

approval before cards are provisioned on a phone to ensure the card is legitimately added to the phone has become unduly burdensome and technically difficult.

[0001] As such, many application developers have allowed accounts to be added to their mobile payment applications without verifying or obtaining approval from account issuers. Thus, because issuers are not contacted during account provisioning, fraudsters may be capable of provisioning account data into a phone that otherwise would be denied by an issuer.

[0002] Further, many mobile application developers have not informed relying parties (e.g., merchants) during transactions that such accounts added to the application have not been verified by an issuer. As such, the relying parties have no means for knowing whether an account has been verified prior to a transaction being initiated. Thus, relying parties do not know whether to trust the account information they receive during mobile payment transactions. Accordingly, there is a need to allow for unverified account information to be used in a transaction initiated by a mobile payment application without creating security concerns for relying transaction parties.

[0003] Embodiments of the invention address these and other problems, individually and collectively.

SUMMARY

[0004] According to a first aspect of the present invention, there is provided a method comprising: receiving, by the mobile device, a priority selection of one or more applets, wherein each of the one or more applets is associated with credentials stored on the mobile device; determining, by the mobile device, a status for each of the one or more applets as being a trusted applet or an untrusted applet based on a provisioning process associated with each of the one or more applets; categorizing, by the mobile device, an applet identifier for each of the one or more applets as trusted applet identifiers or untrusted applet identifiers based on the status for each of the one or more applets; generating, by the mobile device, the list of available applets including the trusted applet identifiers and the untrusted applet identifiers; receiving, by the mobile device, a request for available applets from an access device; providing, by the mobile device, the list of available applets including trusted applet identifiers and untrusted applet identifiers to the access device; receiving, by the mobile device, a selection of an untrusted applet identifier from the list and an entity identifier associated with the access device; validating, by the mobile device, that the access device is authorized to access credentials associated with the selected untrusted applet identifier using the entity identifier; and providing, by the mobile device, the credentials associated with the selected untrusted applet identifier to the access device.

[0005] According to a second aspect of the present invention, there is provided a method comprising: sending, by an access device, a request for available applets to a mobile device; receiving, by the access device, a list of available applets including trusted applet identifiers and untrusted applet identifiers, the list of available applets including a wallet identifier for each of the available applets, wherein the wallet identifier identifies a mobile application that is associated with each of the available applets; determining, by the access device, supported applet identifiers from the list of available applets; determining, by the access device, that a highest priority applet of the supported applet identifiers includes an untrusted applet identifier; validating, by the access device, that the wallet identifier is associated with a trusted entity before selecting the untrusted applet from the list; providing, by the access device, a selection of the untrusted applet identifier from the list; and receiving, by the access device, credentials associated with the selected untrusted applet identifier from the mobile application of the mobile device.

[0006] According to a third aspect of the present invention, there is provided system comprising: a mobile device configured to: receive a request for available applets from an access device; provide a list of available applets including trusted applet identifiers and untrusted applet identifiers to the access device, the list of available applets including a wallet identifier for each of the available applets, wherein the wallet identifier identifies a mobile application that is associated with each of the available applets; receive a selection of an untrusted applet identifier from the list and an entity identifier associated with the access device; validate that the access device is authorized to access credentials associated with the selected untrusted applet identifier using the entity identifier; and provide the credentials associated with the selected untrusted applet identifier to the access device; and the access device configured to: send the request for available applets to the mobile device; receive the list of available applets including the trusted applet identifiers and the untrusted applet identifiers; determine supported applet identifiers from the list of available applets; determine that a highest priority applet of the supported applet identifiers includes an untrusted applet identifier; validate that the wallet identifier is associated with a trusted entity before selecting the untrusted applet from the list; provide the selection of the untrusted applet identifier from the list; and receive credentials associated with the selected untrusted applet identifier from the mobile application of the mobile device.

[0007] These and other embodiments of the invention are described in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] FIG. 1 illustrates an exemplary block diagram of an enhanced data interface system, according to one embodiment of the present invention.

CLAIMS

1. A method comprising:

receiving, by the mobile device, a priority selection of one or more applets, wherein each of the one or more applets is associated with credentials stored on the mobile device;

determining, by the mobile device, a status for each of the one or more applets as being a trusted applet or an untrusted applet based on a provisioning process associated with each of the one or more applets;

categorizing, by the mobile device, an applet identifier for each of the one or more applets as trusted applet identifiers or untrusted applet identifiers based on the status for each of the one or more applets;

generating, by the mobile device, the list of available applets including the trusted applet identifiers and the untrusted applet identifiers;

receiving, by the mobile device, a request for available applets from an access device;

providing, by the mobile device, the list of available applets including trusted applet identifiers and untrusted applet identifiers to the access device;

receiving, by the mobile device, a selection of an untrusted applet identifier from the list and an entity identifier associated with the access device;

validating, by the mobile device, that the access device is authorized to access credentials associated with the selected untrusted applet identifier using the entity identifier; and

providing, by the mobile device, the credentials associated with the selected untrusted applet identifier to the access device.

2. The method of claim 1, wherein categorizing the applet identifier as an untrusted applet identifier comprises mapping the applet identifier to a predetermined untrusted applet identifier associated with the applet identifier.

