

CLAIMS

What is claimed is:

1. ~~—A contactless card, comprising:~~

~~—a processor circuit;~~

~~a communications interface; and~~

~~a memory storing instructions which when executed by the processor circuit, cause the processor circuit to:~~

~~receive, via the communications interface from a mobile device executing an account application, an indication that a server preauthorized a transaction based on location data describing a location of the mobile device and verification of encrypted data, the encrypted data generated by the contactless card using a cryptographic algorithm and a private key stored in the memory of the contactless card, the indication further specifying that one or more credentials for an account associated with the contactless card have received by the account application;~~

~~receive, via the communications interface from a point of sale (POS) device, an indication to pay for the transaction using the contactless card;~~

~~determine, based on one or more rules stored in the memory, that the location of the mobile device is within a threshold distance of one or more locations the contactless card is permitted for use;~~

~~generate transaction data comprising: (i) indications of an account number and an expiration date of the contactless card, and (ii) the indication of the preauthorization of the transaction by the server;~~

~~transmit the transaction data to the POS device as payment for the transaction;~~
~~and~~

~~receive, from the POS device, an indication that the server authorized payment for the transaction using at least a portion of the transaction data and based at least in part on identifying the indication of the preauthorization of the transaction by the server in the transaction data.~~

2. ~~The contactless card of claim 1, the memory storing instructions which when executed by the processor circuit cause the processor circuit to:~~

~~write the indication of the preauthorization of the transaction by the server to a first field of an EMV payload; and~~

~~write an indication of the location data, the indication of the account number, the indication of the expiration date, and an indication of a card verification value (CVV) to one or more other fields of the EMV payload.~~

3. ~~The contactless card of claim 2, wherein the memory stores an authorization applet and a payment applet, wherein the authorization applet determines that the location of the mobile device is within the threshold distance of the one or more locations the contactless card is permitted for use, wherein the authorization applet receives the indication of the preauthorization of the transaction by the server from the mobile device, wherein the authorization applet generates the encrypted data based on a customer ID associated with the contactless card, wherein the payment applet generates the EMV payload and transmits the EMV payload to the POS device responsive to receiving approval from the authorization applet, the authorization applet to provide approval to the payment applet based on the received indication of the preauthorization of the transaction by the server from the mobile device and the determination that the location of the mobile device is within the threshold distance of the one or more locations the contactless card is permitted for use.~~

4. ~~The contactless card of claim 3, the memory storing instructions which when executed by the processor circuit cause the processor circuit to:~~

~~receive, via the communications interface from the account application executing on the mobile device, an indication that multi-factor authentication for the account has been completed~~

using the mobile device, the multi-factor authentication based on at least two of: (i) a login and password for the account, (ii) a one-time password transmitted to a phone number associated with the account, (iii) biometric credentials associated with the account, (iv) a temporary code generated by an authentication application, and (v) data generated by the contactless card.

5. — The contactless card of claim 3, the POS device to transmit the EMV payload and location data describing a location of the POS device to the server, the memory storing instructions which when executed by the processor circuit cause the processor circuit to:

- prior to transmitting an indication of approval for the transaction to the POS device:

- receive an indication specifying that the server determined that the location of the mobile device is within the threshold distance of the location data describing the location of the POS device; and

- receive an indication specifying that the server verified that the transaction has been preauthorized based on the indication of the preauthorization of the transaction by the server in the first field of the EMV payload.

6. — The contactless card of claim 3, the memory storing instructions which when executed by the processor circuit cause the processor circuit to:

- receive, by the authorization applet via the communications interface from the mobile device, updated location data describing an updated location of the mobile device, the updated location different than the location;

- determine, by the authorization applet based on the one or more rules stored in the memory, that the location of the mobile device is not within the threshold distance of one or more of the locations the contactless card is permitted for use;

- receive, by the payment applet from a second POS device, indication to pay for a second transaction using the contactless card;

- request, by the payment applet, approval from the authorization applet to pay for the second transaction;

- deny, by the authorization applet, approval to pay for the second transaction based on the determination that the location of the mobile device is not within the threshold distance of one or more of the locations the contactless card is permitted for use; and

- transmit, by the payment applet to the second POS device, an indication denying payment for the second transaction using the contactless card based on the denial by the authorization applet.

