CLAIMS

WHAT IS CLAIMED IS:

1. A system for digital payment acceptance, the system comprising:

a smart chip powered payment acceptance module, associated with a vend device, communicatively coupled to a mobile user device of a user via a near-field communications device providing a short-range communications channel, the mobile user device hosting a digital wallet application, the short-range communication channel providing communications between the mobile user device and the payment acceptance module in an online mode or an offline mode, wherein the digital wallet application is an application associated with a digital wallet linked to a user payment account provided by an issuer;

at least one processor; and

at least one computer readable medium storing computer-executable instructions, which, when executed by the at least one processor, cause the at least one processor to:

receive, from the digital wallet application, via the short-range communication channel, payment data for vending of at least one item or initiating at least one automated service associated with the vend device;

using the payment data, generate payment transaction data and send the generated payment transaction data to a merchant vending application accessible by integrated with the digital wallet application without being downloaded as a separate application and operating as a cloud-based point-of-sale (POS) terminal that provides a secure virtual Europay, Mastercard, Visa (EMV) terminal, wherein the secure virtual EMV terminal forwards the payment transaction data to an unlock service running on a cloud server, the unlock service obtaining digital secure remote payment (DSRP) credentials from an acquirer payment service provider, wherein the payment transaction data is data of a transaction to unlock the item or the automated service associated with the vend device, and

provide an unlock code to the vend device upon receiving a signed receipt generated by the unlock service based on obtaining the DSRP credentials, the unlock code indicating a completion of the payment transaction, wherein the unlock code triggers the vend device to release the item or unlock the automated service associated with the vend device.

2. The system of claim 1, wherein:

the payment acceptance module in the offline mode having a reader mode and a writer mode, in the reader mode, the payment acceptance module reads payment data from the digital wallet application, and

in the writer mode, the payment acceptance module sends the generated payment transaction data to the merchant vending application.

3. The system of claim 1, further comprising:

a public encryption key associated with a smart chip server, wherein:

the smart chip server encrypts a proof-of-payment (POP) message using the public encryption key, the POP message indicates successful completion of the payment transaction between an issuer and an acquirer, and

the POP message is included within response data received at the mobile user device from an issuer.

4. The system of claim 1, further comprising a private encryption key stored on the payment acceptance module in the offline mode, wherein the payment acceptance module decrypts a POP message using the private encryption key.

5. The system of claim 1, wherein the vend device is a micro-mobility rental device including the payment acceptance module.

6. The system of claim 1, wherein the at least one processor is further caused to:

create a payment session for the payment transaction associated with the vend device in the online mode, the payment session comprising a session identifier (ID);

redirect the user to a merchant webpage viewable from within the digital wallet application, thereby enabling the user to select service options associated with the payment transaction available from a merchant;

trigger a digital secure remote payment (DSRP) request to an issuer application; and

perform customer device cardholder verification method (CDCVM) biometric authentication of the user to authorize payment via the digital wallet application.

7. The system of claim 1, wherein the at least one processor is further caused to present a portion of a merchant webpage within a lightbox displayed in a window by the digital wallet application on the mobile user device, wherein a user selects transaction parameters using functionality provided by the portion of the merchant webpage.

8. A computerized method for digital payment acceptance comprising:

receiving from a digital wallet application, by a smart chip powered payment acceptance module associated with a vend device, via a short-range communication channel, payment data for vending of at least one item or initiating at least one service associated with the vend device, the digital wallet application being an application associated with a digital wallet linked to a user payment account provided by an issuer and being hosted by a mobile user device, the short-range communication channel providing communications between the mobile user device and the payment acceptance module, in an online mode or an offline mode;

using the payment data, generating, by the payment acceptance module, payment transaction data;

sending, via a short-range communication channel, the generated payment transaction data to a merchant vending application integrated with the digital wallet application without being downloaded as a separate application and operating as a cloud-based point-of-sale (POS) terminal that provides a secure virtual Europay, Mastercard, Visa (EMV) terminal, wherein the secure virtual EMV terminal forwards the payment transaction data to an unlock service running on a cloud server, the unlock service obtaining digital secure remote payment (DSRP) credentials from an acquirer payment service provider, wherein; the payment transaction data is data of a transaction to unlock the item or the service associated with the vend device and,

providing an unlock code to the vend device upon receiving a signed receipt generated by the unlock service based on obtaining the DSRP credentials, the unlock code indicating a completion of the payment transaction, wherein the unlock code triggers the vend device to release the item or unlock the service associated with the vend device.

