

WHAT IS CLAIMED IS:

1. A method comprising:

a) receiving, at a first software module on a mobile device, the mobile device comprising the first software module configured to execute acceptance processing and a second software module configured to manage payment credentials and/or tokens and to emulate a user device associated with a user, one or more identifiers associated with one or more physical items external to the mobile device, the one or more identifiers being read by the mobile device using an input component in a purchase transaction;

after step a), b) receiving, by the first software module, configuration data from a remote computer, the configuration data allowing the second software module to communicate with the remote computer via the first software module;

c) receiving, at the first software module, an indication that an authorization request is to be initiated;

d) exchanging, between the first software module and the second software module of the mobile device, interaction data associated with the one or more physical items and a token associated with the user by:

providing, by the first software module, an API call comprising the interaction data to the second software module, wherein the second software module evaluates the interaction data and the first software module and determines whether or not to respond to the API call based on a determination that the first software module is authentic and the interaction data; and

responsive to the evaluation, receiving, by the first software module, an API response comprising the token from the second software module; and

e) transmitting, by the first software module, the interaction data and the token associated with the user to the remote computer comprising acceptance processing software with which the first software module has registered in order to enable the first software module to exchange information with the remote computer, the

transmitting causing the remote computer to generate an authorization request message for the purchase transaction, the authorization request message comprising the interaction data and the token.

2. The method of claim 1, wherein the first software module is hosted by a resource provider, and wherein the mobile device is operated by an entity different from the resource provider associated with the first software module.

3. The method of claim 1, wherein providing, by the first software module, the API call to the second software module is based on the configuration data.

4. The method of claim 1, wherein the API response further includes a cryptogram associated with the token.

5. The method of claim 1, wherein the first software module communicates directly with the second software module via the API call and the API response.

6. The method of claim 1, wherein the one or more physical items are involved in an interaction between the user of the mobile device and a resource provider that hosts the first software module, wherein the remote computer provides the authorization request message to an authorizing entity computer and wherein the authorizing entity computer determines whether or not to authorize the interaction and generates an authorization response message, and wherein the method further comprises:

receiving, by the first software module, the authorization response message comprising an indication of whether or not the interaction is authorized from the remote computer; and

displaying, by the first software module, the indication of whether or not the interaction is authorized to the user.

7. The method of claim 1, wherein the input component includes a code scanner, a reader, a camera, or one or more RF transceivers that send and receive communications using NFC, radio frequency, or wireless communication protocols including Bluetooth, BLE, Wi-Fi, and iBeacon.

8. The method of claim 1, wherein prior to exchanging, between the first software module and the second software module of the mobile device, the interaction data associated with the one or more physical items and the token associated with the user, the method further comprises:

receiving, by the second software module of the mobile device, the token from a mobile application platform; and

storing, by the second software module of the mobile device, the token in a secure element of the mobile device, whereby the first software module cannot access the token without the second software module.

9. A mobile device comprising:

one or more processors; and

one or more memories storing computer executable instructions that, when executed by the one or more processors, cause the mobile device to perform steps comprising:

receiving, at a first software module on the mobile device, the mobile device comprising the first software module configured to execute acceptance processing and a second software module configured to manage payment credentials and/or tokens and to emulate a user device associated with a user, one or more identifiers associated with one or more physical items external to the mobile device, the one or more identifiers being read by the mobile device using an input component in a purchase transaction;

after step a), b) receiving, by the first software module, configuration data from a remote computer, the configuration data allowing the second software module to communicate with the remote computer via the first software module;

c) receiving, at the first software module, an indication that an authorization request is to be initiated;

d) exchanging, between the first software module and the second software module of the mobile device, interaction data associated with the one or more physical items and a token associated with the user by:

providing, by the first software module, an API call comprising the interaction data to the second software module, wherein the second software module evaluates the interaction data and the first software module and determines whether or not to respond to the API call based on a determination that the first software module is authentic and the interaction data; and

responsive to the evaluation, receiving, by the first software module, an API response comprising the token from the second software module; and

e) transmitting, by the first software module, the interaction data and the token associated with the user to the remote computer comprising acceptance processing software with which the first software module has registered in order to enable the first software module to exchange information with the remote computer, the transmitting causing the remote computer to generate an authorization request message for the purchase transaction, the authorization request message comprising the interaction data and the token.

10. The mobile device of claim 9 further comprising:
a secure element; and
the input component.

11. The mobile device of claim 9, wherein prior to exchanging, between the first software module and the second software module of the mobile device, the interaction data associated with the one or more physical items and the token associated with the user further comprises:

receiving a selection of a selected user device of a plurality of user devices presented on the mobile device, wherein the selected user device is the user device.

12. The mobile device of claim 9, wherein prior to receiving, at the first software module, the one or more identifiers associated with the one or more physical items, wherein the steps further comprise:

receiving, by the second software module, user credentials via an interface provided by the second software module;

transmitting, by the second software module, a token request comprising the user credentials to a mobile application platform, wherein the mobile application platform requests the token for the user credentials from a token service; and

receiving, by the second software module, the token from the mobile application platform.

13. The mobile device of claim 9, wherein providing, by the first software module, the API call to the second software module is based on the configuration data.

14. The mobile device of claim 9, wherein the first software module is hosted by a resource provider, and wherein the mobile device is operated by an entity different from the resource provider associated with the first software module.

15. The mobile device of claim 9, wherein the one or more identifiers include one or more barcodes and/or one or more QR codes.

16. The mobile device of claim 9, wherein the steps further comprise exchanging, between the first software module and the second software module of the mobile device, a cryptogram associated with the token.

17. A system comprising:

a remote computer; and

a mobile device comprising:

one or more processors; and

one or more memories storing computer executable instructions

that, when executed by the one or more processors, cause the mobile device to perform operations comprising:

receiving, at a first software module on the mobile device, the mobile device comprising the first software module configured to execute acceptance processing and a second software module configured to manage payment credentials and/or tokens and to emulate a user

device associated with a user, one or more identifiers associated with one or more physical items external to the mobile device, the one or more identifiers being read by the mobile device using an input component in a purchase transaction;

after step a), b) receiving, by the first software module, configuration data from a remote computer, the configuration data allowing the second software module to communicate with the remote computer via the first software module;

c) receiving, at the first software module, an indication that an authorization request is to be initiated;

d) exchanging, between the first software module and the second software module of the mobile device, interaction data associated with the one or more physical items and a token associated with the user by:

providing, by the first software module, an API call comprising the interaction data to the second software module, wherein the second software module evaluates the interaction data and the first software module and determines whether or not to respond to the API call based on a determination that the first software module is authentic and the interaction data; and

responsive to the evaluation, receiving, by the first software module, an API response comprising the token from the second software module; and

e) transmitting, by the first software module, the interaction data and the token associated with the user to the remote computer comprising acceptance processing software with which the first software module has registered in order to enable the first software module to exchange information with the remote computer, the transmitting causing the remote computer to generate an authorization request message for the purchase transaction, the authorization request message comprising the interaction data and the token.

18. The system of claim 17, wherein the remote computer further comprises:
one or more processors; and
one or more memories storing computer executable instructions that,
when executed by the one or more processors, cause the mobile device to perform
operations comprising:
providing, by the remote computer, the configuration data, wherein
the configuration data defines a set of rules associated with interaction
processing;
receiving, by the remote computer, the interaction data and the
token associated with the user from the mobile device;
generating, by the remote computer, the authorization request
message comprising the interaction data and the token; and
transmitting, by the remote computer, the authorization request
message to an authorizing entity computer to cause the authorizing entity
computer to determine whether or not to authorize an interaction.