

Further, while the growing use of chip-based financial cards provides more secure features 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, there is provided a server, comprising: a processor; and a memory, wherein the processor is configured to: generate a session key based on an authentication diversified key, validate a cryptographic result using one or more cryptographic algorithms and the session key, wherein the cryptographic result is generated by a contactless card based on a counter value stored on the contactless card and transmitted to the server via an intermediary device with wireless connectivity to the contactless card~~authenticate one or more login credentials~~, and authorize, based on a validation of the authentication~~cryptographic result~~, sharing of information with a third-party data requestor.

[0007b] According to a second aspect, there is provided a method, comprising the steps of: generating, by ~~the a~~ processor, an authentication diversified key based on a master key and a unique identifier; generating, by ~~a the~~ processor, a session key based on the authentication diversified key; validating, by the processor, a cryptographic result using one or more cryptographic algorithms and the session key, wherein the cryptographic result is generated by a contactless card using a counter value stored on the contactless card, and transmitted to the processor via an intermediary device with wireless connectivity to the contactless card; ~~authenticating, by the processor, one or more login credentials;~~ and authorizing, by the processor, based on a validation of the cryptographic result, sharing of information with a data-requesting party.

[0007c] According to a third aspect, there is provided a contactless card, comprising: a processor; and a memory, ~~the memory containing a counter value and one or more keys; and a communication interface,~~ wherein the processor is configured to: create, in response to a contactless authentication request transmitted from a server communicatively coupled with the contactless card via an intermediary device associated with a user, a first cryptogram using a first counter value associated with a contactless card, transmit the first cryptogram, via the intermediary device, to the server to authorize access to one or more sensitive user data records, create, upon a validation of the first cryptogram by the server, a second cryptogram using a second counter value, the second cryptogram comprising the one or more sensitive user data records, and transmit the second cryptogram, via the intermediary device, to a third-party data requestor. ~~update the counter value when the communication interface is within a range of a first communication field, create a first cryptographic result based on the one or more keys and the counter value, transmit, via the first communication field, the first~~

~~cryptographic result, update the counter value when the communication interface is within a range of a second communication field, create a second cryptographic result based on the one or more keys and the counter value, and transmit, via the second communication field, the second cryptographic result, wherein the second cryptographic result authorizes access to data.~~

[0008] Embodiments of the present disclosure provide a transmitting device comprising: a memory including a counter value, and a plurality of keys; a communication interface; and one or more processors in communication with the memory and communication interface, wherein the one or more processors is configured to: update the counter value when the communication interface is within a range of a first active communication field of a first receiving device; create a first cryptogram based on the plurality of keys and the counter value; transmit the first cryptogram, via the first active communication field, to the first receiving device; receive, from the first receiving device, an authentication request for sensitive data; update the counter value when the communication interface is within a range

CLAIMS

~~What is claimed is:~~

1. A server, comprising:

a processor; and

a memory,

wherein the processor is configured to:

generate a session key based on an authentication diversified key,

validate a cryptographic result using one or more cryptographic algorithms

and the session key, wherein the cryptographic result is generated by a contactless card based on a counter value stored on the contactless card and transmitted to the server via an intermediary device with wireless connectivity to the contactless card, and

~~authenticate one or more login credentials, and~~

authorize, based on a validation of the authentication cryptographic result,

sharing of information with a third-party data requestor.

2. The server of claim 1, wherein:

the processor is further configured to transmit a request, to the intermediary device, and
the request corresponding to a contactless authentication request generated in response to
a data request for sensitive user information received from the third-party data requestor.
~~the information is associated with the request.~~

3. The server of claim 2, wherein the contactless authentication request is associated with a predetermined time out period.

4. The server of claim 2, wherein the processor is further configured to authorize sharing of one or more portions of the information ~~associated with the request~~third-party data requestor, based on authenticating ~~the one or more login credentials via one or more challenges~~provided by a user via the intermediary device.

5. The server of claim 4, wherein the one or more portions corresponds to a proof of age.

6. The server of claim 1, wherein:

the memory includes a master key and a unique identifier, and

the processor is further configured to generate the authentication diversified key based on the master key and ~~a~~the unique identifier.

~~7. The server of claim 1, wherein the cryptographic result is generated by a contactless card based on a counter value using the one or more cryptographic algorithms.~~

8.7. The server of claim ~~1~~2, wherein the processor is further configured to ~~authorize sharing of~~share a public key with the third-party data requestor for decryption of the one or more portions of the sensitive user information ~~associated with the request~~.

