THE INVENTION CLAIMED IS

1. A computer-implemented method for conducting a secure payment transaction for a purchase at a merchant premises of a merchant using a client device and a remote point-of-sale (POS) system associated with the merchant that is external to the merchant premises, the client device comprising a smart shopping cart system and a mobile device including an account identifier associated with an issuer institution and at least one issuer a key, used for authentication in a Card-Present transaction, which is provisioned by and corresponding to the issuer institution, the method further comprising:

pairing, via near-field communication (NFC) the smart shopping cart system with the mobile device, the smart shopping cart system comprising at least one input device and at least one processor;

scanning, with the at least one input device, a data source associated with at least one product to be purchased;

determining, with the client device, at least one identifier for the at least one product to be purchased from the data source, each of the at least one product associated with a transaction value;

detecting a checkout action with the client device when the client device passes through a sensor while exiting the merchant premises to initiate the secure payment transaction;

in response to detecting the checkout action, generating, with the client device, at least one transaction message based at least partially on the transaction value of each of the at least one product to be purchased and the account identifier;

generating, with the client device, a cryptogram based at least partially on the at least one transaction message and the at least one issuer key by digitally signing the at least one transaction message with the at least one issuer key;

transmitting, with the client device, the cryptogram to the remote POS system associated with the merchant for transfer to the issuer institution by way of a transaction server;

verifying, at the issuer institution, the secure payment transaction by generating a second cryptogram based on the at least one transaction message and the at least one issuer key corresponding to the account identifier and matching the second cryptogram to the first cryptogram; and

sending, to the remote POS system, an approval of the secure payment transaction to cause deactivation of a security device on the at least one product to prevent activation of a security alarm when the client device exits the merchant premises.

2. The computer-implemented method of claim 1, wherein the remote POS system comprises a virtual POS system hosted in a network environment.

3. The computer-implemented method of claim 1, wherein each of the at least one issuer key comprises at least one of a symmetric secret key and an asymmetric secret key.

4. The computer-implemented method of claim 1, wherein the client device further comprises a merchant application and an electronic wallet application, wherein the merchant application receives the at least one identifier for the at least one product to be purchased and detects the checkout action with the client device, and wherein the electronic wallet application generates the at least one transaction message and generates the cryptogram, the method further comprising sending, with the merchant application, an initial transaction message to the electronic wallet application, wherein the at least one transaction message is generated based at least partially on the initial transaction message.

5. A system for conducting a secure payment transaction for a purchase at a merchant premises of a merchant using a client device and a remote point-of-sale (POS) system associated with the merchant that is external to the merchant premises, the client device comprising an account identifier associated with an issuer institution and at least one issuer key used for authentication in a Card-Present transaction, which is provisioned by and corresponding to the one issuer institution, the system comprising:

a client device comprising a mobile device and a smart shopping cart system, the client device configured to:

pair, via near-field communication (NFC), the smart shopping cart system with the mobile device, the smart shopping cart system comprising at least one input device and at least one processor;

scan, with the at least one input device, a data source associated with at least one product to be purchased;

determine, with the client device, at least one identifier for the at least one product to be purchased from the data source, each of the at least one product associated with a transaction value;

detect a checkout action; when the client device passes through a sensor while exiting the merchant premises to initiate the secure payment transaction;

in response to detecting the checkout action, generate, with the mobile device, at least one transaction message based on the transaction value of each of the at least one product to be purchased and the account identifier;

generate, with the mobile device, a cryptogram based at least partially on the at least one transaction message and the at least one issuer key by digitally signing the at least one transaction message with the at least one issuer key; and

transmit the cryptogram to the remote POS system associated with the merchant for transfer to the issuer institution by way of a transaction server;

an issuer system associated with the issuer institution and comprising an issuer server, the issuer system configured to verify the secure payment transaction by generating a second cryptogram based on the at least one transaction message and the at least one issuer key corresponding to the account identifier and matching the second cryptogram to the first cryptogram; and

a security device adapted to be arranged on the at least one product, the security device configured to be deactivated in response to approval of the secure payment transaction to prevent activation of a security alarm when the client device exits the merchant premises.

6. The system of claim 5, wherein the remote POS system comprises a virtual POS system unique to the merchant hosted in a network environment.

7. The system of claim 5, wherein each of the at least one issuer key comprises at least one of a symmetric secret key and an asymmetric secret key.

8. The system of claim 5, wherein the client device further comprises a merchant application and an electronic wallet application, wherein the merchant application receives the at least one identifier for the at least one product to be purchased and detects the checkout action with the client device, and wherein the electronic wallet application generates the at least one transaction message and generates the cryptogram, and wherein the client device is further configured to transmit, with the merchant application, an initial transaction message to the electronic wallet application, the at least one transaction message based at least partially on the initial transaction message.

9. At least one non-transitory computer-readable medium for conducting a secure payment transaction for a purchase at a merchant premises of a merchant using a client device and a remote point-of-sale (POS) system associated with the merchant that is external to the merchant premises, the client device comprising an account identifier associated with an issuer institution and at least one issuer key, used for authentication in a Card-Present transaction, which is provisioned by and corresponding to the issuer institution, the at least one non-transitory computer-readable medium comprising program instructions that, when executed by at least one processor of the client device, perform operations comprising:

pairing, via near-field communication (NFC) by the at least one processor of the client device comprising a smart shopping cart system and a mobile device, the smart shopping cart system with the mobile device, the smart shopping cart system comprising at least one input device;

scanning, with the at least one input device, a data source associated with at least one product to be purchased;

determining, with the client device, at least one identifier for the at least one product to be purchased from the data source, each of the at least one product associated with a transaction value;

detecting a checkout action when the client device passes through a sensor while exiting the merchant premises to initiate the secure payment transaction;

in response to detecting the checkout action, generating, with the mobile device, at least one transaction message based on the transaction value of each of the at least one product to be purchased and the account identifier;

generating, with the mobile device, a cryptogram based at least partially on the at least one transaction message and the at least one issuer key by digitally signing the at least one transaction message with the at least one issuer key;

transmitting the cryptogram to the remote POS system associated with the merchant;

verifying, at the issuer institution, the secure payment transaction by generating a second cryptogram based on the at least one transaction message and the at least one issuer key corresponding to the account identifier and matching the second cryptogram to the first cryptogram; and

sending, to the remote POS system, an approval of the secure payment transaction to cause deactivation of a security device on the at least one product to prevent activation of a security alarm when the client device exits the merchant premises.