AUTHENTICATION FOR THIRD PARTY DIGITAL WALLET PROVISIONING

RELATED APPLICATIONS

[0001] This application claims priority to U.S. Patent Application Serial No. 16/725,435, titled "AUTHENTICATION FOR THIRD PARTY DIGITAL WALLET PROVISIONING" filed on December 23, 2019. The contents of the aforementioned application are incorporated herein by reference in their entirety.

BACKGROUND

[0002] A digital wallet refers to an electronic device or online service that allows an individual to make electronic transactions, such as purchasing items online with a computing device, using a smartphone to make purchases at a store, etc. Typically, various types of payment instruments, e.g., bank account, debit card, credit card, are added or linked to the digital wallet. When making an in-store purchase, for example, credentials associated with the individual's preferred payment instrument may be passed to a merchant's terminal wirelessly via near field communication (NFC).

[0003] There are, however, many security-related challenges associated with digital wallets, one of which may be ensuring that the individual is the one who is actually using the payment instrument. For example, a fraudster may use stolen card or identity information to fraudulently add or link a payment instrument to make unauthorized purchases. Accordingly, there is a need for properly verifying the identity of and authenticating the individual adding or linking the payment instrument to the digital wallet in an effective and robust manner.

SUMMARY

[0003a] According to an aspect, there is provided an apparatus comprising: memory configured to store instructions; one or more processors coupled with the memory, the one or more processors configured to process the instructions that, when executed by the one or more processors, causes the one or more processors to: present, in a graphical user interface (GUI) of third-party application, an option to add or link account information associated with a contactless card with a third-party wallet; detect, by the third-party application, a selection of the option to add or link the account information for the contactless card with a third-party wallet; determine, by the third-party application, to perform an authentication operation with the contactless card to authenticate the contactless card; cause, by the third-party application, a first-party application to perform the authentication operation,

wherein the first-party application to perform a near-field communication (NFC) exchange with the contactless card; receive, by the first-party application via an NFC interface, a cryptogram in the NFC exchange from the contactless card, the cryptogram comprising authentication information to authenticate the contactless card; authenticate, by the first-party application, the authentication information; in response to authenticating the authentication information, link, by the third-party application, the account information for the contactless card with the third-party wallet.

[0003b] According to another aspect, there is provided an apparatus comprising: memory configured to store instructions; one or more processors coupled with the memory, the one or more processors configured to process the instructions that, when executed by the one or more processors, causes the one or more processors to: present, in a graphical user interface (GUI) of a first-pay application, an option to add or link account information associated with a contactless card with a third-party wallet for a third-party application; detect, by the first-party application, a selection of the option to add or link the account information for the contactless card with a third-party wallet; determine, by the first-party application, to perform an authentication operation with the contactless card to authenticate the contactless card; perform, by the first-party application, a near-field communication (NFC) exchange with the contactless card; receive, by the first-party application via an NFC interface, a cryptogram in the NFC exchange from the contactless card, the cryptogram comprising authentication information to authenticate the contactless card; authenticate, by the first-party application, the authentication information; in response to authenticating the authentication information, cause the third-party application to add or link the account information for the contactless card with the third-party wallet.

[0003c] According to another aspect, there is provided a computer-implemented method comprising: determining, by a third-party application, to add or link account information associated with a contactless card with a third-party wallet; determining, by the third-party application, to perform an authentication operation with the contactless card to authenticate the contactless card with a first-party application; initiating, by the third-party application, the first-party application to perform the authentication operation; performing, by the first-party application, the authentication operation including performing a near-field communication (NFC) exchange with the contactless card; receiving, by the first-party application via an NFC interface, a cryptogram in the NFC exchange from the contactless card, the cryptogram comprising authentication information to authenticate the contactless card; authenticating, by the first-party application, the authentication information;

in response to authenticating the authentication information, enabling, by the first-party application, the third-party application to link or add the account information with the third-party wallet.

[0004] Various embodiments are directed to securely verifying an identity of a user who is requesting to add or link a financial instrument to a third-party digital wallet using one-tap contactless card authentication. The financial instrument may be added or linked to the third-party wallet in at least two scenarios: pull provisioning and push provisioning. In either provisioning scenarios, the user may be required to authenticate the financial instrument being added or linked by successfully verifying the identity of

CLAIMS

1. An apparatus, comprising:

memory configured to store instructions;

one or more processors coupled with the memory, the one or more processors configured to process the instructions that, when executed by the one or more processors, causes the one or more processors to:

present, in a graphical user interface (GUI) of third-party application, an option to add or link account information associated with a contactless card with a third-party wallet;

detect, by the third-party application, a selection of the option to add or link the account information for the contactless card with a third-party wallet;

determine, by the third-party application, to perform an authentication operation with the contactless card to authenticate the contactless card;

cause, by the third-party application, a first-party application to perform the authentication operation, wherein the first-party application to perform a near-field communication (NFC) exchange with the contactless card;

receive, by the first-party application via an NFC interface, a cryptogram in the NFC exchange from the contactless card, the cryptogram comprising authentication information to authenticate the contactless card;

authenticate, by the first-party application, the authentication information;

in response to authenticating the authentication information, link, by the third-party application, the account information for the contactless card with the third-party wallet.

