CLAIMS

1. A method for dual factor authentication of a request for access to an account associated with a client includes the steps of:

receiving an input PIN from at a user interface;

engaging a contactless card, the contactless card storing a PIN associated with the client;

forwarding the input PIN to the contactless card;

receiving, in response to a match of the input PIN with the stored PIN, a cryptogram from the contactless card, the cryptogram formed using a dynamic key of the contactless card, the dynamic key formed using a counter value maintained by the contactless card, wherein the cryptogram comprises contactless card data that is encoded using the dynamic key;

forwarding the cryptogram to an authenticating device; and

authorizing the request in response to authentication of the cryptogram by the authenticating device.

2. The method of claim 1 wherein the authenticating device maintains a copy of the contactless card data and a copy of the counter value, and authenticates the cryptogram by: encoding the copy of the contactless card data using an expected dynamic key formed from the copy of the counter to generate an expected cryptogram; and comparing the expected cryptogram to the forwarded cryptogram.

3. The method of claim 2 wherein the counter value and the copy of the counter value are each updated according to a predetermined protocol followed by the authenticating device and the contactless card.

4. The method of claim 3 wherein the dynamic key is further formed using a master key that is stored on the contactless card, and wherein the authenticating device stores a copy of the master key and uses the master key copy together with the counter to provide the expected dynamic key.

5. The method of claim 4 wherein the contactless card and the authenticating device each use the same cryptographic hash algorithm to generate the dynamic key and expected dynamic key.

6. The method of claim 5 wherein the contactless card data that is encoded using the dynamic key to form the cryptogram includes the PIN stored on the contactless card, a shared secret, the counter value, or a combination thereof

7. The method of claim 1 including the step of encoding the contactless card data includes applying a cryptographic hash function to the contactless card data.

8. The method of claim 7 wherein the cryptographic hash function is selected from a group of functions including a 3DES (Triple Data Encryption Algorithm), Advanced Encryption Standard (AES) 128, a symmetric Hash-Based Message Authentication

(HMAC) algorithm, and a symmetric cypher-based message authentication code (CMAC) algorithm such as AES-CMAC.

9. The method of claim 1, wherein the authenticating device comprises a client device, a merchant device, an authentication server or a combination thereof.

10. A method for dual factor authentication of a request for access to an account associated with a client includes the steps of:

receiving an input PIN from at a user interface;

engaging a contactless card, the contactless card storing a PIN associated with the client;

receiving a cryptogram from the contactless card, the cryptogram formed using a dynamic key of the contactless card, the dynamic key formed using a counter maintained by the contactless card, wherein the cryptogram comprises contactless card data including the PIN and is encoded using the dynamic key;

forwarding the input PIN and the cryptogram to an authenticating device, the request including a cryptogram; and

authorizing the request in response to authentication of the input PIN and cryptogram by the authenticating device.

11. The method of claim 10 wherein the authenticating device maintains a copy of the contactless card data and a copy of the counter, and authenticates the cryptogram by:

encoding the copy of the contactless card data and the input PIN using an expected dynamic key formed from the copy of the counter to generate an expected cryptogram; and

~~comparing the expected cryptogram to the forwarded cryptogram.~~

~~12. The method of claim 11 wherein the counter value and the copy of the counter value are each updated according to a predetermined protocol followed by the authenticating device and the contactless card.~~

~~13. The method of claim 12 wherein the dynamic key is further formed using a master key that is stored on the contactless card, and wherein the authenticating device stores a copy of the master key and uses the master key copy together with the counter to provide the expected dynamic key.~~

~~14. The method of claim 13 wherein the contactless card and the authenticating device each use the same cryptographic hash algorithm to generate the dynamic key and expected dynamic key.~~

~~15. The method of claim 14 wherein the contactless card data that is encoded using the dynamic key to form the cryptogram includes the PIN stored on the contactless card, a shared secret, the counter value, or a combination thereof~~

~~16. The method of claim 11 including the step of encoding the contactless card data includes applying a cryptographic hash function to the contactless card data.~~

~~17. The method of claim 16 wherein the cryptographic hash function is selected from a group of functions including a 3DES (Triple Data Encryption Algorithm), Advanced~~

Encryption Standard (AES) 128, a symmetric Hash-Based Message Authentication (HMAC) algorithm, and a symmetric cypher-based message authentication code (CMAC) algorithm such as AES-CMAC.

18. The method of claim 11, wherein the authenticating device comprises a client device, a merchant device, an authentication server or a combination thereof.

19. A device comprising:

a contactless card interface configured to communicate with a contactless card associated with a client, the contactless card comprising a stored PIN; a user interface;

a processor;

a non-volatile memory having program code stored thereon for authenticating a request by the client, the program code operable when executed upon by the processor to: forward an input PIN received by the user interface to the contactless card;

receive, in response to a match of the input PIN with the stored PIN, a cryptogram from the contactless card, the cryptogram formed using a dynamic key of the contactless card, the dynamic key formed using a counter value maintained by the contactless card, wherein the cryptogram comprises contactless card data that is encoded using the dynamic key;

forward the cryptogram to an authenticating device; and

authorize the request in response to authentication of the cryptogram by the authenticating device.

