Claims

1. A computer implemented system for providing ~~a secure~~ security and authentication in a payment transaction between a customer and a merchant, the system comprising:

at least a computer processor and a data storage device, the data storage device comprising instructions ~~operative~~ that, when executed by the processor, configure the processor to:

provide, to a computing device of the merchant, a graphical user interface;

receive, from the computing device of the merchant via a computer device of an acquirer, ~~bank of the merchant~~information representing predefined parameters associated with the merchant;

receive, from the computing device of the merchant via the graphical user interface and in response to information provided in the graphical user interface by the computing device of the merchant and via the computer device of the acquirer, information including a request for generation of a merchant token associated with a merchant;

verify information associated with the merchant;

generate and transmit the merchant token to the computing device of the merchant, after verifying the information associated with the merchant;

receive, from the computing device of the merchant via the computer device of the acquirer, a payment request comprising a payment instrument associated with a customer and ~~a~~the merchant token ~~associated with a merchant~~;

de-tokenize the merchant token to identify a merchant identifier associated with the merchant;

map the merchant ~~token~~identifier with information in a database to identify the predefined parameters established by the merchant ~~for performing a merchant authorisation of the payment request~~;

validate the ~~merchant token by checking whether the predefined parameters are met for the~~ payment request~~;~~

~~approve or refuse~~ by determining that the payment request meets the predefined parameters;

approve the payment request based on the validation ~~and, if approved, transmit a payment authorisation request to~~, by:

transmitting, to a computing device of an issuer bank associated with the payment instrument of the customer, an issuer authorization request for payment;

receiving, from the computing device of the issuer bank, in response to the issuer authorization request, an issuer authorization approval; and

transmitting, to the computing device of the acquirer, information for proceeding with the secure payment transaction.

~~for issuer authorisation of the payment request; and~~

~~proceed with the secure payment transaction if the issuer authorisation is successful.~~

2. The computer implemented system as claimed in claim 1, wherein the payment instrument ~~identifies~~ includes one of a debit card, credit card, digital wallet, or virtual payment card.

3. The computer implemented system as claimed in claim 1, wherein the ~~merchant token is generated at least based on a merchant identifier and~~ data storage device comprises instructions that, when executed by the processor, configure the processor to: map the merchant identifier with information in a database to identify one or more payment channels available for the payment transaction.

4. The computer implemented system as claimed in claim 3, wherein the ~~merchant token comprises permitted values of the predefined parameters established by the merchant upon generation of the merchant token~~ one or more payment channels comprise POS (Point-Of-Sale), e-commerce, m-commerce, QR, contactless, DSRP (Digital Secure Remote Payment).

5. The computer implemented system as claimed in claim 1, wherein at least one of the predefined parameters established by the merchant includes permitted values.

~~5~~6. The computer implemented system as claimed in claim 1, wherein the predefined parameters established by the merchant comprise one or more of: maximum transaction value, transaction location, number of allowed transactions in a predefined period of time, maximum total value of transactions, permitted age of the customer for making the payment transaction, permitted countries for initiating the payment transaction.

~~6. The computer implemented system as claimed in claim 3, wherein the one or more payment channels comprise POS (Point-Of-Sale), e-commerce, m-commerce, QR, contactless, DSRP (Digital Secure Remote Payment).~~

7. The computer implemented system as claimed in claim 1, wherein the payment ~~authorisation~~ authorization request ~~by the issuer bank~~further comprises ~~checking~~ information representing customer credentials; and further wherein the data storage device comprises instructions that, when executed by the processor, configure the processor to: associated with the payment instrument with pre-registered customer details.

8. The computer implemented system as claimed in claim 7, wherein the customer credentials associated with the payment instrument comprise one or more of card number, customer

name, expiry date, CVV (Card Verification Value), PIN (Personal Identification Number), OTP (One Time Password), 3D secure PIN.

9. The computer implemented system as claimed in claim 1, ~~further comprises a tokenisation module for generation~~ wherein the data storage device comprises instructions that, when executed by the processor, configure the processor to: send to and receive information from the computing device of the merchant via the merchant token generation interface.

~~10. The computer implemented system as claimed in claim 9, wherein the tokenisation module is communicatively coupled with a merchant token generation interface provided to the merchant for requesting token generation.~~

~~11~~10. The computer implemented system as claimed in claim 1, ~~further comprising~~ wherein the merchant token is stored in a database ~~module for storing the merchant token~~.

