

SYSTEMS AND METHODS FOR PROVIDING ONLINE AND HYBRIDCARD INTERACTIONS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to U.S. Patent Application Serial No. 16/503,285, entitled “SYSTEMS AND METHODS FOR PROVIDING ONLINE AND HYBRIDCARD INTERACTIONS” filed on July 3, 2019. The contents of the aforementioned patent application are incorporated herein by reference in their entirety.

STATEMENT OF INCORPORATION BY REFERENCE

[0002] The present application is related to U.S. Patent Application Serial No. 16/135,954 entitled “SYSTEMS AND METHODS FOR PROVIDING CARD INTERACTIONS” filed on September 19, 2018, the entirety of which is incorporated herein by reference.

TECHNICAL FIELD

[0003] Embodiments herein generally relate to computing platforms, and more specifically, to authenticating a user based on an authenticated communication between a contactless transaction card and a user device.

BACKGROUND

[0004] Activating many cards, and more specifically financial cards (e.g., credit cards), involve the time-consuming process of cardholders calling a telephone number or visiting a website and entering or otherwise providing card information. Further, while the growing use of chip-based financial cards provides more secure features over the previous technology (e.g., magnetic strip cards) for in-person purchases, account access still typically relies 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.

[0005] Accordingly, there is a need for both an improved method of activating a card and an improved authentication for account access.

SUMMARY

[0005a] According to a first aspect of the present disclosure, there is provided a method comprising:

receiving, by an application executing on a processor, an application transaction counter (ATC), a digital signature, and a public key from a contactless card;

verifying, by the application, the digital signature based on the public key;

receiving, by the application, a request comprising a non-payment event;

transmitting, by the application, a message comprising the request and a cryptogram to an authentication server, wherein the cryptogram is based at least in part on the ATC and a symmetric key associated with the card, wherein the message conforms to a payment

format of a payment protocol and comprises an indication to request authorization of the non-payment event using the payment protocol;

receiving, by the application, a response from the authentication server verifying the cryptogram, wherein the response is based on the payment protocol, wherein the response reflects the performance of the non-payment event, wherein the response conforms to the payment format, wherein the server authorizes the non-payment event using the payment protocol based at least in part on the indication to request authorization of the non-payment event using the payment protocol; and

updating, by the application, the ATC of the contactless card based on the verification of the cryptogram based on the payment protocol, wherein the ATC is updated by incrementing the ATC by a predefined value associated with the card; and

synchronizing the updated ATC with the ATC of the authentication server based on the predefined value associated with the card.

[0005b] According to a second aspect of the present disclosure, there is provided a non-transitory computer-readable storage medium, the computer-readable storage medium including instructions that when executed by a processor, cause the processor to:

receive, by an application, an application transaction counter (ATC), a digital signature, and a public key from a contactless card;

verify, by the application, the digital signature based on the public key;

receive, by the application, a request comprising a non-payment event;

transmit, by the application, a message comprising the request and a cryptogram to an authentication server, wherein the cryptogram is based at least in part on the ATC and a symmetric key associated with the card, wherein the message conforms to a payment format of a payment protocol and comprises an indication to request authorization of the non-payment event using the payment protocol;

receive, by the application, a response from the authentication server verifying the cryptogram, wherein the response is based on the payment protocol, wherein the response reflects the performance of the non-payment event, wherein the response conforms to the payment format, wherein the server authorizes the non-payment event using the payment protocol based at least in part on the indication to request authorization of the non-payment event using the payment protocol; and

update, by the application, the ATC of the contactless card based on the verification of the cryptogram based on the payment protocol, wherein the ATC is updated by incrementing the ATC by a predefined value associated with the card; and

synchronize the updated ATC with the ATC of the authentication server based on the predefined value associated with the card.

[0005c] According to a third aspect of the present disclosure, there is provided a method, comprising:

receiving, by a server from an application executing on a client device, a message conforming to a payment format of a payment protocol, the message comprising: (i) a request to perform a non-payment event associated with a contactless card, (ii) an application transaction counter (ATC) generated by the contactless card, (iii) a digital signature generated by the contactless card, (iv) a cryptogram generated based on the ATC and a symmetric key associated with the card, and (v) an indication to request authorization of the non-payment event using the payment protocol;

verifying, by the server, the digital signature based on a public key associated with the card;

decrypting, by the server, the cryptogram based at least in part on the ATC and the symmetric key;

authorizing, by the server, the non-payment event using the payment protocol based at least in part on the indication to request authorization of the non-payment event using the payment protocol in the message;

transmitting, by the server to the application based on the verification of the digital signature and the decryption of the cryptogram, a response based on the payment protocol, wherein the response reflects the performance of the non-payment event, wherein the response conforms to the payment format; and

updating, by the server based on the verification of the cryptogram based on the payment protocol, an instance of the ATC stored by the server, wherein the ATC is updated by incrementing the ATC by a predefined value associated with the card; and

synchronizing the updated ATC with the ATC of generated by the contactless card based on the predefined value associated with the card.