3. The method of claim 1, wherein the status of an applet is determined to be untrusted where an issuer associated with the credentials of the applet did not participate in the provisioning process of the applet.

4. The method of claim 1, wherein the status of an applet is determined to be untrusted based on an identity of an application that provisioned the applet.

5. The method of claim 1, wherein validating that the access device is authorized to use the selected untrusted applet further comprises:

comparing, by the mobile device, the entity identifier to a list of trusted entity identifiers associated with the mobile application.

6. The method of claim 1, wherein the list of available applets includes a wallet identifier associated with the mobile application, and wherein the access device validates that the wallet identifier is associated with a trusted entity before selecting the untrusted applet identifier from the list of available applets.

7. The method of claim 1, wherein before providing the credentials, the method further comprises:

receiving, by the mobile device, access device configuration information; and
validating, by the mobile device, that the access device is configured to support transactions initiated using untrusted applet identifiers based on the access device configuration information.

8. The method of claim 1, wherein the provided credentials associated with the selected untrusted applet include an untrusted applet indicator, wherein the untrusted applet indicator allows entities relying on transaction information within a transaction payload to identify the transaction as being initiated using an untrusted applet.

9. A method comprising:

sending, by an access device, a request for available applets to a mobile device;

receiving, by the access device, a list of available applets including trusted applet identifiers and untrusted applet identifiers, the list of available applets including a wallet identifier for each of the available applets, wherein the wallet

identifier identifies a mobile application that is associated with each of the available applets;

determining, by the access device, supported applet identifiers from the list of available applets;

determining, by the access device, that a highest priority applet of the supported applet identifiers includes an untrusted applet identifier;

validating, by the access device, that the wallet identifier is associated with a trusted entity before selecting the untrusted applet from the list;

providing, by the access device, a selection of the untrusted applet identifier from the list; and

receiving, by the access device, credentials associated with the selected untrusted applet identifier from the mobile application of the mobile device.

10. The method of claim 9, wherein determining supported applet identifiers from the list of available applets comprises:

matching, by the access device, each of the applet identifiers in the list of available applets to a list of supported applet identifiers stored in the access device; and

storing, by the access device, each of the matching applet identifiers as one of the supported applet identifiers in order of priority indicated by the mobile device.

11. The method of claim 9, wherein determining that the highest priority applet identifier of the supported applet identifiers includes the untrusted applet identifier comprises:

comparing, by the access device, the highest priority applet identifier to a directory of trusted applet identifiers and untrusted applet identifiers; and

matching, by the access device, the highest priority applet identifier to an untrusted applet identifier within the directory.

12. The method of claim 9, wherein an applet is assigned an untrusted applet identifier by the mobile application where an issuer associated with credentials of the applet did not participate in the provisioning process of the applet.

13. The method of claim 9, wherein before receiving the credentials associated with the selected untrusted applet identifier, the method further comprises:

providing, by the access device, an entity identifier associated with the access device to the mobile device, wherein the mobile application of the mobile device validates that the access device is authorized to access the credentials associated with the selected untrusted applet identifier using the entity identifier.

14. The method of claim 13, wherein the mobile application validates that the access device is authorized to access the credentials associated with the selected untrusted applet identifier using the entity identifier by comparing the entity identifier to a list of trusted entity identifiers associated with the mobile application.

15. The method of claim 9, wherein before receiving the credentials associated with the selected untrusted applet identifier, the method further comprises:

providing, by the access device, access device configuration information, wherein the mobile application validates that the access device is configured to support transactions initiated using untrusted applet identifiers based on the access device configuration information.

16. The method of claim 9, wherein the received credentials associated with the selected untrusted applet identifier include an untrusted applet indicator, wherein the untrusted applet indicator allows entities to identify the credentials as being associated with an untrusted applet.

17. The method of claim 9, wherein the list of available applets further comprises a multiple entity applet identifier, wherein the method further comprises:

determining, by the access device, that the multiple entity applet identifier is supported by the access device;

providing, by the access device, a selection of the multiple entity applet to the mobile device;

providing, by the access device, an entity identifier associated with the access device, wherein the multiple entity applet associated with the multiple entity applet

identifier uses the entity identifier to determine relevant information to the entity associated with the access device; and

receiving, by the access device, the relevant information.

18. A system comprising:

a mobile device configured to:

receive a request for available applets from an access device;

provide a list of available applets including trusted applet identifiers and untrusted applet identifiers to the access device, the list of available applets including a wallet identifier for each of the available applets, wherein the wallet identifier identifies a mobile application that is associated with each of the available applets;

receive a selection of an untrusted applet identifier from the list and an entity identifier associated with the access device;

validate that the access device is authorized to access credentials associated with the selected untrusted applet identifier using the entity identifier; and

provide the credentials associated with the selected untrusted applet identifier to the access device; and

the access device configured to:

send the request for available applets to the mobile device;

receive the list of available applets including the trusted applet identifiers and the untrusted applet identifiers;

determine supported applet identifiers from the list of available applets;

determine that a highest priority applet of the supported applet identifiers includes an untrusted applet identifier;

validate that the wallet identifier is associated with a trusted entity before selecting the untrusted applet from the list;

provide the selection of the untrusted applet identifier from the list; and

receive credentials associated with the selected untrusted applet identifier from the mobile application of the mobile device.