9. The method of claim 8 wherein the payment transaction is a transaction to unlock the item or service associated with the vend device; and the method further comprises transmitting an unlock code to the mobile user device or a merchant server upon receiving a signed receipt generated by an unlock service indicating completion of the payment transaction, the unlock code causing the vend device to release the at least one item or unlock the at least one service associated with the vend device when the unlock code is provided to the vend device.

10. The method of claim 8, further comprising reading, by the payment acceptance module, payment data from a digital wallet application associated with a mobile user device communicatively coupled to the payment acceptance module in response to the payment acceptance module being in a reader mode.

11. The method of claim 8, further comprising displaying a portion of a merchant webpage within a lightbox displayed in a window by the digital wallet application on

the mobile user device, wherein a user selects transaction parameters using functionality provided by the portion of the merchant webpage.

12. The method of claim 8, further comprising:

creating a payment session for the payment transaction associated with the vend device in an online mode, the payment session comprising a session identifier (ID);

redirecting a user to a merchant webpage viewable from within a digital wallet application, thereby enabling the user to select service options associated with the payment transaction available from a merchant;

triggering a digital secure remote payment (DSRP) request to an issuer application; and

performing customer device cardholder verification method (CDCVM) biometric authentication of the user to authorize payment via the digital wallet application.

13. The method of claim 8, further comprising:

calculating a total transaction amount for a given transaction;

dividing the total transaction amount into two or more partial payments; and

performing two or more separate digital payment transactions associated with two or more mobile user devices to obtain the total transaction amount from two or more different users.

14. One or more non-transitory computer storage devices having computer-executable instructions for digital payment acceptance that, upon execution by a processor, cause the processor to at least:

receive from a digital wallet application, by a smart chip powered payment acceptance module associated with a vend device, via a short-range communication channel, payment data for vending of at least one item or initiating at least one service

from the vend device, the digital wallet application being an application associated with a digital wallet linked to a user payment account provided by an issuer and being hosted by a mobile user device, the short-range communication channel providing a short-range communication between a payment acceptance module of the vend device and the mobile user device;

using the payment data, generate payment transaction data and send the generated payment transaction data to a merchant vending application integrated with the digital wallet application without being downloaded as a separate application and operating as a cloud-based point-of-sale (POS) terminal that provides a secure virtual Europay, Mastercard, Visa (EMV) terminal, wherein the secure virtual EMV terminal forwards the payment transaction data to an unlock service running on a cloud server, the unlock service obtaining digital secure remote payment (DSRP) credentials from an acquirer payment service provider, wherein

the payment transaction data is data of a transaction to unlock the item or the service associated with the vend device, and

provide an unlock code to the vend device upon receiving a signed receipt generated by the unlock service based on obtaining the DSRP credentials, the unlock code indicating a completion of the payment transaction, wherein the unlock code triggers the vend device to release the item or unlock an automated service associated with the vend device.

15. The one or more computer storage devices of claim 14, wherein the DSRP credentials indicate completion of the payment transaction, including a signed receipt generated by the unlock service indicating successful completion of the payment transaction between an issuer and an acquirer.

16. The one or more computer storage devices of claim 14, wherein the computer-executable instructions, upon execution by a processor, further cause the processor to at least read payment data from a digital wallet application associated with a mobile

user device communicatively coupled to the payment acceptance module in response to the payment acceptance module being in reader mode.

17. The one or more computer storage devices of claim 15, wherein the payment acceptance module having a reader mode and a writer mode,

in the reader mode, the payment acceptance module reads payment data from the digital wallet application, and

in the writer mode, the payment acceptance module sends the generated payment transaction data to the merchant vending application.

18. The one or more computer storage devices of claim 17, wherein the vend device is a micro-mobility rental device including the payment acceptance module.

19. The one or more computer storage devices of claim 14 further comprising a private encryption key stored on the payment acceptance module in an offline mode, wherein the payment acceptance module decrypts a POP message using the private encryption key.

20. The one or more computer storage devices of claim 14, wherein the processor is further caused to present a portion of a merchant webpage within a lightbox displayed in a window by the digital wallet application on the mobile user device, wherein a user selects transaction parameters using functionality provided by the portion of the merchant webpage.