CLAIMS

1. A method for ~~facilitating~~ controlling data during a payment transaction to prevent fraud, the method comprising:

receiving, by a ~~server system associated with a~~ payment ~~network~~ server, a scanned machine-readable code and a transaction amount from a customer device, wherein:

a point of sale (POS) terminal generates a machine-readable code ~~comprising at least~~ by encrypting information ~~corresponding to~~ comprising a merchant ID, merchant details, and a dynamic token, ~~the machine-readable code being valid for a pre-defined duration;~~

the dynamic token is representative of a certificate validation indicating that the customer device and the POS terminal are linked based on a pair of encryption keys,

the POS terminal executes instructions changing the information encrypted within the dynamic token at pre-defined intervals resulting in generation of a new dynamic token at each given pre-defined interval,

the POS terminal displays the machine-readable code to a customer, and an application in the customer device scans the displayed machine-readable code, and

the application is associated with a default payment card of the customer, and the customer enters the transaction amount associated with the payment transaction in a field presented at an interface of the application;

sending, by the payment server ~~system~~, a notification ~~associated with~~ to a merchant device, wherein the notification includes the scanned machine-readable code and the transaction amount received from the customer device~~, to a merchant device for approval of the payment transaction~~;

receiving, by the payment server ~~system~~, a ~~merchant defined transaction code~~ purchase request from the merchant device ~~in response to receipt of~~, wherein:

the purchase request includes a~~notification at the merchant device, the~~ merchant defined transaction code ~~indicating a nature of the payment transaction;~~ and the

~~facilitating, by the server system, the payment~~ transaction amount, and

the merchant device verifies that the scanned ~~upon receipt of the merchant~~

~~defined transaction code from the merchant device.~~

~~2. The method as claimed in claim 1, wherein receiving the~~ machine-readable code ~~further comprises receiving~~ received from the payment server matches the machine-readable code ~~from an application available at~~ displayed to the customer;

~~device, wherein the application is managed~~ validating, by the payment server ~~system.~~, the purchase request; and

sending, by the payment server, a payment transaction request to an issuer server, wherein:

the payment transaction request includes the transaction amount and merchant parameters, and

after receiving the payment transaction request, the issue server completes the payment transaction by processing the payment transaction and crediting a merchant account with the transaction amount.

~~3~~2. The method as claimed in claim ~~2~~1, ~~wherein receiving the machine-readable code further comprises receiving the machine-readable code upon scanning of the machine-readable code by the customer device.~~ further comprising:

managing, by the payment server, the application; and

enabling, by the payment server, a payment option in the application.

~~4~~3. The method as claimed in claim 2, further ~~further~~ comprising~~es~~:

managing, by the payment server, a validated pair of encryption keys for linking the ~~merchant~~ POS terminal and the customer device; and ~~a certificate for validating the pair of encryption keys.~~

managing, by the payment server, a certificate for validating the pair of encryption keys.

~~5~~4. The method as claimed in claim ~~4~~3, further comprising:

validating, by the payment server, the payment transaction at the POS terminal by facilitating an interaction between the validated pair of encryption keys ~~for validation of the~~

~~payment transaction at the merchant terminal~~.

~~6. The method as claimed in claim 1, wherein the notification includes machine-readable code received from the customer device.~~

~~7. The method as claimed in claims 1 or 6, further comprising facilitating the merchant device to verify the information corresponding to the merchant and the dynamic token upon receipt of the notification by comparing the dynamic token received from the server system with the dynamic token scanned by the customer device.~~

~~8~~5. The method as claimed in claim 1, wherein the machine-readable code is a quick response (QR) code ~~displayed at the merchant terminal~~, and wherein the QR code is generated with a new pattern~~s~~ upon ~~changing~~ generating the new dynamic token at the given pre-defined interval~~s~~.

~~9~~6. The method as claimed in claim 1, wherein the merchant defined transaction code indicates the ~~nature of the~~ payment transaction to be at least one of: an authentication transaction, a purchase transaction, a refund transaction, a void transaction, and a purchase with cashback transaction.