[0006] Embodiments disclosed herein provide systems, methods, articles of manufacture, and computer-readable media for authenticating a user utilizing a payment protocol for purposes distinct from making a payment. According to one example, an application executing on a computer system may initiate a communication to verify an identity of a user or verify a card with a third-party device. The application executed on the system, as part of the communication, may utilize near field communication (NFC), with a card associated with the user. (In various embodiments, the application may be launched by tapping the contactless card on a user device, e.g. a mobile device). The communication may include receiving a plurality of inputs by the application, including an application transaction counter (ATC) and generating a cryptogram based

CLAIMS

What is claimed is:

1. ~~—A method comprising:~~
 - ~~initiating, by a mobile device, a wireless communication to verify a contactless card using near field communication (NFC);~~
 - ~~—receiving, at the mobile device and as part of the wireless communication, a plurality of inputs, including an application transaction counter (ATC);~~
 - ~~—generating, with the mobile device, a cryptogram based on the plurality of inputs of the wireless communication and a symmetric key associated with the card;~~
 - ~~—receiving, at the mobile device, a response from the authentication server verifying the identity of the contactless card based on the cryptogram;~~
 - ~~—wherein the generation of the cryptogram and the received response from the authentication server is based on a payment protocol, and wherein the wireless communication and the card verification is distinct from completing a payment in relation to the payment protocol.~~
2. ~~—The method of claim 1, wherein the card having a radio frequency identification (RFID) chip, the card being within an NFC range of a digital reader associated with a computer device wherein the cryptogram is an authorization request cryptogram (ARQC).~~
3. ~~—The method of claim 2, wherein the verification of the contactless card is determined from the received response from the authentication server.~~
4. ~~—The method of claim 2 further comprising:~~
 - ~~—storing an updated version of the ATC on a host device associated with the authentication server.~~
5. ~~—The method of claim 4, wherein the identity verification associated with the updated ATC is logged as a non-payment event.~~
6. ~~—The method of claim 5, wherein the initiation of the wireless communication is based on a first tap, and the method further comprising:~~
 - ~~—performing an antifraud measure for a payment event associated with the card by using the non-payment event associated with the updated ATC.~~
7. ~~—An apparatus, comprising:~~
 - ~~a memory to store instructions; and~~
 - ~~processing circuitry, coupled with the memory, operable to execute the instructions, that when executed, cause the processing circuitry to:~~
 - ~~—receive, by an application associated with a computing device and from a user, a first application user credential associated with a user profile;~~

~~—— compare, for a first match and by a processor associated with the application, the first application user credential with a stored second application user credential, the stored second application user credential being associated with a user identity; and~~
~~—— responsive to finding a first match, verify the user identity by performing at least one of i) a plurality of host-less verification operations and ii) a plurality of authentication server verification operations, the host-less verification operations include:~~

~~communicating, by the application and using near field communication (NFC), with a card;~~

~~receiving, by the application and from the card, a public key of a key pair of the card and cardholder identification information of an account holder of the card;~~

~~instructing, by the application, generation of a digital signature by the card using a private key of the key pair of the card;~~

~~receiving the digital signature from the card;~~

~~verifying the digital signature using the public key; and~~

~~—— wherein the authentication server verification operations include:~~

~~providing, by the application and from the card, the computer device with a plurality of inputs, including an application transaction counter (ATC);~~

~~generating, by the application and from the card, a cryptogram based on the plurality of inputs and a symmetric key associated with the card;~~

~~—— transmitting, by the application, the cryptogram and the ATC to the authentication server; and~~

~~—— receiving a response from the authentication server verifying the identity of the contactless card based on the transmitted cryptogram, wherein the received response is based on recreating the cryptogram by the authentication server in response to receiving the cryptogram.~~

8. ~~The apparatus of claim 7, wherein the process circuitry is caused to perform only the plurality of authentication server verification operations if the plurality of authentication server verification operations can be performed, otherwise the process circuitry is caused to perform the plurality of host-less operations.~~

9. ~~The apparatus of claim 7, wherein the card having a radio frequency identification (RFID) chip, the card being within an NFC range of a digital reader associated with the computing device, and wherein the process circuitry is caused to determine if the plurality of authentication server verification operations can be performed.~~

10. ~~The apparatus of claim 9, wherein the processor circuitry is further caused to compare for a second match between at least a portion of the user identity with at least a portion of the~~

