

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] There are disclosed 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 invention, there is provided a contactless card, comprising:

- a processor; and

- a memory, the memory containing a first private key generated by diversifying a master key with a unique card identifier, transmission data, and a counter value,

- wherein the contactless card is configured to:

- generate, after entry into a communication field of a client device, a first diversified key by encrypting the counter value with the first private key,

- encrypt the transmission data using the first diversified key to yield an encrypted transmission data, and

transmit a cryptographic result comprising the counter value and the encrypted transmission data, via the client device, to a server, for decryption with a second diversified key generated from a public key associated with the master key and the counter value.

[0007b] According to a second aspect of the present invention, there is provided a method for transmitting data by a contactless card having a processor and a memory containing a first private key, transmission data, and a counter, the method comprising:

generating, by the contactless card upon entry into a communication field of a client device, a first diversified key by encrypting the counter using the first private key;

generating a first public key based on the first private key;

encrypting the transmission data using the first private key to yield an encrypted transmission data;

encrypting the transmission data using the first diversified key ; and

transmitting a cryptographic result comprising the counter and the encrypted transmission data, via the client device to a server; and

decrypting, by the server, the cryptographic result with a second diversified key generated from the public key and the counter.

[0007c] According to a third aspect of the present invention, there is provided a data transmission system, comprising:

a contactless card having a processor and a memory, the memory containing a first private key generated by diversifying a master key with a unique card identifier, a transmission data and a counter value,

wherein the contactless card, when within a communication range of a client device, is configured to:

encrypt the transmission data using the first private key and the counter value,
and

transmit a cryptographic result comprising the encrypted transmission data
and the counter value, to an application on the client device, via near field
communication; and

a server storing a first public key associated with the first private key, the server
being communicatively coupled with the application running on the client device, wherein
the server is configured to:

receive, from the contactless card via the application, the cryptographic
result,

decrypt the cryptographic result using the first public key generated from the
master key and the counter.

[0008] A data transmission system can include, for example, a transmitting device having
a transmitting device processor and a transmitting device memory, the transmitting device
memory containing a first master key, transmission data and a counter value; a receiving
device having a receiving device processor and a receiving device memory, the receiving
device memory containing a second master key; where the transmitting device is
configured to: generate a first diversified key using the first master key and a first
cryptographic algorithm(s) and store the first diversified key in the transmitting device
memory, where the first master key is a secret key, protect the counter value using a
second cryptographic algorithm(s) and the first diversified key to yield a cryptographic
result including the counter value, encrypt the transmission data using a third
cryptographic algorithm(s) and the first diversified key to yield encrypted transmission
data, and transmit the protected counter value

CLAIMS

1. A contactless card, comprising:

a processor; and

a memory, the memory containing a first private key generated by diversifying a master key with a unique card identifier, transmission data, and a counter value,

wherein the contactless card is configured to:

generate, after entry into a communication field of a client device, a first diversified key by encrypting the counter value with the first private key,

encrypt the transmission data using the first diversified key to yield an encrypted transmission data, and

transmit a cryptographic result comprising the counter value and the encrypted transmission data, via the client device, to a server, for decryption with a second diversified key generated from a public key associated with the master key and the counter value.

2. The contactless card of claim 1, wherein the contactless card is further configured to encrypt the cryptographic result using a public key of the server.

3. The contactless card of claim 1, wherein one or more encryption processes associated with the first diversified key correspond to at least one selected from the group of an asymmetric encryption algorithm, a digital signature algorithm, an ElGamal encryption algorithm, an elliptical curve algorithm, and a Paillier cryptosystem algorithm.

4. The contactless card of claim 1, wherein the cryptographic result includes a one-time passcode.
5. The contactless card of claim 1, wherein the first diversified key is generated for each transmission between the contactless card and the server.
6. The contactless card of claim 1, wherein the public key is stored on the contactless card.
7. The contactless card of claim 6, wherein the contactless card is further configured to generate the second diversified key by encrypting the counter value with the public key and send the second diversified key to the server.
8. The contactless card of claim 6, wherein the public key is signed with the first private key to enable a receiving server to verify an authenticity of the public key.
9. The contactless card of claim 1, wherein the transmission data comprises activation data for the contactless card.
10. The contactless card of claim 6, wherein the first public key is transmitted to the server via the cryptographic result.
11. A method for transmitting data by a contactless card having a processor and a memory containing a first private key, transmission data, and a counter, the method comprising:
 - generating, by the contactless card upon entry into a communication field of a client device, a first diversified key by encrypting the counter using the first private key;

generating a first public key based on the first private key;
encrypting the transmission data using the first private key to yield an encrypted transmission data;
encrypting the transmission data using the first diversified key;
transmitting a cryptographic result comprising the counter and the encrypted transmission data, via the client device, to a server; and
decrypting, by the server, the cryptographic result with a second diversified key generated from the public key and the counter.

12. The method of claim 11, further comprising storing the first public key on the contactless card and transmitting the first public key to the server along with the cryptographic result.

13. The method of claim 11, further comprising encrypting the cryptographic result with a public key of the server.

14. A data transmission system, comprising:

a contactless card having a processor and a memory, the memory containing a first private key generated by diversifying a master key with a unique card identifier, a transmission data and a counter value,

wherein the contactless card, when within a communication range of a client device, is configured to:

encrypt the transmission data using the first private key and the counter value,

and

transmit a cryptographic result comprising the encrypted transmission data and the counter value, to an application on the client device, via near field communication; and

a server storing a first public key associated with the first private key, the server being communicatively coupled with the application running on the client device, wherein the server is configured to:

receive, from the contactless card via the application, the cryptographic result,

decrypt the cryptographic result using the first public key generated from the master key and the counter.

15. The data transmission system of claim 14, wherein the contactless card is further configured to sign the counter value using the first private key prior to transmission of the cryptographic result to the application running on the client device.

16. The data transmission system of claim 14, wherein the contactless card is further configured to encrypt the cryptographic result with a public key of the server.

17. The data transmission system of claim 14, wherein the cryptographic result includes a one-time password.

18. The data transmission system of claim 14, wherein:

the transmission data comprises activation data for the contactless card, and

the server is further configured to activate the contactless card using the activation data.

19. The data transmission system of claim 14, wherein the first public key is stored on the contactless card and transmitted to the server along with the cryptographic result.

20. The data transmission system of claim 14, wherein the cryptographic result is retrieved by the server via a read of the contactless card by the client device communicatively coupled to the server.