

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 master key, transmission data, and a counter value,

wherein the contactless card is configured to:

generate, upon entry into a communication field of a client device, a first diversified key using the first master key, the counter value, and at least one first cryptographic algorithm,

generate a second master key based on the first master key,

~~encrypt the second master key using at least one second cryptographic algorithm,~~

~~generate a cryptographic result including~~encrypt the counter value using at least one ~~third-second~~ cryptographic algorithm and the first ~~diversified-master~~ key, to yield a cryptographic result,

encrypt the transmission data using at least one ~~fourth-third~~ cryptographic algorithm and the first diversified key to yield encrypted transmission data, and

transmit the cryptographic result and the encrypted transmission data, via the client device, to a server,

wherein the first master key is a first secret key, and

wherein the second master key is a first public key.

[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 secret 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 using a-the first secret key, a counter value, and at least one first cryptographic algorithm;

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

~~encrypting the first public key using at least one second cryptographic algorithm;~~

encrypting a-the counter value using at least one ~~third-second~~ cryptographic algorithm and the first secret key;

encrypting the transmission data using at least one ~~fourth-third~~ cryptographic algorithm and the first diversified key; and

transmitting the encrypted counter value and the encrypted transmission data, via the client device to a server.

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

a processor; and

a memory, the memory containing ~~an encrypted~~ first master key,

wherein the server is configured to:

receive, from a contactless card, encrypted transmission data and a cryptographic result including a counter value, the encrypted transmission data and the cryptographic results being retrieved via a read of the contactless card by a client device communicatively coupled to the server,

decrypt the cryptographic result using the~~encrypted~~ first master key ~~using one of a first public key or a first secret key to validate the counter value,~~

generate a first diversified key based on the first master key and the counter value,

decrypt the encrypted transmission data ~~and the cryptographic result~~ using at least one first cryptographic algorithm and the first diversified key, and

validate the ~~counter value, and~~transmission data.

~~wherein the first master key is a second public key.~~

[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 master key, transmission data, and a counter value,

wherein the contactless card is configured to:

generate, upon entry into a communication field of a client device, a first diversified key using the first master key, the counter value, and at least one first cryptographic algorithm,

generate a second master key based on the first master key,

~~encrypt the second master key using at least one second cryptographic algorithm,~~

~~generate a cryptographic result including~~encrypt the counter value using at least one ~~third~~second cryptographic algorithm and the first ~~diversified~~master key, to yield a cryptographic result,

encrypt the transmission data using at least one ~~fourth~~third cryptographic algorithm and the first diversified key to yield encrypted transmission data, and

transmit the cryptographic result and the encrypted transmission data, via the client device, to a server,

wherein the first master key is a first secret key, and

wherein the second master key is a first public key.

~~2. The contactless card of claim 1, wherein the contactless card is further configured to sign the counter value using the first secret key.~~

~~32~~. The contactless card of claim ~~21~~, wherein the contactless card is further configured to encrypt the signed counter value using ~~a further~~the first public key.

~~43~~. The contactless card of claim 1, wherein the at least one first, second, and third~~, and fourth~~ cryptographic algorithms each include 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.

~~54~~. The contactless card of claim 1, wherein the ~~counter value~~cryptographic result includes a one-time passcode.

~~65~~. The contactless card of claim 1, wherein the first diversified key is generated for each transmission between the contactless card and the server.

~~76~~. The contactless card of claim ~~51~~, wherein the first diversified key is generated using at least one of the counter value or a portion of the counter value.

~~87~~. The contactless card of claim 1, wherein the contactless card is further configured to send the ~~encrypted~~ second master key to the server.

~~98~~. The contactless card of claim 1, wherein the first public key includes a signed certificate to authenticate an issuer of the first public key.

~~109.~~ 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 secret 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 using a-the first secret key, a counter value, and at least one first cryptographic algorithm;

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

~~encrypting the first public key using at least one second cryptographic algorithm;~~

encrypting a-the counter value using at least one ~~third-second~~ cryptographic algorithm and the first secret key;

encrypting the transmission data using at least one ~~fourth-third~~ cryptographic algorithm and the first diversified key; and

transmitting the encrypted counter value and the encrypted transmission data, via the client device, to a server.

12. The method of claim 11, further comprising transmitting the first public key to the server.

~~13. The method of claim 11, further comprising:~~

~~signing the counter value using the first secret key; and~~

~~encrypting the signed counter value using a public key.~~

~~1413.~~ The method of claim 11, wherein the first diversified key is generated using at least one of the counter value or a portion of the counter value.

~~1514.~~ A server, comprising:

a processor; and

a memory, the memory containing ~~an encrypted~~ first master key,

wherein the server is configured to:

receive, from a contactless card, encrypted transmission data and a cryptographic result including a counter value, ~~the encrypted transmission data and the cryptographic results being retrieved via a read of the contactless card by a client device communicatively coupled to the server,~~

decrypt the ~~cryptographic result using the encrypted~~ first master key ~~to validate the counter value using one of a first public key or a first secret key,~~

generate a first diversified key based on the first master key and the counter value,

decrypt the encrypted transmission data ~~and the cryptographic result~~ using at least one first cryptographic algorithm and the first diversified key, and

validate the ~~counter value~~ transmission data, ~~and wherein the first master key is a second public key.~~

~~1615.~~ The server of claim ~~1514~~, wherein the first diversified key is generated for each receipt of the cryptographic result and encrypted transmission data from the contactless card.

~~17~~16. The server of claim ~~16~~15, wherein the first diversified key is generated using at least one of the counter value or a portion of the counter value.

~~18~~17. The server of claim ~~15~~14, wherein:

the counter value is signed by a second secret key and encrypted by a ~~further~~ public key, and

the server is further configured to decrypt the signed counter value using ~~a further~~ the public key and verify the counter value using the second secret key.

~~19~~18. The server of claim ~~15~~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.

~~20~~19. The server of claim ~~15~~14, wherein the server is further configured to receive ~~the an~~ encrypted first master key from the contactless card.

20. The server of claim 17, wherein the second secret key is retrieved by the server via a read of the contactless card by a client device communicatively coupled to the server.