~~cardholder identification information and perform the host less operations only in response to finding a second match.~~

~~11.—The apparatus according to claim 10, wherein, if the plurality of authentication server verification operations cannot be performed as a result of a network failure associated with the authentication server, the process circuitry is further caused to: extract an updated ATC from the card after the plurality of host less operations have been performed, store the updated ATC on the computer device, and transmit the updated ATC to the authentication server when the network failure subsides.~~

~~12.—The apparatus of claim 10, wherein the process circuitry is caused to perform both the plurality of host less operations and the plurality of authentication server verification operations, wherein the application is associated with at least one payment feature and at least one non-payment feature, wherein all of the operations of the plurality of host less operations are based on a payment protocol, wherein all of the operations of the plurality of host less operations are performed to enable the at least one non-payment feature, and wherein the at least one non-payment feature is distinct from the payment feature.~~

~~13.—The apparatus of claim 12, wherein generation of the cryptogram and the received response from the authentication server is based on a payment protocol, and wherein all of the operations of the plurality of authentication server verification operations are performed to verify the user to enable the non-payment feature of the application.~~

~~14.—The apparatus of claim 13, wherein the cryptogram is an authorization request cryptogram (ARQC).~~

~~15.—The apparatus of claim 14, wherein the process circuitry is further caused to store an updated version of the ATC on the authentication server.~~

~~16.—The apparatus of claim 15, wherein the process circuitry is further caused to log, at the authentication server, the received response from the authentication server that is associated with the updated ATC as a non-payment event.~~

~~17.—A host system associated with an issuer of a card associated with a user, the host system including a non-transitory computer readable storage medium storing computer readable program code executable by a processor to:~~

~~———receive, at an authentication server, a communication data associated with a card verification communication initiated by i) an application associated with the card and ii) at least one computer device, the communication data including i) an application transaction counter (ATC) and ii) a cryptogram based on a plurality of inputs of the communication and a symmetric key associated with the card; and~~

~~transmit a response from the authentication server verifying the card based on the received cryptogram, wherein the transmitted response is based on recreating the cryptogram by the authentication server in response to receiving the communication data;~~

~~wherein the cryptogram and the transmitted response from the authentication server are based on a payment protocol, and wherein the card verification is distinct from completing a payment in relation to the payment protocol.~~

~~18. The host system of claim 17, wherein the cryptogram is an authorization request cryptogram (ARQC).~~

~~19. The host system of claim 18, wherein the card verification is determined from the transmitted response from the authentication server.~~

~~20. The host system of claim 19, further including computer readable program code executable by the processor to:~~

~~store an updated version of the ATC, wherein the card verification associated with the updated ATC is logged as a non-payment event; and~~

~~perform an antifraud measure for a payment event associated with the card by using the non-payment event associated with the updated ATC.~~

1. A method comprising:

receiving, by an application executing on a processor, an application transaction counter (ATC), a digital signature, and a public key from a contactless card;

verifying, by the application, the digital signature based on the public key;

receiving, by the application, a request comprising a non-payment event;

transmitting, by the application, a message comprising the request and a cryptogram to an authentication server, wherein the cryptogram is based at least in part on the ATC and a symmetric key associated with the card, wherein the message conforms to a payment format of a payment protocol and comprises an indication to request authorization of the non-payment event using the payment protocol;

receiving, by the application, a response from the authentication server verifying the cryptogram, wherein the response is based on the payment protocol, wherein the response reflects the performance of the non-payment event, wherein the response conforms to the payment format, wherein the server authorizes the non-payment event using the payment protocol based at least in part on the indication to request authorization of the non-payment event using the payment protocol; and

updating, by the application, the ATC of the contactless card based on the verification of the cryptogram based on the payment protocol, wherein the ATC is updated by incrementing the ATC by a predefined value associated with the card; and

synchronizing the updated ATC with the ATC of the authentication server based on the predefined value associated with the card.

2. The method of claim 1, wherein the non-payment event comprises one or more of: (i) activating the contactless card, (ii) modifying a personal identification number (PIN) of the contactless card, or (iii) modifying an address associated with the contactless card.

3. The method of claim 2, wherein the response from the authentication server reflects one or more of: (i) the activation of the contactless card, (ii) the modification of the PIN of the contactless card, or (iii) the modification of the address associated with the contactless card.

4. The method of claim 1, wherein the ATC, the digital signature, and the public key are received using near field communication (NFC).

5. The method of claim 1, wherein the cryptogram is generated by one of the contactless card or the application.

6. The method of claim 1, wherein the cryptogram is generated based on the payment protocol, wherein the cryptogram is an authorization request cryptogram (ARQC).