7. — The contactless card of claim 1, wherein the indication of the preauthorization of the transaction by the server in the transaction data comprises a different indication of the preauthorization of the transaction by the server, wherein the communications interface of the contactless card is configured to support at least one of near field communication (NFC), Bluetooth, and Wi-Fi, the memory storing instructions which when executed by the processor circuit cause the processor circuit to:

- receive a current time associated with the transaction;

- determine, based on the one or more rules stored in the memory, that the current time is within an amount of time permitted to use the contactless card;

- receive, from the POS device, an indication of an amount of the transaction; and

- determine, based on one or more rules stored in the memory, that the amount of the transaction is less than a maximum spend amount associated with the contactless card.

8. — A non-transitory computer-readable storage medium storing instructions which when executed by a processor cause the processor to:

- verify, by a server, encrypted data generated by a contactless card using a cryptographic algorithm and a private key, the encrypted data received by the server from a mobile device executing an account application, one or more credentials for an account associated with the contactless card received by the account application;

determine, by the server based on one or more rules associated with the account, that location data received from the mobile device is within a threshold distance of one or more locations the contactless card is permitted for use;

preauthorize, by the server, a transaction using the contactless card based on the verification of the encrypted data and the determination that the mobile device is within the threshold distance of the one or more locations the contactless card is permitted for use;

transmit, by the server to the account application executing on the mobile device, an indication of the preauthorization for the transaction;

receive, by the server from a point of sale (POS) device, transaction data comprising: (i) indications of an account number and an expiration date of the contactless card, and (ii) the indication of the preauthorization of the transaction by the server; and

approve the transaction by the server based at least in part on identifying the indication of the preauthorization of the transaction by the server in the transaction data.

9. — The non-transitory computer-readable storage medium of claim 8, the transaction data comprising an EMV payload, the non-transitory computer-readable storage medium storing instructions which when executed by the processor cause the processor to:

identify, by the server, the indication of the preauthorization of the transaction by the server in a first field of the EMV payload; and

identify the indication of the account number, the indication of the expiration date, and an indication of a card verification value (CVV) in one or more other fields of the EMV payload.

10. — The non-transitory computer-readable storage medium of claim 9, storing instructions which when executed by the processor cause the processor to:

store, by the server, the indication of the preauthorization; and

compare, by the server, the stored indication of the preauthorization of the transaction by the server to the indication of the preauthorization of the transaction by the server in the first field of the EMV payload.

11. — The non-transitory computer-readable storage medium of claim 10, the preauthorization comprising one or more levels of preauthorization, the levels of preauthorization based on: (i) the server decrypting the encrypted data using a copy of the private key and the cryptographic algorithm, and (ii) determining that location data received from the mobile device is within the threshold distance of one or more locations the contactless card is permitted for use.

12. — The non-transitory computer-readable storage medium of claim 11, the POS device to transmit the EMV payload and location data describing a location of the POS device to the server, the non-transitory computer-readable storage medium storing instructions which when executed by the processor cause the processor to, prior to transmitting an indication of approval for the transaction to the POS device:

determine, by the server, that the location of the mobile device is within the threshold distance the location of the POS device.

13. — The non-transitory computer-readable storage medium of claim 11, storing instructions which when executed by the processor cause the processor to:

receive, by the server, a current time associated with the transaction; and

determine, by the server based on the one or more rules associated with the account, that the current time is within an amount of time permitted to use the contactless card.

14. — The non-transitory computer-readable storage medium of claim 8, wherein a communications interface of the contactless card is configured to support at least one of near field communication (NFC), Bluetooth, and Wi-Fi, storing instructions which when executed by the processor cause the processor to:

receive, by the server from the POS device, an indication of an amount of the transaction; and

determine, by the server based on the one or more rules associated with the account, that the amount of the transaction is less than a maximum spend amount associated with the contactless card;

15. — A method, comprising:

verifying, by a server, encrypted data generated by a contactless card using a cryptographic algorithm and a private key, the encrypted data received by the server from a mobile device executing an account application, one or more credentials for an account associated with the contactless card received by the account application;

determining, by the server based on one or more rules associated with the account, that location data received from the mobile device is within a threshold distance of one or more locations the contactless card is permitted for use;

preauthorizing, by the server, a transaction using the contactless card based on the verification of the encrypted data and the determination that the mobile device is within the threshold distance of the one or more locations the contactless card is permitted for use;

transmitting, by the server to the account application executing on the mobile device, an indication of the preauthorization for the transaction;

receiving, by the server from a point of sale (POS) device, transaction data comprising: (i) indications of an account number and an expiration date of the contactless card, and (ii) the indication of the preauthorization of the transaction by the server; and

approving the transaction by the server based at least in part on identifying the indication of the preauthorization of the transaction by the server in the transaction data.

