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 an activation ~~information~~link, wherein the activation ~~information~~ link comprises a ~~link~~ universal resource locator (URL) including an email address~~, an email field,~~ and an encrypted payload, and wherein the applet is configured to, after an entry of the contactless card into a communication field of a client device: dynamically generate the ~~email address~~URL, and transmit the activation ~~information for~~ link including the URL to the client device, to facilitate a validation of the encrypted payload by a server communicatively coupled to the client device, wherein: the URL is configured to launch an email application on the client device and generate an email message, the email message contains the encrypted payload in a data field, and the contactless card is activated upon successful validation of the encrypted payload by the server.

[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~~activation link after entry of the contactless card into a communication field of a client device, the activation link comprising and an email address and an encrypted payload; transmitting, by the applet, the activation ~~information for validation, wherein the activation information comprises a link including the email address, an email field, and an encrypted payload~~ link to the client device, the activation link being configured to generate an email message, using an email application of the client device; receiving, by a server from the client device, the email message, including the encrypted payload, wherein the contactless card is activated upon successful validation of the encrypted payload by the server; 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, from a client device, ~~activation information comprising a link including~~ an email ~~address~~message, comprising an email data field, and storing an encrypted payload, wherein the ~~activation information is associated with~~ email message is transmitted in response to an activation link received via a read of a contactless card, validate the ~~activation information~~encrypted payload, activate the contactless card, and transmit a notification regarding activation of the contactless card to the client device.

[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 an activation ~~information~~link,

wherein the activation ~~information~~ link comprises a ~~link~~ universal resource locator (URL) including an email address~~, an email field,~~ and an encrypted payload, and

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

dynamically generate the ~~email address~~URL, and

transmit the activation ~~information for~~ link including the URL to the client device, to facilitate a validation of the encrypted payload by a server communicatively coupled to the client device, wherein:

the URL is configured to launch an email application on the client device and generate an email message,

the email message contains the encrypted payload in a data field, and

the contactless card is activated upon successful validation of the encrypted payload by the server.

2. The contactless card of claim 1, wherein the ~~email address precedes the email field~~ server associated with an activation of the contactless card is identified by the email address.

3. The contactless card of claim 1, wherein the ~~email~~ data field ~~comprises a token~~ corresponds to a subject line of the email message.

4. The contactless card of claim 1, wherein URL provided via the activation ~~information~~ link ~~comprises a uniform resource locator that~~ is dynamically generated to activate the contactless card based on the successful authentication of the encrypted payload.

5. The contactless card of claim 1, wherein the ~~activation information~~encrypted payload comprises a card verification value ~~configured to activate~~associated with 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 of the client device.

~~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.~~9. 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~~activation link after entry of the contactless card into a communication field of a client device, the activation link comprising and an email address and an encrypted payload;

transmitting, by the applet, the activation ~~information for validation, wherein the activation information comprises a link including the email address, an email field, and an encrypted payload~~ link to the client device, the activation link being configured to generate an email message, using an email application of the client device;

receiving, by a server from the client device, the email message, including the encrypted payload, wherein the contactless card is activated upon successful validation of the encrypted payload by the server; and

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

~~11.~~10. The method of claim ~~10~~9, wherein the encrypted payload comprises ~~a limited use~~ an encrypted one-time password token.

~~12.~~11. The method of claim ~~10~~9, wherein the encrypted payload is provided in an email data field ~~comprises a token~~ associated with the email message.

~~13~~12. The method of claim ~~10~~9, wherein the activation ~~information~~ link comprises a uniform resource locator that is dynamically generated to activate the contactless card.

~~14~~13. The method of claim ~~10~~9, wherein the ~~activation information~~encrypted payload comprises a card verification value ~~configured to activate~~associated with the contactless card.

~~15~~14. The method of claim 10, wherein the ~~encrypted payload comprises a~~ one-time password token is generated by the applet.

~~16~~15. The method of claim ~~10~~9, wherein disabling the dynamic generation of the email address by the applet compris~~es~~~~ing~~ transmitting, by a second applet, an instruction to the applet to halt the dynamic generation of the email ~~address~~ message after an additional entry of the contactless card into ~~a~~ the communication field.

~~17~~16. A server, comprising:

a processor; and

a memory,

wherein the processor is configured to:

receive, from a client device, ~~activation information comprising a link including~~ an email ~~address~~message, comprising an email data field, and storing an encrypted payload, wherein the ~~activation information is associated with~~email message is transmitted in response to an activation link received via a read of a contactless card,

validate the ~~activation information~~encrypted payload,

activate the contactless card, and

transmit a notification regarding activation of the contactless card to the client device.

~~18~~17. The server of claim ~~17~~16, wherein:

the email data field ~~comprises~~ corresponds to a ~~"From" field~~subject line of the email message, and

the processor is further configured to validate the ~~activation information~~encrypted payload by validating the email data field.

~~19~~18. The server of claim ~~17~~16, wherein:

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

the processor is further configured to ~~validate the activation information~~activate the contactless card by decrypting and validating the encrypted one-time password token.

~~20~~19. The server of claim ~~17~~16, wherein the email ~~address is dynamically generated by the contactless card~~ data field corresponds to a "From" field of the email message.

20. The server of claim 16, wherein the notification comprises at least one selected from the group of a text message and an email.