9.8. The server of claim ~~1~~2, wherein:

~~the information comprises sensitive information, and~~

the sensitive user information is retrieved from a secure element associated with the server.

~~10.9.~~ 10.9. A method, comprising the steps of:

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

generating, by ~~a the~~ processor, a session key based on the authentication diversified key;

validating, by the processor, a cryptographic result using one or more cryptographic algorithms and the session key, wherein the cryptographic result is generated by a contactless card using a counter value stored on the contactless card, and transmitted to the processor via an intermediary device with wireless connectivity to the contactless card; and

~~authenticating, by the processor, one or more login credentials; and~~

authorizing, by the processor, based on a validation of the cryptographic result, sharing of information with a data-requesting party.

~~11.10.~~ 11.10. The method of claim ~~109~~, further comprising:

transmitting, by the processor, a contactless authentication request to the intermediary device for contactless authentication with the contactless card,

wherein the contactless authentication request initiates the generation of the cryptographic result by the contactless card upon entering a communication field of the intermediary device.~~information is associated with the request, and~~

~~wherein the request is associated with a predetermined time-out period.~~

~~12.11.~~ 12.11. The method of claim ~~119~~, further comprising authorizing, by the processor, sharing of one or more portions of the information associated with the request

based on authenticating ~~the~~ one or more login credentials ~~via one or more challenges~~
provided by a user via the intermediary device.

13.12. The method of claim ~~109~~, wherein the information comprises sensitive information.

14.13. The method of claim ~~109~~, wherein the cryptographic result is generated ~~based on a counter value~~ using the one or more cryptographic algorithms.

15.14. The method of claim ~~109~~, further comprising retrieving, by the processor, the information from a secure element associated with the processor.

15. The method of claim 10, wherein the contactless authentication request is associated with a predetermined time out period.

16. The method of claim 10, wherein the contactless authentication request initiates a user notification to be displayed on the intermediary device.

17. The method of claim 16, wherein the user notification prompts the user to perform a contactless authentication using the contactless card and the intermediary device.

18. The method of claim 9, wherein sharing of information with the data-requesting party comprises signing of the information with a private key stored on the contactless

card, the information, signed with the private key, being transmitted to the data-requesting party by the intermediary device.

19. The method of claim 18, further comprising sharing, by the processor, a public key with the data-requesting party for decryption of the information.

20. A contactless card, comprising:

a processor; and

a memory,

wherein the processor is configured to:

create, in response to a contactless authentication request transmitted from a server communicatively coupled with the contactless card via an intermediary device associated with a user, a first cryptogram using a first counter value associated with a contactless card,

transmit the first cryptogram, via the intermediary device, to the server to authorize access to one or more sensitive user data records,

create, upon a validation of the first cryptogram by the server, a second cryptogram using a second counter value, the second cryptogram comprising the one or more sensitive user data records, and

transmit the second cryptogram, via the intermediary device, to a third-party data requestor.

16. A contactless card, comprising:

a processor; and

a memory, the memory containing a counter value and one or more keys; and

a communication interface,

wherein the processor is configured to:

~~update the counter value when the communication interface is within a range of a first communication field,~~

~~create a first cryptographic result based on the one or more keys and the counter value,~~

~~transmit, via the first communication field, the first cryptographic result,~~

~~update the counter value when the communication interface is within a range of a second communication field,~~

~~create a second cryptographic result based on the one or more keys and the counter value, and~~

~~transmit, via the second communication field, the second cryptographic result, wherein the second cryptographic result authorizes access to data.~~

~~17. The contactless card of claim 16, wherein, prior to updating the counter value when the communication interface is within a range of the second communication field, the processor is further configured to:~~

~~receive, via the communication interface, a request for data via the first communication field,~~

~~wherein the transmission of the second cryptographic result via the second communication field, is responsive to the request, and~~

~~wherein the data is associated with the request.~~

~~18. The contactless card of claim 17, wherein the request expires after authorized access to the data.~~

~~19. The contactless card of claim 16, wherein the processor is further configured to transmit one or more login credentials via the second communication field.~~

~~20. The contactless card of claim 16, wherein:~~

~~the data comprises personally identifiable information, and~~

~~the data is stored in at least one selected from the group of a cloud storage, a secure element, and a blockchain.~~