

CONSTRAINING TRANSACTIONAL CAPABILITIES FOR CONTACTLESS CARDS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to U.S. Patent Application Serial No. 16/503,142, entitled “CONSTRAINING TRANSACTIONAL CAPABILITIES FOR CONTACTLESS CARDS” filed on July 3, 2019. The contents of the aforementioned patent application are incorporated herein by reference in their entirety.

TECHNICAL FIELD

[0002] Embodiments herein generally relate to contactless cards, and more specifically, to constraining transactional capabilities for contactless cards.

BACKGROUND

[0003] Cardholders (e.g., credit card holders, bank card holders, etc.) often obtain additional physical cards and/or virtual card numbers for trusted individuals, such as family members, employees, and the like. However, doing so may expose security risks. Conventional solutions do not provide the requisite security mechanisms to ensure that the physical cards and/or virtual card numbers are used in accordance with any defined restrictions.

SUMMARY

[0004] Embodiments disclosed herein provide systems, methods, articles of manufacture, and computer-readable media for constraining transactional capabilities of contactless cards. In one example, a communications interface may receive, 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, one or more credentials for an account associated with the contactless card received by the account application. The communications interface may receive, from a point of sale (POS) device, an indication to pay for the transaction using the contactless card. The contactless card may 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. The contactless card may 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. The contactless card may transmit the transaction data to the POS device as payment for the transaction, the server to authorize payment for the transaction using at least a portion of the transaction data based at least in part on identifying the indication of the preauthorization of the transaction by the server in the transaction data.

[0004a] An aspect of the disclosure provides 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.

[0004b] Another aspect of the disclosure provides 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.

[0004c] Another aspect of the disclosure provides 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.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] Figures 1A-1D illustrate embodiments of a system to constrain transactional capabilities for contactless cards.

[0006] Figures 2A-2B illustrate embodiments of constraining transactional capabilities for contactless cards.

[0007] Figures 3A-3D illustrate embodiments of constraining transactional capabilities for contactless cards.

[0008] Figure 4 illustrates an embodiment of a first logic flow.

[0009] Figure 5 illustrates an embodiment of a second logic flow.

[0010] Figure 6 illustrates an embodiment of a third logic flow.

[0011] Figure 7 illustrates an embodiment of a fourth logic flow.

[0012] Figure 8 illustrates an embodiment of a fifth logic flow.

[0013] Figure 9 illustrates an embodiment of a computing architecture.

[0014] Figures 10A-10B illustrate an example contactless card.

DETAILED DESCRIPTION

[0015] Embodiments disclosed herein provide secure techniques to constrain transactional capabilities of contactless cards. Generally, a contactless card may be programmed to include