Claims

1. A customer electronic device authenticating a customer in connection with an offline contactless payment transaction, the customer electronic device comprising:

a biometric sensor;

an operating system including an authentication module and a cryptography module;

a mobile application installed at the customer electronic device, the mobile application including a verification module and an access module, the verification module and the access module in communication with the cryptography module of the operating system; and

a local database accessible by the operating system and the mobile application, the local database including a transaction personal identification number (PIN) in an encrypted form and a registered customer identifier input; wherein the customer electronic device is configured to during an offline contactless payment transaction between the customer electronic device and a merchant terminal, wherein the merchant terminal is offline, to:

receive, by the authentication module of the operating system, from the biometric sensor, a customer identifier input, the customer identifier input including a biometric of a customer associated with the customer electronic device, the biometric including at least one of: a fingerprint, a facial recognition, an iris recognition, a voice recognition, and a gesture;

authenticate, by the operating system, the customer based on a comparison of the received customer identifier input and the registered customer identifier input in the local database;

in response to a successful authentication of the customer, derive, by the cryptography module of the operating system, a cipher from a key generated by the operating system and provide the cipher to the verification module;

receive, by the verification module of the mobile application, the cipher from the operating system;

in response to receiving the cipher at the verification module, provide, by the access module of the mobile application, to the cryptography module of the operating system, an instruction to decrypt the transaction PIN;

in response to the instruction provided by the access module of the mobile application, retrieve, by the cryptography module of the operating system, the transaction PIN from the local database, initialize, by the cryptography module of the operating system, the cipher in the customer electronic device using the key generated by the operating system, and decrypt, by the cryptography module of the operating system, the transaction PIN based on the initialized cipher;

receive, by the access module of the mobile application, from the cryptography module of the operating system, the transaction PIN once decrypted;

access, by the access module of the mobile application, a payment token stored in the local database based on the transaction PIN, the payment token associated with payment account details for processing the offline contactless payment transaction to a payment account of the customer; and

transmit the payment token to a payment network, wherein the payment token is indicative of an offline authentication of the customer, within the customer electronic device and independent of the merchant terminal, thereby enabling processing of the offline contactless payment transaction.

2. The customer electronic device of claim 1, wherein the mobile application further includes a registration module and a communication module;

wherein the registration module is configured to:

receive a registration request from the customer to register the mobile application for use in authenticating the offline contactless payment transaction; and

instruct the operating system to generate the key;

wherein the verification module is further configured to instruct the operating system to authenticate the customer to verify the registration request; and

wherein the communication module is configured to:

transmit a result of the registration request to an account server associated with a payment account used in the offline contactless payment transaction; and

receive the transaction PIN from the account server, the transaction PIN associated with authenticating the offline contactless payment transaction.

3. The customer electronic device of claim 2, wherein the key is a symmetric key; and, wherein, in response to an instruction from the registration module, the operating system is further configured to:

derive the cipher using the symmetric key;

encrypt the transaction PIN using the cipher; and

store the transaction PIN in encrypted form in the local database.

4. The customer electronic device of claim 2, wherein the key is an asymmetric key pair and the asymmetric key pair comprises a private key and a public key;

wherein the communication module is further configured to

transmit the public key to the account server for use by the account server to encrypt the transaction PIN, wherein the transaction PIN is received in an encrypted form; and

wherein the registration module is further configured to

store the transaction PIN in encrypted form in the local database.

5. The customer electronic device of claim 1, wherein the verification module is further configured to:

prompt the customer for the customer identifier input for authentication when the mobile application is initialised; and

prompt the operating system to receive the customer identifier input from the customer.

6. The customer electronic device of claim 1, wherein the verification module is further configured to instruct the operating system to prompt the customer for a customer identifier input for authentication.

7. A computer-implemented method for authenticating a customer in connection with an offline contactless payment transaction between a customer electronic device and an offline merchant terminal, the method comprising:

receiving, by an authentication module of an operating system of the customer electronic device, from a biometric sensor of the customer electronic device, a biometric of a customer associated with the customer electronic device, the biometric including at least one of: a fingerprint, a facial recognition, an iris recognition, a voice recognition, and a gesture;

authenticating, by the operating system, the customer based on a comparison of the received biometric and a reference biometric stored in a local database of the customer electronic device;

in response to a successful authentication of the customer, deriving, by a cryptography module of the operating system, a cipher from a key generated by the operating system and providing the cipher to a verification module of a mobile application implemented on the customer electronic device;

receiving, by the verification module of the mobile application, the cipher from the operating system;

in response to receiving the cipher at the verification module, providing, by the application, by an access module of the mobile application, an instruction to the cryptography module of the operating system to decrypt a transaction personal identification number (PIN) using the cipher, the transaction PIN stored in the local database of the customer device in an encrypted form;

retrieving, by the cryptography module of the operating system, the transaction PIN from the local database, initializing, by the cryptography module of the operating system, the cipher with the key, and decrypting, by the cryptography module of the operating system, the transaction PIN based on the initialized cipher;

receiving, by the access module of the mobile application, from the cryptography module of the operating system, the transaction PIN as retrieved and decrypted by the cryptography module of the operating system;

accessing, by the access module of the mobile application, a payment token stored in the local database based on the transaction PIN, the payment token associated with payment account details for processing the offline contactless payment transaction to a payment account; and

transmitting the payment token to a payment network, wherein the payment token is indicative of an offline authentication of the customer, within the customer electronic device and independent of the merchant terminal, thereby enabling processing of the offline contactless payment transaction.

8. The method of claim 7, further comprising:

receiving a registration request from the customer to register the mobile application for use in authenticating the customer in connection with the offline contactless payment transaction;

instructing the operating system to generate the key;

instructing the operating system to authenticate the customer to verify the registration request;

transmitting a result of the registration request to an account server associated with the payment account used in the offline contactless payment transaction; and

receiving the transaction PIN from the account server, the transaction PIN associated with authenticating the customer in connection with the offline contactless payment transaction.

9. The method of claim 8, wherein the key is a symmetric key; and wherein the method further comprises:

deriving, by the operating system, the cipher using the symmetric key; encrypting, by the operating system, the transaction PIN using the cipher; and

storing, by the operating system, the transaction PIN in encrypted form in the local database.

10. The method of claim 8, wherein the key is an asymmetric key pair and the asymmetric key pair comprises a private key and a public key; wherein the method further comprises:

transmitting the public key to the account server for use by the account server to encrypt the transaction PIN, wherein the transaction PIN received from the account server is the transaction PIN in encrypted form; and

storing the transaction PIN in encrypted form in the local database.

11. The method of claim 9, further comprising salting the transaction PIN by the account server if the transaction PIN is determined by the customer.

12. The method of claim 9, wherein the transaction PIN is randomly generated by the account server.

13. The method of claim 8, wherein the key is stored in a trusted execution environment (TEE) of the operating system.

14. The method of claim 7, further comprising:

prompting, by the mobile application, the customer for the biometric for authentication when the mobile application is initialised; and

prompting the operating system to receive, from the biometric sensor, the biometric from the customer.

15. The method of claim 8, further comprising:

instructing the operating system to prompt the customer for the biometric for authentication.