SUMMARY

[005a] According to one aspect, there is disclosed a transaction card readable by an application executing on a user device associated with a user of the transaction card, the transaction card comprising a memory device storing a counter value and a private key, one or more microprocessors having access to the counter value and the private key, and a near field communication transmitter configured to transmit to the application in response to a wireless read signal received from the user device. Responsive to the wireless read signal, the one or more microprocessors are configured to increment the counter value, generate an encrypted value based on the incremented counter value and the private key, and provide the encrypted value to the near field communication transmitter for transmission to the application executing on the user device, the encrypted value being communicated, via the application, to a service provider device as part of an authentication request generated by the application.

[005b] According to another aspect, there is disclosed a computer-implemented method for authenticating a user with a transaction card. The method comprises generating, by an application executing on a user device associated with the user an authentication request; transmitting, by the application to a server via a network, the authentication request; incrementing by the transaction card in response to a wireless read signal from the user device, a counter value stored on the transaction card, the transaction card being associated with the user; generating, by the transaction card, an encrypted value from the incremented counter value using a private key stored on the transaction card; transmitting, by the transaction card, the encrypted value to the application; transmitting, by the application, the encrypted value to the server as part of the authentication request generated by the application and transmitted by the application to the server; receiving, by the server, via the network, the for authentication request and the encrypted value transmitted, as part of the authentication request, from the application executing on the user device; generating, by the server a generated counter value in response to the authentication request; generating, by the server, a generated encrypted value based on the generated counter value and a private key associated with the transaction card; and authenticating, by the server the user based on a comparison of the generated encrypted value and the encrypted value received as part of the authentication request.

[005c] According to another aspect, there is provided a computing system for authenticating a user with a transaction card. The computing system comprises a service provider (SP) device comprising a processor and a memory, the SP device being in network communication with an application executing on a user device associated with a user, wherein the application is configured to transmit an authentication request to the SP device; a transaction card comprising a processor, a memory storing a counter value and a private key, and a near field communication (NFC) transmitter, wherein the transaction card is associated with the user. The processor of the transaction card,

responsive to a wireless read signal from the mobile device, is configured to increment the counter value, generate an encrypted value based on the incremented counter and the private key, and transmit the encrypted value, via the NFC transmitter, to the application executing on the mobile device, the application being configured to transmit the encrypted value to the SP device as part of the authentication request. The processor of the SP device, responsive to receiving the authentication request from the application, is configured to receive, from the application, a received encrypted value generated by the transaction card, generate a generated counter value, generate a generated encrypted value based on the generated counter value and a private key associated with the transaction card, and compare the generated encrypted value and the received encrypted value to authenticate the user.

[006] Consistent with disclosed embodiments, a transaction card associated with a financial account and for generating an encrypted value as part of an authentication request is provided. The transaction card comprises a radio frequency transmitter; a clock generator coupled to the radio frequency transmitter, the clock generator being configured to increment a counter value responsive to a wireless read signal received from an external radio frequency reader device; and a near field communication tag coupled to the radio frequency transmitter and storing a permanent identifier and the counter value. The near field communication tag may be configured, in response to the received read signal, to: generate an encrypted value based on the permanent identifier and the counter value; and provide the encrypted value to the radio frequency transmitter for transmission to the external radio frequency reader device.

[007] Consistent with another disclosed embodiment, a transaction card associated with a financial account and for generating an encrypted value as part of an authentication request is provided. The transaction card comprises a radio frequency transmitter; a near field communication tag coupled to the radio frequency transmitter; and a clock coupled to the near field communication tag and powered by a power source. The clock may be configured to send a time value to the near field communication tag responsive to a wireless read signal received by the near field communication tag from an external radio frequency reader device. The near field communication tag may be configured to: store a permanent identifier and the time value; and, in response to the received read signal, to: generate an encrypted value based on the permanent identifier and the time value; and provide the encrypted value to the radio frequency transmitter for transmission to the external radio frequency reader device.

[008] Consistent with another disclosed embodiment, a transaction card associated with a financial account and for generating an encrypted value as part of an authentication request is provided. The transaction card comprises: a radio frequency transmitter; a near field communication tag coupled to the radio frequency transmitter; and a microprocessor coupled to the near field communication tag and powered by a power source. The microprocessor may be configured to calculate an update value responsive to a wireless read signal received from an external radio

frequency reader device. The near field communication tag may be configured to: store a permanent identifier and the update value, and in response to the received read signal: generate an encrypted value based on the permanent identifier and the update value, and provide the encrypted value to the radio frequency transmitter for transmission to the external radio frequency reader device.

[009] Consistent with other disclosed embodiments, tangible computer-readable storage media may store program instructions that are executable by one or more processors to implement any of the processes disclosed herein.

[010] It is to be understood that both the foregoing general description and the following detailed description are exemplary and explanatory only, and are not restrictive of the disclosed embodiments.

