the email field.

19. The server of claim 17, wherein:

the email field comprises an encrypted one-time password token, and

the processor is further configured to validate the activation information by decrypting and validating the one-time password token.

20. The server of claim 17, wherein the email address is dynamically generated by the contactless card.