2. The apparatus of claim 1, wherein the instructions are further configured to cause the one or more processors to receive, by the third-party application, user login information to log into an account associated with the third-party application.

3. The apparatus of claim 1, wherein the third-party application is a payment application and the first-party application is a banking application.

4. The apparatus of claim 1, wherein the instructions further cause the one or more processors to receive, by the first-party application, permission to share the account information with the third-party wallet.

5. The apparatus of claim 1, wherein the instructions are further configured to cause the one or more processors to send, by the first-party application, the cryptogram to a remote server to authenticate the authentication information.

6. The apparatus of claim 5, wherein the instructions are further configured to cause the one or more processor to receive, by the first-party application, an indication that the authentication information is successfully authenticated by the remote server.

7. The apparatus of claim 1, wherein the cryptogram is received as one or more NFC data exchange format (NDEF) messages from the contactless card.

8. An apparatus, comprising:

memory configured to store instructions;

one or more processors coupled with the memory, the one or more processors configured to process the instructions that, when executed by the one or more processors, causes the one or more processors to:

present, in a graphical user interface (GUI) of a first-pay application, an option to add or link account information associated with a contactless card with a third-party wallet for a third-party application;

detect, by the first-party application, a selection of the option to add or link the account information for the contactless card with a third-party wallet;

determine, by the first-party application, to perform an authentication operation with the contactless card to authenticate the contactless card;

perform, by the first-party application, a near-field communication (NFC) exchange with the contactless card;

receive, by the first-party application via an NFC interface, a cryptogram in the NFC exchange from the contactless card, the cryptogram comprising authentication information to authenticate the contactless card;

authenticate, by the first-party application, the authentication information;

in response to authenticating the authentication information, cause the third-party application to add or link the account information for the contactless card with the third-party wallet.

9. The apparatus of claim 8, wherein the instructions are further configured to cause the one or more processors to receive, by the first-party application, user login information to log into an account associated with the first-party application.

10. The apparatus of claim 8, wherein the third-party wallet is associated with a payment application and the first-party application is a banking application.

11. The apparatus of claim 8, wherein the instructions further cause the one or more processors to receive, by the first-party application, permission to share the account information with the third-party wallet.

12. The apparatus of claim 8, wherein the instructions are further configured to cause the one or more processors to send, by the first-party application, the cryptogram to a remote server to authenticate the authentication information.

13. The apparatus of claim 12, wherein the instructions are further configured to cause the one or more processor to receive, by the first-party application, an indication that the authentication information is successfully authenticated by the remote server.

14. The apparatus of claim 8, wherein the cryptogram is received as one or more NFC data exchange format (NDEF) messages from the contactless card.

15. A computer-implemented method, comprising:

determining, by a third-party application, to add or link account information associated with a contactless card with a third-party wallet;

determining, by the third-party application, to perform an authentication operation with the contactless card to authenticate the contactless card with a first-party application;

initiating, by the third-party application, the first-party application to perform the authentication operation;

performing, by the first-party application, the authentication operation including performing a near-field communication (NFC) exchange with the contactless card;

receiving, by the first-party application via an NFC interface, a cryptogram in the NFC exchange from the contactless card, the cryptogram comprising authentication information to authenticate the contactless card;

authenticating, by the first-party application, the authentication information;

in response to authenticating the authentication information, enabling, by the first-party application, the third-party application to link or add the account information with the third-party wallet.

16. The computer-implemented method of claim 15, comprising receiving, by the third-party application, user login information to log into an account associated with the third-party application.

17. The computer-implemented method of claim 15, wherein the third-party application is a payment application and the first-party application is a banking application.

18. The computer-implemented method of claim 15, comprising receiving, by the first-party application, permission to share the account information with the third-party wallet.

19. The computer-implemented method of claim 15, comprising:

sending, by the first-party application, the cryptogram to a remote server to authenticate the authentication information; and

receiving, by the first-party application, an indication that the authentication information is successfully authenticated by the remote server.

20. The computer-implemented method of claim 15, wherein the cryptogram is received as one or more NFC data exchange format (NDEF) messages from the contactless card.