~~10~~7. A payment server ~~system~~ for ~~facilitating~~ controlling data during a payment transaction to prevent fraud, the payment server ~~system~~ comprising:

a memory comprising stored instructions; and

a processor configured to execute the stored instruction and thereby cause the payment server ~~system~~ to ~~perform~~:

receive~~ing~~ a scanned machine-readable code and a transaction amount~~,~~ from a customer device, wherein:

a point of sale (POS) terminal generates a machine-readable code ~~comprising at least~~ by encrypting information ~~corresponding to~~ comprising a merchant ID, merchant details, and a dynamic token, ~~the machine-readable code being valid for a pre-defined duration;~~

the dynamic token is representative of a certificate validation

indicating that the customer device and the POS terminal are linked based on a pair of encryption keys,

the POS terminal executes instructions changing the information encrypted within the dynamic token at pre-defined intervals resulting in generation of a new dynamic token at each given pre-defined interval,

~~sending a notification associated with~~ the POS terminal displays the machine-readable code to a customer, and an application in the customer device scans the displayed machine-readable code, and

the application is associated with a default payment card of a customer, and the customer enters the transaction amount associated with the payment transaction in a field presented at an interface of the application;

send a notification to a merchant device, wherein the notification includes the scanned machine-readable code and the transaction amount received from the customer device~~, to a merchant device for approval of the payment transaction~~; and

receive~~ing~~ a ~~merchant defined transaction code~~ purchase request from the merchant device ~~in response to receipt of~~, wherein:

~~the notification at the merchant device, the merchant defined transaction code indicating a nature of the payment transaction; and~~

~~facilitating the payment transaction upon receipt of~~ the purchase request includes a ~~the~~ merchant defined transaction code ~~from the merchant device~~ and the transaction amount, and

the merchant device has verified that the scanned machine-readable code received from the payment server matches the machine-readable code displayed to the customer;

validate the purchase request; and

send a payment transaction request to an issuer server, wherein:

the payment transaction request includes the transaction amount and merchant parameters, and

after receiving the payment transaction request, the issue server completes the payment transaction by processing the payment transaction and crediting a merchant ~~device~~account with the transaction amount.

~~11~~8. The payment server ~~system~~ as claimed in claim ~~10~~7, wherein the payment server ~~system~~ is further caused to ~~receive~~ :

manage the ~~machine-readable code from an~~ application ~~available at the customer device,~~; and

enable a payment option in ~~wherein~~ the application ~~is managed by the server system~~.

~~12~~9. The payment server ~~system~~ as claimed in claim ~~11~~8, wherein the payment server ~~system~~ is further caused to:

manage a validated pair of encryption keys for linking the ~~merchant~~ POS terminal and the customer device; and

manage a certificate for validating the pair of encryption keys.

~~13~~10. The payment server ~~system~~ as claimed in claim ~~12~~9, wherein the payment server ~~system~~ is further caused to ~~facilitate~~:

Validate the payment transaction at the POS terminal by facilitating an interaction between the validated pair of encryption keys ~~for validation of the payment transaction at the merchant terminal~~.

~~14~~11. The payment server ~~system~~ as claimed in claim ~~10~~7, wherein the machine-readable code is a quick response (QR) code ~~displayed at the merchant terminal~~, and wherein the QR code is generated with a new pattern~~s~~ upon ~~changing~~ generating the new dynamic token at the given pre-defined interval~~s~~.