16. — The method of claim 15, the transaction data comprising an EMV payload, the method further comprising:

identifying, by the server, the indication of the preauthorization of the transaction by the server in a first field of the EMV payload; and

identifying the indication of the account number, the indication of the expiration date, and an indication of a card verification value (CVV) in one or more other fields of the EMV payload.

17. — The method of claim 16, further comprising:

— storing, by the server, the indication of the preauthorization; and

— comparing, by the server, the stored indication of the preauthorization of the transaction by the server to the indication of the preauthorization of the transaction by the server in the first field of the EMV payload.

18. — The method of claim 17, the preauthorization comprising one or more levels of preauthorization, the levels of preauthorization based on: (i) the server decrypting the encrypted data using a copy of the private key and the cryptographic algorithm, and (ii) determining that location data received from the mobile device is within the threshold distance of one or more locations the contactless card is permitted for use.

19. — The method of claim 17, wherein the POS device transmits the EMV payload and location data describing a location of the POS device to the server, the method further comprising prior to transmitting an indication of approval for the transaction to the POS device:

determining, by the server, that the location of the mobile device is within the threshold distance the location of the POS device.

20. — The method of claim 15, wherein a communications interface of the contactless card is configured to support at least one of near field communication (NFC), Bluetooth, and Wi-Fi, the method further comprising prior to approving the transaction:

receiving, by the server, a current time associated with the transaction;

determining, by the server based on the one or more rules associated with the account, that the current time is within an amount of time permitted to use the contactless card;

receiving, by the server from the POS device, an indication of an amount of the transaction; and

~~determining, by the server based on the one or more rules associated with the account, that the amount of the transaction is less than a maximum spend amount associated with the contactless card.~~

1. A contactless card, comprising:

a processor circuit;

a communications interface; and

a memory storing instructions which when executed by the processor circuit, cause the processor circuit to:

receive, via the communications interface from an account application executing on a mobile device, an indication that a server preauthorized a transaction based on location data describing a location of the mobile device and decryption of encrypted data, the encrypted data generated by the contactless card using a cryptographic algorithm and a key stored in the memory of the contactless card, the indication further specifying that one or more credentials for an account associated with the contactless card have received by the account application;

receive, via the communications interface from a point of sale (POS) device, an indication to pay for the transaction using the contactless card;

determine, based on one or more rules stored in the memory, that the location of the mobile device is within a threshold distance of one or more locations the contactless card is permitted for use;

generate transaction data comprising: (i) indications of an account number and an expiration date of the contactless card, and (ii) the indication of the preauthorization of the transaction by the server;

transmit the transaction data to the POS device as payment for the transaction; and

receive, from the POS device, an indication that the server authorized payment for the transaction using at least a portion of the transaction data and based at least in part on identifying the indication of the preauthorization of the transaction by the server in the transaction data.

2. The contactless card of claim 1, the memory storing instructions which when executed by the processor circuit cause the processor circuit to:

write the indication of the preauthorization of the transaction by the server to a first field of an EMV payload; and

write an indication of the location data, the indication of the account number, the indication of the expiration date, and an indication of a card verification value (CVV) to one or more other fields of the EMV payload.

3. The contactless card of claim 2, wherein the memory stores an authorization applet and a payment applet, wherein the authorization applet determines that the location of the mobile device is within the threshold distance of the one or more locations the contactless card is permitted for use, wherein the authorization applet receives the indication of the preauthorization of the transaction by the server from the mobile device, wherein the authorization applet generates the encrypted data based on a customer ID associated with the contactless card, wherein the payment applet generates the EMV payload and transmits the EMV payload to the POS device responsive to receiving approval from the authorization applet, the authorization applet to provide approval to the payment applet based on the received indication of the preauthorization of the transaction by the server from the mobile device and the determination that the location of the mobile device is within the threshold distance of the one or more locations the contactless card is permitted for use.

