

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] In a first aspect, the present disclosure provides a server, comprising: a processor; and a memory, wherein the memory stores a server counter, the server counter being updated for each transaction conducted with a contactless card, wherein the processor is configured to: receive a card counter value from a client device, the card counter value being stored on the contactless card and corresponding to a number of reads of the contactless card by the client device, compare the card counter value received from the client device, to the server counter for synchronization, resynchronize the card counter value, and authenticate the contactless card based on the resynchronization of the card counter.

[0007b] In a second aspect, the present disclosure provides a method of resynchronization, comprising: receiving, by a server comprising a processor and a memory storing a server counter, a card counter from a client device, the card counter tracking reads of a contactless card by the client device; comparing, by the server, the card counter to the server counter for synchronization; resynchronizing, by the server, the card counter; and authenticating, by the server, the contactless card based on the resynchronization of the card counter.

[0007c] In a third aspect, the present disclosure provides a resynchronization system, comprising: a contactless card including a processor and a memory, the memory of the contactless card storing a card counter; and a server in data communication with the contactless card via a client device, the server including a processor and a memory, the memory of the server storing a server counter, wherein: the contactless card is configured to transmit the card counter to the server, via the client device, the client device being configured to establish a short-range wireless communication with the contactless card, the server is configured to compare the card counter to the server counter for synchronization; the contactless card and the server are configured to resynchronize the card counter, and the server is configured to authenticate the contactless card based on the resynchronization of the card counter.

[0008] Embodiments of the present disclosure provide a counter resynchronization system comprising: a contactless card including one or more processors, and a memory, wherein the memory comprises one or more applets and a counter; a client application comprising instructions for execution on a client device including one or more processors and a memory; and one or more servers in data communication with the client application, the one or more servers including a memory comprising an expected counter value, wherein the client application is configured to read the counter from the contactless card and transmit the counter to the one or more servers, wherein the one or more servers are configured to compare the counter to the expected counter value for synchronization; wherein the contactless card and the one or more servers are configured to resynchronize the counter, via one or more processes, based on one or more reads of the one or more applets, and wherein the one or more servers are configured to authenticate the contactless card based on the resynchronization.

CLAIMS

~~What is claimed is:~~

1. A server, comprising:
 - a processor; and
 - a memory, wherein the memory stores a server counter, the server counter being updated for each transaction conducted with a contactless card,wherein the processor is configured to:
 - receive a card counter value from a client device, the card counter value being stored on the contactless card and corresponding to a number of reads of the contactless card by the client device,
 - compare the card counter value received from the client device, to the server counter for synchronization,
 - resynchronize the card counter value, and
 - authenticate the contactless card based on the resynchronization of the card counter.
2. The server of claim 1, wherein the card counter value is configured to ~~signal~~ prevent an attack associated with a fraudulent use of the contactless card.
3. The server of claim 2, wherein the attack is associated with physical access to the contactless card.
4. The server of claim 1, wherein ~~the processor is configured to receive~~ the card counter value is read from the contactless card via ~~an intermediary~~ near field communication with the client device.
5. A method of resynchronization, comprising:

receiving, by a server comprising a processor and a memory storing a server counter, a card counter from a client device, the card counter tracking reads of a contactless card by the client device;

comparing, by the server, the card counter to the server counter for synchronization;

resynchronizing, by the server, the card counter; and

authenticating, by the server, the contactless card based on the resynchronization of the card counter.

6. The method of claim 5, wherein the resynchronizing reads of the card counter is-are based on a read of an applet contained in a memory of the contactless card.

7. The method of claim 6, further comprising:

performing, by an application comprising instructions for execution on a-the client device, the read of the applet during a gesture of the contactless card within a communication field of the client device; and

receiving, by the server from the application, the read so as to resynchronize the card counter.

8. The method of claim 7, further comprising:

determining, by the server, if an adjustment of the card counter belongs to a first sequence within a first window, and

determining, by the server, that the adjustment of the card counter does not belong to the first sequence within the first window.

9. The method of claim 8, further comprising:

after an additional gesture of the contactless card within the communication field, determining, by the server, that the card counter is within a second window, and resynchronizing the card counter.

10. The method of claim 9, wherein the second window includes a second sequence.
11. The method of claim 8, further comprising:
- after an additional gesture of the contactless card within the communication field,
- determining, by the server, that the card counter is outside of a second window; and
- deactivating, by the server, the contactless card.
12. The method of claim 5, wherein the card counter is configured to ~~signal-prevent~~ an attack associated with a fraudulent use of the contactless card.
13. The method of claim 12, wherein the attack comprises at least one selected from the group of an attempted extraction of a master key from a secure element of the contactless card, a side channel attack of the contactless card, and a fuzzing of the contactless card.
14. A resynchronization system, comprising:
- a contactless card including a processor and a memory, the memory of the contactless card storing a card counter; and
- a server in data communication with the contactless card via a client device, the server including a processor and a memory, the memory of the server storing a server counter, wherein:
- the contactless card is configured to transmit the card counter to the server, via the client device, the client device being configured to establish a short-range wireless communication with the contactless card,
- the server is configured to compare the card counter to the server counter for synchronization,
- the contactless card and the server are configured to resynchronize the card counter, and

the server is configured to authenticate the contactless card based on the resynchronization of the card counter.

15. The resynchronization system of claim 14, wherein the card counter is configured to ~~signal-prevent~~ an attack associated with a fraudulent use of the contactless card.

16. The resynchronization system of claim 15, wherein the attack comprises an impersonation attack.

17. The resynchronization system of claim 14, wherein:

the contactless card is configured to decrement the card counter in a pre-generated sequence, and

the server is configured to decrement the server counter in the pre-generated sequence.

18. The resynchronization system of claim 14, wherein the contactless card is configured to decrement the card counter in a non-monotonic sequence.

19. The resynchronization system of claim 14, wherein the contactless card is configured to increment the card counter in a non-monotonic sequence.

20. The resynchronization system of claim 14, wherein:

the memory of the contactless card further contains an applet, and

upon detection of an attack, the applet is configured to transition to a non-functional state.