WHAT IS CLAIMED IS:

1. A transaction card readable by an application executing on a user device associated with a user of the transaction card, the transaction card comprising:

a memory device storing a counter value and a private key;

one or more microprocessors having access to the counter value and the private key; and

a near field communication transmitter configured to transmit to the application in response to a wireless read signal received from the user device,

wherein, responsive to the wireless read signal, the one or more microprocessors are configured to:

increment the counter value,

generate an encrypted value based on the incremented counter value and the private key, and

provide the encrypted value to the near field communication transmitter for transmission to the application executing on the user device, the encrypted value being communicated, via the application, to a service provider device as part of an authentication request generated by the application.

2. The transaction card of claim 1, wherein the one or more microprocessors are further configured to increment the counter value by a predetermined amount.

3. The transaction card of claim 2, wherein the predetermined amount is unique to the transaction card.

4. The transaction card of claim 1, wherein the one or more microprocessors are further configured to increment the counter value by a different amount each time.

5. The transaction card of claim 1, wherein the encrypted value comprises a hash of the private key and the incremented counter value.

6. The transaction card of claim 1, wherein a value by which the counter is incremented is calculated by an algorithm.

7. The transaction card of claim 1, wherein the one or more microprocessors are further configured to, in response to the wireless read signal received from the user device, reset the counter value to an initial counter value or a value different than the initial counter value.

8. The transaction card of claim 1, wherein the one or more microprocessors are included within an EMV chip.

9. The transaction card of claim 1, wherein the transaction card comprises at least one selected from the group of a credit card, a debit card, a gift card, a rewards card, a frequent flyer card, a merchant-specific card, a discount card, a passport card, a driver's license, and an entry point access card.

10. A computer-implemented method for authenticating a user with a transaction card, the method comprising:

generating, by an application executing on a user device associated with the user an authentication request;

transmitting, by the application to a server via a network, the authentication request;

incrementing by the transaction card in response to a wireless read signal from the user device, a counter value stored on the transaction card, the transaction card being associated with the user;

generating, by the transaction card, an encrypted value from the incremented counter value using a private key stored on the transaction card;

transmitting, by the transaction card, the encrypted value to the application;

transmitting, by the application, the encrypted value to the server as part of the authentication request generated by the application and transmitted by the application to the server;

receiving, by the server, via the network, the authentication request and the encrypted value transmitted, as part of the authentication request, from the application executing on the user device;

generating, by the server, a generated counter value in response to the authentication request;

generating, by the server, a generated encrypted value based on the generated counter value and a private key associated with the transaction card; and

authenticating, by the server, the user based on a comparison of the generated encrypted value and the encrypted value received as part of the authentication request.

11. The computer-implemented method of claim 10, further comprising, in response to a signal received from the user device, resetting the generated counter value to an initial counter value.

12. The computer-implemented method of claim 10, further comprising, in response to a signal received from the user device, resetting the generated counter value to a value different than an initial counter value.

13. The computer-implemented method of claim 10, further comprising transmitting, to the user device, instructions configured to cause the user device to complete an action associated with the request for authentication.

14. The computer-implemented method of claim 10, wherein at least one selected from the group of the generated encrypted value and the received encrypted value is valid for a predetermined amount of time.

15. The computer-implemented method of claim 10, further comprising:

determining, by the server, that the encrypted value, received from the transaction card via the user device, and the generated encrypted value are not equal;

generating, by the server, a fraud alert message; and

transmitting, by the server, the fraud alert message to the user device.

16. The computer-implemented method of claim 10, wherein authenticating the user allows for at least one selected from the group of a completion of a transaction, a log-in or authentication with a website or device, a cash withdrawal, a wire transfer, a PIN reset, and a call center transaction.

17. The computer-implemented method of claim 16, wherein:

the request for authentication comprises identifying information, and

the identifying information comprises at least one selected from the group of a user identification and an account number.

18. A computing system for authenticating a user with a transaction card, the computing system comprising:

a service provider (SP) device comprising a processor and a memory, the SP device being in network communication with an application executing on a user device associated with a user, wherein the application is configured to transmit an authentication request to the SP device;

a transaction card comprising a processor, a memory storing a counter value and a private key, and a near field communication (NFC) transmitter, wherein the transaction card is associated with the user;

wherein the processor of the transaction card, responsive to a wireless read signal from the mobile device, is configured to:

increment the counter value,

generate an encrypted value based on the incremented counter and the private key, and

transmit the encrypted value, via the NFC transmitter, to the application executing on the mobile device, the application being configured to transmit the encrypted value to the SP device as part of the authentication request;

wherein the processor of the SP device, responsive to receiving the authentication request from the application, is configured to:

receive, the application, a received encrypted value generated by the transaction card,

generate a generated counter value,

generate a generated encrypted value based on the generated counter value and a private key associated with the transaction card, and

compare the generated encrypted value and the received encrypted value to authenticate the user.

19. The computing system of claim 18, wherein the processor of the SP device is further configured to, in response to a signal received from the user device, reset the counter value to an initial counter value or a value different than the initial counter value.

20. The computing system of claim 18, wherein authenticating the user allows for at least one selected from the group of a completion of a transaction, a log-in or authentication with a website or device, a cash withdrawal, a wire transfer, a PIN reset, and a call center transaction.