

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 an aspect of the present disclosure, there is provided a system, comprising: a contactless card comprising a processor and a memory; and a server, wherein the server is configured to: identify a transaction ~~between an account and~~ associated with a transaction request received from a merchant, identify the transaction as high risk, transmit ~~an a contactless~~ authentication request to a client application in wireless communication with the contactless card, the authentication request prompting for entry of the contactless card into a communication field of a client device executing the client application, receive, responsive to the authentication request, a cryptogram generated by the contactless card, wherein the cryptogram is transmitted to the server via the client device, verify the cryptogram based on a session key using a cryptographic algorithm, and authorize the transaction based on the verified cryptogram.

[0007b] According to another aspect of the present disclosure, there is provided a method for secure electronic authentication with a contactless card, the method comprising: identifying, by a processor, a transaction between an account and a merchant; identifying, by the processor, the transaction as high risk; transmitting, by the processor, ~~an~~ a contactless authentication request to a client application in wireless communication with the contactless card, the authentication request prompting for entry of the contactless card into a communication field of a client device executing the client application; receiving, by the processor responsive to the authentication request, a cryptogram generated by the contactless card, wherein the cryptogram is transmitted to the server via the client device; verifying, by the processor, the cryptogram based on a session key using a cryptographic algorithm; and authorizing, by the processor, the transaction based on the verified cryptogram.

[0007c] According to yet another aspect of the present disclosure, there is provided a server, comprising: a processor, wherein the processor is configured to: identify a transaction ~~between an account and~~ associated with a transaction request received from a merchant, identify the transaction as high risk, transmit ~~an~~ a contactless authentication request to a client application in wireless communication with a contactless card, the authentication request prompting for entry of the contactless card into a communication field of a client device executing the client application, receive, responsive to the contactless authentication request, a cryptogram generated by the contactless card, wherein the cryptogram is transmitted to the server via the client device, verify the cryptogram based on a session key using a cryptographic algorithm, and authorize the transaction based on the verified cryptogram.

[0008] Embodiments of the present disclosure provide an authentication system comprising: an authentication server; a client application comprising instructions for execution on a client device in data communication with the authentication server; and a contactless card

containing a processor and a memory; wherein the authentication server is configured to: receive a transaction request, wherein the transaction request includes account information for an account requesting to engage in a transaction and transaction information for the transaction, in response to receiving the transaction request, send an authentication request to the client application requesting at least one authentication factor when a value of the transaction exceeds a predetermined value, wherein the at least one authentication factor includes a cryptogram generated by placing the contactless card in a communication field of the client device, receive an authentication signal from the client device, the authentication

CLAIMS

~~What is claimed is:~~

1. A system, comprising:

a contactless card comprising a processor and a memory; and

a server,

wherein the server is configured to:

identify a transaction ~~between an account and~~ associated with a transaction request received from a merchant,

identify the transaction as high risk,

transmit ~~an a contactless~~ authentication request to a client application in wireless communication with the contactless card, the authentication request prompting for entry of the contactless card into a communication field of a client device executing the client application,

receive, responsive to the authentication request, a cryptogram generated by the contactless card, wherein the cryptogram is transmitted to the server via the client device,

verify the cryptogram based on a session key using a cryptographic algorithm, and

authorize the transaction based on the verified cryptogram.

2. The system of claim 1, wherein the server is further configured to:

generate an authentication diversified key based on a master key and a unique identifier,

and

generate the session key based on the authentication diversified key.

3. The system of claim 1, wherein the identification of the transaction as high risk is based on a comparison of the transaction with a historical transaction pattern ~~for the account.~~

4. The system of claim 3, wherein the transaction is conducted at a time that is inconsistent with the historical transaction pattern.

5. The system of claim 3, wherein the transaction is conducted at a geographical region that is inconsistent with the historical transaction pattern.

6. The system of claim 1, wherein the identification of the transaction as high risk is based on an association of the merchant with a fraudulent transaction.

7. The system of claim 1, wherein:

the identification of the transaction as high risk is based on the location of the merchant,
and

the location of the merchant is in a geographical region associated with fraudulent transactions.

~~8. The system of claim 1, wherein the cryptogram is generated by a contactless card and transmitted to the server via an intermediary device.~~

~~9.8.~~ The system of claim 1, wherein:

the server is further configured to transmit a second authentication request for at least one selected from the group of biometric information and a password, and

the server is further configured to delay the transaction pending the authentication request.

~~10.9.~~ The system of claim 1, wherein the server is further configured to:

prior to transmitting the authentication request, compare the value of the transaction to a threshold, and

transmit the authentication request if the value of the transaction exceeds the threshold.

~~11.10.~~ A method for secure electronic authentication with a contactless card, the method comprising:

identifying, by a processor, a transaction between an account and a merchant;

identifying, by the processor, the transaction as high risk;

transmitting, by the processor, ~~an~~ a contactless authentication request to a client application in wireless communication with the contactless card, the authentication request prompting for entry of the contactless card into a communication field of a client device executing the client application;

receiving, by the processor responsive to the authentication request, a cryptogram generated by the contactless card, wherein the cryptogram is transmitted to the server via the client device;

verifying, by the processor, the cryptogram based on a session key using a cryptographic algorithm; and

authorizing, by the processor, the transaction based on the verified cryptogram.

~~12.11.~~ The method of claim ~~11~~10, further comprising:

generating, by the processor, an authentication diversified key based on a master key and a unique identifier; and

generating, by the processor, the session key based on the authentication diversified key.

~~13.~~12. The method of claim ~~11~~10, further comprising transmitting, by the processor, a second authentication request for at least one selected from the group of biometric information and a password.

~~14.~~13. The method of claim ~~11~~10, further comprising delaying, by the processor, the transaction pending the authentication request.

~~15.~~14. The method of claim ~~11~~10, wherein identifying the transaction as high risk comprises:

comparing, by the processor, the transaction with a historical transaction pattern for the account, and

determining the transaction is conducted at a time that is inconsistent with the historical transaction pattern.

~~16.~~15. The method of claim ~~11~~10, wherein identifying the transaction as high risk comprises:

comparing, by the processor, the transaction with a historical transaction pattern for the account, and

determining the transaction is conducted in a geographical region that is inconsistent with the historical transaction pattern.

[17.16.](#) A server, comprising:

a processor,

wherein the processor is configured to:

identify a transaction ~~between an account and~~ associated with a transaction request received from a merchant,

identify the transaction as high risk,

transmit ~~an a contactless~~ authentication request to a client application in wireless communication with a contactless card, the authentication request prompting for entry of the contactless card into a communication field of a client device executing the client application,

receive, responsive to the contactless authentication request, a cryptogram generated by the contactless card, wherein the cryptogram is transmitted to the server via the client device,

verify the cryptogram based on a session key using a cryptographic algorithm, and

authorize the transaction based on the verified cryptogram.

[18.17.](#) The server of claim [17.16](#), wherein the processor is further configured to:

generate an authentication diversified key based on a master key and a unique identifier,

and

generate the session key based on the authentication diversified key.

~~19.~~18. The server of claim ~~17~~16, wherein the identification of the transaction as high risk is based on an association of the merchant with a fraudulent transaction.

~~20.~~19. The server of claim ~~17~~16, wherein:

identification of the transaction as high risk is based on the location of the merchant, and the location of the merchant is in a geographical region associated with fraudulent transactions.

20. The server of claim 16, wherein:

the server is further configured to transmit a second authentication request for at least one selected from the group of biometric information and a password to the client device.