

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.

[0004] 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.

[0005] 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.

[0006] Embodiments of the invention address these and other problems, individually and collectively.

SUMMARY

[0007] 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.

[0008] 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.

[0009] 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.

[0010] These and other embodiments of the invention are described in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] FIG. 1 illustrates an exemplary block diagram of an enhanced data interface system, according to one embodiment of the present invention.