~~20. The device of claim 19 wherein the authenticating device maintains a copy of the contactless card data and a copy of the counter value, and authenticates the cryptogram by: encoding the copy of the contactless card data using an expected dynamic key formed from the copy of the counter to generate an expected cryptogram; and comparing the expected cryptogram to the forwarded cryptogram, wherein the counter value and the copy of the counter value are each updated according to a predetermined protocol followed by the authenticating device and the contactless card.~~

1. A method for dual factor authentication of a request for access to an account associated with a client includes the steps of:

receiving an input personal identification number (PIN) from a user interface;

engaging a contactless card, the contactless card storing a PIN associated with the client;

communicating the input PIN to the contactless card;

receiving, in response to a match of the input PIN with the stored PIN, a cryptogram from the contactless card, the cryptogram formed using a key of the contactless card, the key formed using a counter value maintained by the contactless card, wherein the cryptogram comprises contactless card data;

communicating the cryptogram to an authenticating device; and

authorizing the request in response to authentication of the cryptogram by the authenticating device.

2. The method of claim 1 wherein the authenticating device maintains a copy of the contactless card data and a copy of the counter value, and authenticates the cryptogram by:

decoding the contactless card data using an expected key formed from the copy of the counter to generate decoded contactless card data; and comparing the decoded contactless card data to the copy of the contactless card data.

3. The method of claim 2 wherein the counter value and the copy of the counter value are each updated according to a predetermined protocol followed by the authenticating device and the contactless card.

4. The method of claim 3 wherein the key is further formed using a master key that is stored on the contactless card, and wherein the authenticating device stores a copy of the master key and uses the master key copy together with the counter to provide the expected dynamic key.

5. The method of claim 4 wherein the contactless card and the authenticating device each use the same cryptographic hash algorithm to generate the key and expected key.

6. The method of claim 5 wherein the contactless card data that is encoded using the key to form the cryptogram includes the PIN, a shared secret, the counter value, or a combination thereof.

7. The method of claim 1 including the step of encoding the contactless card data includes applying a cryptographic hash function to the contactless card data.

8. The method of claim 7 wherein the cryptographic hash function is selected from a group of functions including a 3DES (Triple Data Encryption Algorithm), Advanced Encryption Standard (AES) 128, a symmetric Hash-Based Message Authentication (HMAC) algorithm, and a symmetric cypher-based message authentication code (CMAC) algorithm such as AES-CMAC.

9. The method of claim 1, wherein the authenticating device comprises a client device, a merchant device, an authentication server or a combination thereof.

10. A method for dual factor authentication of a request for access to an account associated with a client includes the steps of:

receiving an input personal identification number (PIN) from a user interface;

engaging a contactless card, the contactless card storing a PIN associated with the client;

receiving a cryptogram from the contactless card, the cryptogram formed using a dynamic key of the contactless card, the dynamic key formed using a counter maintained by the contactless card, wherein the cryptogram comprises contactless card data and is encoded using the dynamic key;

communicating the input PIN and the cryptogram to an authenticating device, the request including a cryptogram; and

authorizing the request in response to authentication of the input PIN and cryptogram by the authenticating device.

11. The method of claim 10 wherein the authenticating device maintains a copy of the contactless card data and a copy of the counter, and authenticates the cryptogram by:

encoding the copy of the contactless card data and the input PIN using an expected dynamic key formed from the copy of the counter to generate an expected cryptogram; and

comparing the expected cryptogram to the forwarded cryptogram.

12. The method of claim 11 wherein the counter value and the copy of the counter value are each updated according to a predetermined protocol followed by the authenticating device and the contactless card.

13. The method of claim 12 wherein the dynamic key is further formed using a master key that is stored on the contactless card, and wherein the authenticating device stores a copy of the master key and uses the master key copy together with the counter to provide the expected dynamic key.

14. The method of claim 13 wherein the contactless card and the authenticating device each use the same cryptographic hash algorithm to generate the dynamic key and expected dynamic key.

15. The method of claim 14 wherein the contactless card data that is encoded using the dynamic key to form the cryptogram includes the PIN stored on the contactless card, a shared secret, the counter value, or a combination thereof.

16. The method of claim 11 including the step of encoding the contactless card data includes applying a cryptographic hash function to the contactless card data.

17. The method of claim 16 wherein the cryptographic hash function is selected from a group of functions including a 3DES (Triple Data Encryption Algorithm), Advanced Encryption Standard (AES) 128, a symmetric Hash-Based Message Authentication (HMAC) algorithm, and a symmetric cypher-based message authentication code (CMAC) algorithm such as AES-CMAC.

18. The method of claim 11, wherein the authenticating device comprises a client device, a merchant device, an authentication server or a combination thereof.

19. A device comprising:

a contactless card interface configured to communicate with a contactless card associated with a client, the contactless card comprising a stored personal identification number (PIN);

a user interface;

a processor;

a non-volatile memory having program code stored thereon for authenticating a request by the client, the program code operable when executed upon by the processor to:

communicate an input PIN received by the user interface to the contactless card;

receive, in response to a match of the input PIN with the stored PIN, a cryptogram from the contactless card, the cryptogram formed using a dynamic key of the contactless card, the dynamic key formed using a counter value maintained by the contactless card, wherein the cryptogram comprises contactless card data that is encoded using the dynamic key;

communicate the cryptogram to an authenticating device; and

authorize the request in response to authentication of the cryptogram by the authenticating device.

20. The device of claim 19 wherein the authenticating device maintains a copy of the contactless card data and a copy of the counter value, and authenticates the cryptogram by:

decoding the contactless card data using an expected key formed from the copy of the counter to generate decoded contactless card data; and

comparing the decoded contactless card data to the copy of the contactless card data.