losses due to breaches of data security. In addition to monetary costs, data security breaches erode user confidence in a business, and a large or otherwise notable breach often attracts significant public attention.

[0005] Accordingly, there are significant, and competing, needs to safeguard sensitive data while ensuring ready access by authorized users.

SUMMARY

[0006] Therefore, it is an object of this disclosure to describe a smart card that enhances the security of data while promoting accessibility. Various embodiments provide a smart card and systems and methods incorporating a smart card, proximate communication devices, and remote servers.

[0006a] In accordance with one aspect, there is provided a system, comprising a server storing a server counter, a smart card comprising a microprocessor, a contactless communication interface, and a memory, wherein the memory stores an applet, a card counter, and a customer identifier; and a client application comprising instruction for execution on a communication device having a communication field, wherein, upon entry of the contactless communication interface into the communication field of the communication device, the microprocessor is configured to: increment the card counter to yield an incremented card counter, transmit the incremented card counter via the contactless communication interface for synchronization with a counter value stored on the communication device, synchronize the incremented card with a counter value stored on the communication device, generate, upon synchronizing the incremented card counter with the counter value stored on the communication device, a unique one-time uniform resource locator (URL) using the incremented and synchronized card counter and the customer identifier, and transmit the unique one-time URL via the contactless communication interface to the client application executing on the communication device, wherein, upon receiving the unique one-time URL from the

microprocessor, the client application is configured to: synchronize the counter value stored on the communication device with the server counter, and transmit the unique one-time URL to the server for authentication, wherein, upon receiving the unique one-time URL from the client application, the server is configured to: authenticate the unique one-time URL using the server counter and the customer identifier, and transmit one or more data records requested by the unique one-time URL to the client application.

[0006b] In accordance with another aspect, there is provided a method for using a smart card comprising a microprocessor, a contactless communication interface, and a memory, wherein the memory stores an applet, a card counter, and a customer identifier, the method comprising the steps of: incrementing the card counter after entering of the contactless communication interface into a communication field generated by a communication device the communication device comprising a microprocessor and a memory storing an application comprising instructions for execution by the microprocessor of the communication device; transmitting the incremented card counter for synchronization via the contactless communication interface to the application; synchronizing the incremented card counter with a counter value stored on the communication device; generating a unique one-time uniform resource locator (URL) using the incremented and synchronized card counter and the customer identifier; and transmitting the unique one-time URL via the contactless communication interface to the application.

[0006c] In accordance with another aspect, there is provided a smart card, comprising a microprocessor; a memory, the memory storing an applet, a card counter, and a customer identifier; and a contactless communication interface, wherein the microprocessor is configured to: increment the card counter in response to the contactless communication interface entering a communication field of a communication device, transmit the incremented

card counter for synchronization to the communication device via the contactless communication interface, synchronize the incremented card counter with a counter value stored on the communication device, generate a unique one-time uniform resource locator (URL) using the incremented and synchronized card counter and the customer identifier, and transmit the unique one-time URL via the contactless communication interface.

[0007] Embodiments of the present disclosure provide a smart card comprising a substrate; a memory embedded in the substrate, wherein the memory contains an applet, a counter, and a unique customer identifier, a contactless communication interface embedded in the substrate; and a microprocessor embedded in the substrate, wherein the microprocessor is in data communication with the memory and the contactless communication interface, wherein, upon entry of the contactless communication interface into a communication field of a communication device, the microprocessor increments the counter and synchronizes the value of the counter with a second counter stored in the communication device, and wherein the applet generates a unique uniform resource locator (URL) based on the incremented value of the counter and the unique customer identifier, and wherein the unique URL is transmitted to the communication device via the contactless communication interface.

[0008] Embodiments of the present disclosure provide a system for the secure access of information, comprising a server containing financial information; a smart card including

CLAIMS

1. A system, comprising:

a server storing a server counter;

a smart card comprising a microprocessor, a contactless communication interface, and a memory, wherein the memory stores an applet, a card counter, and a customer identifier; and

a client application comprising instruction for execution on a communication device having a communication field,

wherein, upon entry of the contactless communication interface into the communication field of the communication device, the microprocessor is configured to:

increment the card counter to yield an incremented card counter,

transmit the incremented card counter via the contactless communication interface for synchronization with a counter value stored on the communication device,

synchronize the incremented card with a counter value stored on the communication device,

generate, upon synchronizing the incremented card counter with the counter value stored on the communication device, a unique one-time uniform resource locator (URL) using the incremented and synchronized card counter and the customer identifier, and

transmit the unique one-time URL via the contactless communication interface to the client application executing on the communication device,

wherein, upon receiving the unique one-time URL from the microprocessor, the client

application is configured to:

synchronize the counter value stored on the communication device with the server counter, and

transmit the unique one-time URL to the server for authentication,

wherein, upon receiving the unique one-time URL from the client application, the server is configured to:

authenticate the unique one-time URL using the server counter and the customer identifier, and

transmit one or more data records requested by the unique one-time URL to the client application.

