

Claims

1. ~~A customer electronic device~~ ~~An application system for authenticating a customer in connection with an offline contactless payment transaction, the customer electronic device application system 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 ~~a verification module 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, ~~from an operating system~~ by the verification module of the mobile application, a the cipher from the operating system;

~~_____~~ if a customer is authenticated;

~~_____~~ 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—~~an access module configured to:~~

~~instruct the operating system to use the cipher to decrypt a transaction personal identification number (PIN) which is stored in a local database in an encrypted form;~~

~~receive the transaction PIN once decrypted; and~~

~~use the transaction PIN to access a token, the token being associated with payment details for processing the payment transaction.~~

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

wherein the ~~a~~ registration module is configured to:

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

instruct the operating system to generate ~~a~~ 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 ~~application system further comprises a communication module, the communication module is configured to:~~

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

receive the transaction PIN ~~a code~~ from the account server, the transaction PIN ~~code being~~ associated with authenticating the offline contactless payment transaction.

3. The customer electronic device ~~application system~~ of claim 2, wherein the key is a symmetric key; and, wherein, in response to an instruction from ~~the code received from the~~

~~account server is the transaction PIN, and the registration module, the operating system is further configured to:~~

~~instruct the operating system 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 application system 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 public key is used by the account server to encrypt the transaction PIN such that the code received from the account server is the transaction PIN in encrypted form,~~ 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~~application system of any preceding claim,~~ wherein the verification module is further configured to:

~~prompt the customer for a the customer identifier input for authentication when the system 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~~application system of any one of claims 1 to 4,~~ wherein the verification module is further configured to:

~~instruct the operating system to prompt the customer for a customer identifier input for authentication.~~

~~7. The application system of claim 5 or claim 6, wherein the customer identifier input is selected from one of the following: a biometric, a fingerprint, a facial recognition, an iris recognition, a voice recognition, a gesture, or a password.~~

87. 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;

receiving, from an operating system, a cipher if a customer is authenticated;

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 instructing the cryptography module of the operating system to use the cipher to decrypt a transaction personal identification number (PIN) using the cipher, the transaction PIN which is stored in a the local database of the customer device in an encrypted form;

receiving the transaction PIN once decrypted;

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,

using the transaction PIN to access a token 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 being associated with payment details for processing of the offline contactless payment transaction.

98. The method of claim 8-7 further comprising:

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

instructing the operating system to generate ~~a~~ 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, ~~the account server being associated with a~~ the payment account used in the offline contactless payment transaction; and

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

~~109.~~ The method of claim ~~98~~, wherein the key is a symmetric key; ~~the code received from the account server is the transaction PIN, and~~ wherein the method further comprises: ~~instructing the operating system to:~~

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

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

~~110.~~ The method of claim ~~98~~, wherein the key is an asymmetric key pair and the asymmetric key pair comprises a private key and a public key; ~~the public key is used by the account server to encrypt the transaction PIN such that the code received from the account server is the transaction PIN in encrypted form,~~ 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.

~~1211.~~ The method of claim ~~10-9~~ further comprising salting the transaction PIN by the account server if the transaction PIN is determined by the customer.

~~1312.~~ The method of claim ~~10-9~~ ~~or claim 11~~, 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 ~~any one of claims 8 to 13~~claim 7, further comprising:

~~prompting, by the mobile application, the customer for a customer identifier input~~the biometric for authentication when the ~~system~~mobile application is initialised; and

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

15. The method of ~~any one of claims 8 to 13~~claim 8 further comprising:÷

~~instructing the operating system to prompt the customer for a customer identifier input~~the biometric for authentication.

~~16. The method of any one of claims 9 to 15 wherein the key is stored in a trusted execution environment (TEE) of the operating system.~~

~~17. A computerised network for authenticating a contactless payment transaction, the computerised network comprising:~~

~~— an application system comprising:~~

~~a registration module configured to:~~

~~receive a registration request from a customer, the registration request being a request to register the application system for use in authenticating the payment transaction; and~~

~~instruct an operating system to generate a key;~~

~~a verification module configured to:~~

~~instruct the operating system to authenticate the customer to verify the registration request;~~

~~a communication module configured to:~~

~~transmit a result of the registration request; and~~

~~receive a code from the account server, the code being associated with authenticating the payment transaction; and~~

~~wherein the application system is registered, the verification module is further configured to:~~

~~receive, from the operating system, a cipher if the customer is authenticated; and~~

~~the application system further comprises an access module, the access module is configured to:~~

_____ instruct the operating system to use the cipher to decrypt a transaction personal identification number (PIN) which is stored in a local database in an encrypted form;

_____ receive the transaction PIN once decrypted; and

_____ use the transaction PIN to access a token, the token being associated with payment details for processing the payment transaction; and

_____ an account server, the account server being associated with a payment account used in the payment transaction, wherein the account server comprises:

_____ a server communication module configured to:

_____ receive the result of the registration; and

_____ transmit the code to the application system.

18. The computerised network of claim 17, wherein the key is a symmetric key, the code received from the account server is the transaction PIN, and the registration module of the application system is further configured to:

_____ instruct the operating system 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.

19. The computerised network of claim 17, wherein the key is an asymmetric key pair and the asymmetric key pair comprises a private key and a public key, the code received from the account server is the transaction PIN in encrypted form, the communication module of the application system is further configured to:

_____ transmit the public key to the account server;

the registration module of the application system is further configured to:

_____ store the transaction PIN in encrypted form in the local database; and

the account server is further configured to:

_____ receive the public key from the application system;

_____ encrypt the transaction PIN using the public key; and

_____ transmit the transaction PIN in encrypted form to the application system.

20. A non-transitory computer readable medium having stored thereon program instructions for causing at least one processor to perform the method according to any one of claims 8 to 16.