4. The contactless card of claim 3, the memory storing instructions which when executed by the processor circuit cause the processor circuit to:

receive, via the communications interface from the account application executing on the mobile device, an indication that multi-factor authentication for the account has been completed using the mobile device, the multi-factor authentication based on at least two of: (i) a login and password for the account, (ii) a one-time password transmitted to a phone number associated with the account, (iii) biometric credentials associated with the account, (iv) a temporary code generated by an authentication application, and (v) data generated by the contactless card.

5. The contactless card of claim 3, the memory storing instructions which when executed by the processor circuit cause the processor circuit to:

prior to transmitting an indication of approval for the transaction to the POS device: receive an indication specifying that the server determined that the location of the mobile device is within the threshold distance of location data describing a location of the POS device; and

receive an indication specifying that the server verified that the transaction has been preauthorized based on the indication of the preauthorization of the transaction by the server in the first field of the EMV payload.

6. The contactless card of claim 3, the memory storing instructions which when executed by the processor circuit cause the processor circuit to:

receive, by the authorization applet via the communications interface from the mobile device, updated location data describing an updated location of the mobile device, the updated location different than the location;

determine, by the authorization applet based on the one or more rules stored in the memory, that the location of the mobile device is not within the threshold distance of one or more of the locations the contactless card is permitted for use;

receive, by the payment applet from a second POS device, indication to pay for a second transaction using the contactless card;

request, by the payment applet, approval from the authorization applet to pay for the second transaction;

deny, by the authorization applet, approval to pay for the second transaction based on the determination that the location of the mobile device is not within the threshold distance of one or more of the locations the contactless card is permitted for use; and

transmit, by the payment applet to the second POS device, an indication denying payment for the second transaction using the contactless card based on the denial by the authorization applet.

7. The contactless card of claim 1, wherein the indication of the preauthorization of the transaction by the server in the transaction data comprises a different indication of the preauthorization of the transaction by the server, wherein the communications interface of the contactless card is configured to support at least one of near field communication (NFC), Bluetooth, and Wi-Fi, the memory storing instructions which when executed by the processor circuit cause the processor circuit to:

receive a current time associated with the transaction;

determine, based on the one or more rules stored in the memory, that the current time is within an amount of time permitted to use the contactless card;

receive, from the POS device, an indication of an amount of the transaction; and

determine, based the on one or more rules stored in the memory, that the amount of the transaction is less than a maximum spend amount associated with the contactless card.

8. A non-transitory computer-readable storage medium storing instructions which when executed by a processor of a server cause the processor to:

receive encrypted data from an account application of a mobile device;

decrypt the encrypted data using a cryptographic algorithm and a key, wherein the key is associated with a contactless card;

determine, based on one or more rules associated with the account, that location data received from the mobile device is within a threshold distance of one or more locations the contactless card is permitted for use;

preauthorize a transaction using the contactless card based on the decryption of the encrypted data and the determination that the mobile device is within the threshold distance of the one or more locations the contactless card is permitted for use;

transmit, to the account application, an indication of the preauthorization for the transaction;

receive, from a point of sale (POS) device, transaction data comprising: (i) indications of an account number and an expiration date of the contactless card, and (ii) an instance of the indication of the preauthorization of the transaction received by the POS device from the contactless card; and

approve the transaction based at least in part on identifying the indication of the preauthorization of the transaction by the server in the transaction data.

9. The non-transitory computer-readable storage medium of claim 8, the transaction data comprising an EMV payload, the non-transitory computer-readable storage medium storing instructions which when executed by the processor of the server cause the processor to:

identify the instance of the indication of the preauthorization of the transaction in a first field of the EMV payload; and

identify the indication of the account number, the indication of the expiration date, and an indication of a card verification value (CVV) in one or more other fields of the EMV payload.

10. The non-transitory computer-readable storage medium of claim 9, storing instructions which when executed by the processor cause the processor to:

store the indication of the preauthorization;

compare, the stored indication of the preauthorization of the transaction to the instance of the indication of the preauthorization of the transaction in the first field of the EMV payload;

determine the comparison results in a match; and

transmit an indication of approval for the transaction to the POS device.