7. The method of claim 1, wherein the message includes a predefined transaction value to mimic the payment protocol to verify contactless card perform the non-payment event without completing a payment, wherein the payment protocol comprises the Europay, Mastercard, and Visa (EMV) protocol.

8. A non-transitory computer-readable storage medium, the computer-readable storage medium including instructions that when executed by a processor, cause the processor to: receive, by an application, an application transaction counter (ATC), a digital signature, and a public key from a contactless card;

verify, by the application, the digital signature based on the public key;

receive, by the application, a request comprising a non-payment event;

transmit, by the application, a message comprising the request and a cryptogram to an authentication server, wherein the cryptogram is based at least in part on the ATC and a symmetric key associated with the card, wherein the message conforms to a payment format

of a payment protocol and comprises an indication to request authorization of the non-payment event using the payment protocol;

receive, by the application, a response from the authentication server verifying the cryptogram, wherein the response is based on the payment protocol, wherein the response reflects the performance of the non-payment event, wherein the response conforms to the payment format, wherein the server authorizes the non-payment event using the payment protocol based at least in part on the indication to request authorization of the non-payment event using the payment protocol; and

update, by the application, the ATC of the contactless card based on the verification of the cryptogram based on the payment protocol, wherein the ATC is updated by incrementing the ATC by a predefined value associated with the card; and

synchronize the updated ATC with the ATC of the authentication server based on the predefined value associated with the card.

9. The computer-readable storage medium of claim 8, wherein the non-payment event comprises one or more of: (i) activating the contactless card, (ii) modifying a personal identification number (PIN) of the contactless card, or (iii) modifying an address associated with the contactless card.

10. The computer-readable storage medium of claim 9, wherein the response from the authentication server reflects one or more of: (i) the activation of the contactless card, (ii) the modification of the PIN of the contactless card, or (iii) the modification of the address associated with the contactless card.

11. The computer-readable storage medium of claim 8, wherein the ATC, the digital signature, and the public key are received using near field communication (NFC).

12. The computer-readable storage medium of claim 8, wherein the cryptogram is generated by one of the contactless card or the application.

13. The computer-readable storage medium of claim 8, wherein the cryptogram is generated based on the payment protocol, wherein the cryptogram is an authorization request cryptogram (ARQC).

14. The computer-readable storage medium of claim 8, wherein the message includes a predefined transaction value to mimic the payment protocol to verify contactless card perform the non-payment event without completing a payment, wherein the payment protocol comprises the Europay, Mastercard, and Visa (EMV) protocol.

15. A method, comprising:

receiving, by a server from an application executing on a client device, a message conforming to a payment format of a payment protocol, the message comprising: (i) a request to perform a non-payment event associated with a contactless card, (ii) an application transaction counter (ATC) generated by the contactless card, (iii) a digital signature generated by the contactless card, (iv) a cryptogram generated based on the ATC and a symmetric key associated with the card, and (v) an indication to request authorization of the non-payment event using the payment protocol;

verifying, by the server, the digital signature based on a public key associated with the card;

decrypting, by the server, the cryptogram based at least in part on the ATC and the symmetric key;

authorizing, by the server, the non-payment event using the payment protocol based at least in part on the indication to request authorization of the non-payment event using the payment protocol in the message;

transmitting, by the server to the application based on the verification of the digital signature and the decryption of the cryptogram, a response based on the payment protocol, wherein the response reflects the performance of the non-payment event, wherein the response conforms to the payment format; and

updating, by the server based on the verification of the cryptogram based on the payment protocol, an instance of the ATC stored by the server, wherein the ATC is updated by incrementing the ATC by a predefined value associated with the card; and

synchronizing the updated ATC with the ATC of generated by the contactless card based on the predefined value associated with the card.

16. The method of claim 15, wherein the non-payment event comprises one or more of: (i) activating the contactless card, (ii) modifying a personal identification number (PIN) of the contactless card, or (iii) modifying an address associated with the contactless card.

17. The method of claim 15, wherein the cryptogram is generated by one of the contactless card or the application.

18. The method of claim 15, wherein the cryptogram is generated based on the payment protocol, wherein the cryptogram is an authorization request cryptogram (ARQC).

19. The method of claim 15, wherein the payment protocol comprises the Europay, Mastercard, and Visa (EMV) protocol.

20. The method of claim 15, wherein the message further comprises an indication of a type of the application, wherein server determines, based on the type of the application, that the application does not include payment features or does not use the payment protocol to complete payments, wherein the server further authorizes the non-payment event using the payment protocol based on the determination that the application does not include the payment features or does not use the payment protocol to complete payments.