

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.

[0007a] According to a first aspect of the present disclosure, there is provided a data transmission system, including a contactless card, including a processor; and a memory, the memory of the contactless card containing a card key and transmission data; and an application executing on a receiving device communicatively coupled with the contactless card, wherein, after entry into a communication field of the receiving device, the contactless card is configured to: ~~generate a cryptogram~~, encrypt the transmission data using a cryptographic algorithm and the card key to yield encrypted transmission data, transmit the encrypted transmission data to the application~~cryptogram~~, and transmit a tap password to the application, the tap password corresponding to a number of taps of the contactless card against the receiving device, and wherein the application is configured to: verify the tap password received from the contactless card, and transmit the encrypted transmission data to a server for validation of one or more transactions.

[0007b] According to a second aspect of the present disclosure, there is provided a method for transmitting data by a contactless card having a processor and a memory, the memory containing a card key and transmission data, the method including: ~~generating a cryptogram~~; encrypting the transmission data~~cryptogram~~ using the card key to yield an encrypted transmission data;

transmitting, via a short-range wireless communication, the encrypted transmission data to an application executing on a receiving device~~cryptogram;~~~~and~~ transmitting a tap password to the receiving device, wherein the tap password corresponds to a number of taps of the contactless card against the receiving device; verifying, by the application, the tap password received from the contactless card; and transmitting the encrypted transmission data to a server for validation of one or more transactions.

[0007c] According to a third aspect of the present disclosure, there is provided a server, including a processor₃; and a memory, the memory containing a key, a reference tap password, and an application including instructions for execution by the processor, wherein, the application is configured to: receive, from a receiving device, an~~encrypted~~ cryptogram generated by a contactless card, decrypt the~~encrypted~~ cryptogram using the key, request a tap password, the tap password including a plurality of taps of a contactless card on the receiving device, and receive ~~the~~a tap password via a network communication with the receiving device.

CLAIMS

1. A data transmission system, comprising:

a contactless card, comprising:

a processor; and

a memory, the memory of the contactless card containing a card key and transmission data;

and;

an application executing on a receiving device communicatively coupled with the contactless card,

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

~~generate a cryptogram;~~

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

transmit the encrypted transmission data to the application~~cryptogram~~, and

transmit a tap password to the application, the tap password corresponding to a

number of taps of the contactless card against the receiving device, and

wherein the application is configured to:

verify the tap password received from the contactless card, and

transmit the encrypted transmission data to a server for validation of one or more transactions.

2. The data transmission system of claim 1, wherein the tap password ~~corresponds~~comprises to a duration of one or more ~~plurality of~~ taps of the contactless card on ~~the~~ receiving device.

~~3. The data transmission system of claim 2, wherein the taps comprising the plurality of taps are at least one selected from the group of a tap directly on the receiving device and a tap directly on an intermediary device that is transmitted to the receiving device.~~

~~4.3.~~ The data transmission system of claim 12, wherein the receiving device comprises at least one selected from the group of a mobile device, a smart device, a terminal, a server, and a wearable device.

~~5.4.~~ The data transmission system of claim 12, wherein:

the tap password is associated with a sequence of at least one selected from the group of a first set of taps and a second set of taps performed by the contactless card, and

the first set of taps comprises one or more taps having a first duration and the second set ~~second~~ of taps comprises one or more taps having a second duration.

~~6.5.~~ The data transmission system of claim 12, wherein:

the number~~plurality~~ of taps comprises ~~a~~ two short taps and one long tap, and each of the two short taps has ~~ve~~ a duration less than a duration of the long tap.

~~7.6.~~ The data transmission system of claim 1, ~~further comprising an application comprising instructions for execution on the receiving device~~, wherein:

the application is configured to request a tap password from the contactless card, and

the contactless card is configured to transmit the tap password in response to the request.

~~8.7.~~ The data transmission system of claim ~~67~~, wherein the transmission data includes a reference tap password stored onto the contactless card and the application is configured to ~~verify~~validate the tap password by comparison with ~~the~~ reference tap password.

~~9.8.~~ The data transmission system of claim ~~78~~, wherein, upon validation of the tap password, the application is configured to approve a transaction that exceeds a threshold value.

~~10.9.~~ A method for transmitting data by a contactless card having a processor and a memory, the memory containing a card key and transmission data, the method comprising:

~~generating a cryptogram;~~

encrypting the ~~transmission data~~cryptogram using the card key to yield an encrypted transmission data;

transmitting, via a short-range wireless communication, the encrypted transmission data to an application executing on a receiving device~~cryptogram~~; and

transmitting a tap password to the receiving device, wherein the tap password corresponds to a number of taps of the contactless card against the receiving device;

verifying, by the application, the tap password received from the contactless card; and

transmitting the encrypted transmission data to a server for validation of one or more transactions.

~~11.10.~~ The method of claim ~~940~~, wherein the tap password is further associated with~~comprises~~ a duration of each tap in the number~~plurality~~ of taps of the contactless card on ~~the~~ receiving device.

~~12.~~ The method of claim ~~11~~, wherein the plurality of taps comprises a sequence of taps.

~~13.~~11. The method of claim ~~10~~1, wherein the tap password corresponds to a sequence plurality of taps comprises ~~ing~~es a two short taps and one long tap.

~~14.~~12. The method of claim ~~11~~3, wherein:

each of the two short taps lasts ~~s~~ less than one second, and
the long tap lasts more than one second.

~~15.~~13. The method of claim ~~11~~3, wherein the two short taps and the one long tap may occur in any order.

~~16.~~14. The method of claim ~~9~~10, wherein the tap password, generated by the contactless card, specifies an order in which the contactless card was read by the receiving device for ~~the plurality of taps~~ a transaction involving one or more distinct contactless cards.

~~17.~~15. The method of claim ~~9~~10, further comprising, prior to the transmission of the tap password, receiving a request for the tap password from ~~the~~an application executing~~comprising~~ instructions for execution on ~~the~~a receiving device.

~~18.~~16. A server, comprising:

a processor; ~~;~~ and

a memory, the memory containing a key, a reference tap password, and an application comprising instructions for execution by the processor,

wherein, the application is configured to:

receive from a receiving device, an encrypted cryptogram generated by a contactless card,

decrypt the ~~encrypted~~ cryptogram using the key,

request a tap password, the tap password comprising a number~~plurality~~ of taps of a contactless card against the receiving device, and

receive ~~the~~ tap password via a network communication with the receiving device.

~~19.17.~~ The server of claim 1~~6~~8, wherein the application is further configured to:

compare the tap password to the reference password, and

upon determining that the tap password matches the reference password, authorize a transaction.

~~20. The server of claim 18, wherein the application is configured to receive the tap password from the contactless card via an intermediary device.~~

18. The data transmission system of claim 1, wherein the application is further configured to:

read a tap password stored on the contactless card, and

match the stored tap password with the transmitted tap password corresponding to a pattern of taps against the receiving device.

19. The data transmission of claim 1, wherein the transmission data includes at least one of account information associated with a user financial account and payment information associated with the user financial account.

20. The server of claim 16, wherein the number of taps corresponding to the tap password is associated with a number of taps and a duration of each tap applied, by the contactless card, against the receiving device.