2. The system of claim 1, wherein, after receipt of the incremented card counter, the server is configured to synchronize the incremented card counter and the server counter.

3. The system of claim 1, wherein:

the unique one-time URL is configured to request at least one selected from the group of an account balance, a credit score, and a product availability, and

upon determining that the unique one-time URL is configured to request an account balance or a credit score, the server is configured to request additional authentication information.

4. The system of claim 1, wherein the microprocessor is configured to generate the unique one-time URL by cryptographically hashing the incremented card counter and the customer identifier.

5. The system of claim 4, wherein:

the unique one-time URL is generated by the applet stored on the smart card, and

the client application is configured to receive the unique one-time URL from the smart card and transmit the unique one-time URL to the server.

6. The system of claim 1, wherein the client application is configured to append device identification information to the unique one-time URL prior to transmitting the unique one-time URL to the server.

7. The system of claim 1, wherein the client application is configured to append location information to the unique one-time URL prior to transmitting the unique one-time URL to the server.

8. The system of claim 1, wherein the client application is configured to append user identification information to the unique one-time URL prior to transmitting the unique one-time URL to the server.

9. The system of claim 1, wherein the server is configured to:

recreate the cryptographic hash using an expected value of the server counter,

compare the recreated cryptographic hash to the received unique one-time URL, and

upon a successful match of the recreated cryptographic hash to the received unique one-time URL, transmit the one or more requested data records to the client application.

10. The system of claim 9, wherein prior to transmitting financial information to the application, the server is configured to request entry of authentication information via the client application.

11. A method for using a smart card comprising a microprocessor, a contactless communication interface, and a memory, wherein the memory stores an applet, a card counter, and a customer identifier, the method comprising the steps of:

incrementing the card counter after entering of the contactless communication interface into a communication field generated by a communication device, the communication device comprising a microprocessor and a memory storing an application comprising instructions for execution by the microprocessor of the communication device;

transmitting the incremented card counter for synchronization via the contactless communication interface to the application;

synchronizing the incremented card counter with a counter value stored on the communication device;

generating a unique one-time uniform resource locator (URL) using the incremented and synchronized card counter and the customer identifier; and

transmitting the unique one-time URL via the contactless communication interface to the application.

12. The method of claim 11, wherein generating a unique one-time URL using the incremented card counter and the customer identifier comprises cryptographically hashing the incremented card counter and the customer identifier.

13. The method of claim 11, further comprising:

transmitting, by the application, the incremented card counter to a server storing a server counter; and

synchronizing, by the server, the incremented card counter with the server counter.

14. The method of claim 13, further comprising:

recreating, by the server, the cryptographic hash using an expected server counter value and the customer identifier;

comparing, by the server, the recreated cryptographic hash to the unique one-time URL; and

transmitting, by the server, financial information to the application if the recreated cryptographic hash matches the unique one-time URL.

15. The method of claim 13, further comprising:

appending, by the application, location information to the unique one-time URL; and

transmitting, by the application, the unique one-time URL to the server.

16. The method of claim 15, further comprising receiving, by the application, location-specific data from the server in response to the appended location information.

17. The method of claim 13, further compromising appending, by the application, information identifying the communication device to the unique one-time URL before transmitting the unique one-time URL to the server.

18. A smart card, comprising:

a microprocessor;

a memory, the memory storing an applet, a card counter, and a customer identifier; and

a contactless communication interface,

wherein the microprocessor is configured to:

increment the card counter in response to the contactless communication interface entering a communication field of a communication device,

transmit the incremented card counter for synchronization to the communication device via the contactless communication interface,

synchronize the incremented card counter with a counter value stored on the communication device,

generate a unique one-time uniform resource locator (URL) using the incremented and synchronized card counter and the customer identifier, and

transmit the unique one-time URL via the contactless communication interface.

19. The smart card of claim 18, wherein the microprocessor is further configured to generate the unique one-time URL using the incremented card counter and the customer identifier by cryptographically hashing the incremented card counter and the customer identifier.

20. The smart card of claim 19, wherein the microprocessor is further configured to:

include the cryptographic hash in the unique one-time URL, and

append a tag comprising the customer identifier to the unique one-time URL.