~~12~~11. A computer implemented method for providing ~~a secure~~ security and authentication in a payment transaction between a customer and a merchant comprising the steps of:

~~receiving~~ providing a graphical user interface to a computing device of the merchant, by at least one computing device of a payment ~~request from~~ service provider comprising a computer processor configured by executing instructions stored by a data storage device;

receiving, by the at least one computing device from the computing device of the merchant via a computer device of an acquirer bank of the merchant, ~~the~~information representing predefined parameters associated with the merchant;

receiving, by the at least one computing device from the computing device of the merchant via the graphical user interface and in response to information provided in the graphical user interface by the computing device of the merchant and via the computer device of the acquirer bank of the merchant, information including a request for generation of a merchant token associated with a merchant;

verifying, by the at least one computing device, information associated with the merchant;

generating and transmitting, by the at least one computing device, the merchant token to the computing device of the merchant, after verifying the information associated with the merchant;

receiving, by the at least one computing device from the computing device of the merchant via the computer device of the acquirer bank of the merchant, a payment request comprising a payment instrument associated with a customer and ~~a~~the merchant token ~~associated with a merchant~~;

~~mapping~~ de-tokenizing, by the at least one computing device, the merchant token to identify a merchant identifier associated with the merchant;

mapping, by the at least one computing device, the merchant identifier with information in a database to identify predefined parameters established by the merchant ~~for performing a merchant authorisation of~~;

validating, by the at least one computing device, that the payment request meets the predefined parameters;

~~validating the merchant token by checking whether the predefined parameters are met for~~approving the payment request~~;~~, by the at least one computing device, by:

~~approving or refusing the payment request based on the validation and, if approved, transmitting a payment authorisation request to~~ transmitting, by the at least one computing device to a computing device of an issuer bank associated with the payment instrument of the customer ~~for~~, an issuer ~~authorisation of the payment~~authorization request~~; and~~ for payment;

receiving, by the at least one computing device from the computing device of the issuer bank, in response to the issuer authorization request, an issuer authorization approval; and

transmitting, by the at least one computing device to the computing device of the acquirer bank of the merchant, information for proceeding with the secure payment transaction ~~if the issuer authorisation is successful~~.

~~13~~12. The computer implemented method as claimed in claim ~~12~~11, ~~further comprising initiating~~ wherein the payment request ~~by the customer with the merchant~~ is initiated at one of a merchant POS terminal, a web portal or a mobile portal of the merchant.

~~14. The computer implemented method as claimed in claim 12, further comprising receiving the payment request at the acquirer bank of the merchant based on a customer payment initiation and sending the payment request to a payment network system at least including a tokenisation module.~~

~~15. The computer implemented method as claimed in claim 14, wherein the mapping of the merchant token is performed by the tokenisation module.~~

~~16. The computer implemented method as claimed in claim 12, wherein validating the merchant token further comprises comparing the predefined parameters associated with the merchant token with permitted values of the predefined parameters as established by the merchant upon generation of the merchant token.~~

13. The computer implemented method as claimed in claim 11, wherein at least one of the predefined parameters as established by the merchant includes permitted values.

~~17~~14. The computer implemented method as claimed in claim ~~12~~11, ~~wherein approving or refusing the payment request~~ further comprising:

providing, by the at least one computing device, a full approval if all the predefined parameters are met;

providing, by the at least one computing device, a partial approval if one or more of the predefined parameters require further checking by the issuer bank; and

providing, by at least one the computing device, a refusal if one or more of the predefined parameters is not met.

~~18~~15. The computer implemented method as claimed in claim ~~12~~11, ~~wherein the issuer authorisation~~further comprising:~~es~~ checking customer credentials associated with the payment instrument with pre-registered customer details by the issuer bank.

~~19~~16. The computer implemented method as claimed in claim ~~12~~11, ~~further comprising providing a~~wherein the merchant token ~~generation~~ interface ~~to the~~ includes one or more options for a merchant ~~for allowing the merchant to generate and~~ to manage the predefined parameters ~~associated with the merchant token~~.

~~20~~17. 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 12 to 19~~following:

provide, to a computing device of the merchant, a graphical user interface;

receive, from the computing device of the merchant via a computer device of an acquirer, information representing predefined parameters associated with the merchant;

receive, from the computing device of the merchant via the graphical user interface and in response to information provided in the graphical user interface by the computing device of the merchant and via the computer device of the acquirer, information including a request for generation of a merchant token associated with a merchant;

verify information associated with the merchant;~~:~~

generate and transmit the merchant token to the computing device of the merchant, after verifying the information associated with the merchant;

receive, from the computing device of the merchant via the computer device of the acquirer, a payment request comprising a payment instrument associated with a customer and the merchant token;

de-tokenize the merchant token to identify a merchant identifier associated with the merchant;

map the merchant identifier with information in a database to identify the predefined parameters established by the merchant;

validate the payment request by determining that the payment request meets the predefined parameters;

approve the payment request based on the validation, by:

transmitting, to a computing device of an issuer bank associated with the payment instrument of the customer, an issuer authorization request for payment;

receiving, from the computing device of the issuer bank, in response to the issuer authorization request, an issuer authorization approval; and

transmitting, to the computing device of the acquirer, information for proceeding with the secure payment transaction.