11. The non-transitory computer-readable storage medium of claim 10, the preauthorization comprising one or more levels of preauthorization, the levels of preauthorization based on: (i) the server decrypting the encrypted data using a copy of the key and the cryptographic algorithm, and (ii) determining that location data received from the mobile device is within the threshold distance of one or more locations the contactless card is permitted for use.

12. The non-transitory computer-readable storage medium of claim 11, storing instructions which when executed by the processor cause the processor to, prior to prior to transmitting the indication of approval for the transaction to the POS device:

receive, from the POS device, the EMV payload and location data describing a location of the POS device; and

determine that the location of the mobile device is within the threshold distance the location of the POS device.

13. The non-transitory computer-readable storage medium of claim 11, storing instructions which when executed by the processor cause the processor to:

receive a current time associated with the transaction; and

determine, based on the one or more rules associated with the account, that the current time is within an amount of time permitted to use the contactless card.

14. The non-transitory computer-readable storage medium of claim 8, wherein the indication of the preauthorization is one of a plurality of indications of preauthorization, wherein each indication of preauthorization is for a respective transaction of a plurality of transactions including the transaction, wherein each indication of preauthorization further comprises a unique identifier of the respective indication of preauthorization, the medium storing instructions which when executed by the processor cause the processor to:

receive, from the POS device, an indication of an amount of the transaction; and

determine, based on the one or more rules associated with the account, that the amount of the transaction is less than a maximum spend amount associated with the contactless card.

15. A method, comprising:

receiving, by a server, encrypted data from an account application executing on a mobile device;

decrypting, by the server, the encrypted data using a cryptographic algorithm and a key, wherein the key is associated with a contactless card;

determining, by the server based on one or more rules associated with the account, that location data received from the mobile device is within a threshold distance of one or more locations the contactless card is permitted for use;

preauthorizing, by the server, a transaction using the contactless card based on the decryption of the encrypted data and the determination that the mobile device is within the threshold distance of the one or more locations the contactless card is permitted for use;

transmitting, by the server to the account application, an indication of the preauthorization for the transaction;

receiving, by the server from a point of sale (POS) device, transaction data comprising: (i) indications of an account number and an expiration date of the contactless card, and (ii) an instance of the indication of the preauthorization of the transaction received by the POS device from the contactless card; and

approving the transaction by the server based at least in part on identifying the indication of the preauthorization of the transaction by the server in the transaction data.

16. The method of claim 15, the transaction data comprising an EMV payload, the method further comprising:

identifying, by the server, the indication of the preauthorization of the transaction by the server in a first field of the EMV payload; and

identifying the indication of the account number, the indication of the expiration date, and an indication of a card verification value (CVV) in one or more other fields of the EMV payload.

17. The method of claim 16, further comprising:

storing, by the server, the indication of the preauthorization;

comparing, by the server, the stored indication of the preauthorization of the transaction to the indication of the preauthorization of the transaction in the first field of the EMV payload;

determining the comparison results in a match; and

transmitting an indication of approval for the transaction to the POS device.

18. The method of claim 17, wherein the preauthorization is a first level of preauthorization of a plurality of levels of preauthorization, wherein the plurality of levels of preauthorization are distinct from the account number of the contactless card.

19. The method of claim 18, further comprising:

selecting, by the server, the first level of preauthorization based on: (i) the server decrypting the encrypted data using a copy of the key and the cryptographic algorithm, (ii) determining that location data received from the mobile device is within the threshold distance of one or more locations the contactless card is permitted for use, (iii) completion of multi-factor authentication for the account, and (iv) the one or more rules.

20. The method of claim 15, wherein the indication of the preauthorization is one of a plurality of indications of preauthorization, wherein each indication of preauthorization is for a respective transaction of a plurality of transactions including the transaction, wherein each indication of preauthorization further comprises a unique identifier of the respective indication of preauthorization, wherein a communications interface of the contactless card is configured to support at least one of near field communication (NFC), Bluetooth, and Wi-Fi, the method further comprising prior to approving the transaction:

receiving, by the server, a current time associated with the transaction;

determining, by the server based on the one or more rules associated with the account, that the current time is within an amount of time permitted to use the contactless card;

receiving, by the server from the POS device, an indication of an amount of the transaction; and

determining, by the server based on the one or more rules associated with the account, that the amount of the transaction is less than a maximum spend amount associated with the contactless card.