

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.