~~15. The server system as claimed in claim 14, wherein the QR code comprises a merchant ID of the merchant, merchant details of the merchant and a dynamic token representative of a pair of encryption keys and a certificate for validation of the pair of encryption keys.~~

~~16. The server system as claimed in claim 10, wherein the notification includes machine-readable code received from the customer device.~~

~~17~~12. A point of sale (POS) terminal for controlling data during a payment transaction to prevent fraud, the POS ~~merchant~~ terminal comprising:

a memory comprising stored instructions; and

a processor executing the stored instructions and thereby causing the ~~merchant~~ POS terminal to ~~perform~~:

~~displaying~~generate a machine-readable code ~~for a customer to scan~~ , wherein:

the machine-readable code ~~using an application present in~~ encrypts information comprising a merchant ID, merchant details, and a dynamic token, and

the dynamic token is representative of a certificate validation indicating that a customer device~~,~~ and the POS terminal are linked based on a pair of encryption keys;

execute instructions changing the information encrypted within the dynamic token at pre-defined intervals resulting in generation of a new dynamic token at each given pre-defined interval; and

display the machine-readable code ~~comprising information corresponding to a merchant and a dynamic token,~~ to a customer, wherein:

the machine-readable code ~~being valid for a pre-defined duration;~~is scanned by an application in the customer device,

~~receiving a notification associated with~~ the application is associated with a default payment card of the customer, and the customer enters a transaction amount associated with the payment transaction in a field presented at an interface of the application,

the customer device sends the scanned machine-readable code ~~from a server system associated with~~ and the transaction amount to a payment ~~network, wherein~~ server,

the payment server ~~system~~ sends ~~the~~a notification ~~in response to receipt of~~ that includes the scanned machine-readable code ~~at the server system~~ and the transaction amount received from the customer device to a merchant device,

the merchant device verifies that the scanned machine-readable code received from the payment server matches the machine-readable code displayed to the customer,

based on the verified match of the scanned machine-readable code and the displayed machine-readable code, the merchant device sends a purchase request including a merchant defined transaction code and the transaction amount to the payment server,

the payment server validates the purchase request and sends a payment transaction request including the transaction amount and merchant parameters to an issue server, and

the issue server completes the payment transaction by processing the payment transaction and crediting a merchant account with the transaction amount.

~~upon scanning the machine-readable code by the customer device;~~

~~receiving from an agent associated with the merchant, a merchant defined transaction code indicating a nature of a payment transaction intended at the merchant terminal; and~~

~~sending a payment transaction request associated with the payment transaction intended at the merchant terminal to the server system through a payment network for processing of the payment transaction.~~

~~18~~13. The POS ~~merchant~~ terminal as claimed in claim 12~~17~~, wherein the machine-readable code is a quick response (QR) code, and wherein the QR code is generated with a new pattern upon generating the new dynamic token at the given pre-defined interval~~the merchant terminal is further caused to generate machine-readable codes with new patterns upon changing the dynamic token at pre-defined intervals~~.

~~19. The merchant terminal as claimed in claim 17, wherein the merchant terminal is further caused to verify a customer device based on a relationship between a pair of encryption keys associated with the merchant terminal and the customer device, wherein the encryption keys are managed by the server system.~~

~~20. The merchant terminal as claimed in claim 17, wherein the machine-readable code is a QR code, and the QR code comprises a merchant ID of the merchant, merchant details of the merchant and a dynamic token representative of a pair of encryption keys and a certificate~~

~~for validation of the pair of encryption keys.~~

14. The payment server as claimed in claim 7, wherein the POS terminal verifies that the customer device scanning the machine-readable code is linked to the POS terminal on basis of a validated pair of encryption keys.

15. The payment server as claimed in claim 7, wherein the merchant defined transaction code indicates the payment transaction to be at least one of: an authentication transaction, a purchase transaction, a refund transaction, a void transaction, and a purchase with cashback transaction.

16. The POS terminal as claimed in claim 12, wherein the POS terminal is further caused to:

verify that the customer device scanning the machine-readable code is linked to the POS terminal on basis of a validated pair of encryption keys.

17. The POS terminal as claimed in claim 12, wherein the payment server manages the application, and wherein the payment server enables a payment option in the application.

18. The POS terminal as claimed in claim 16, wherein the payment server manages the validated pair of encryption keys for linking the POS terminal and the customer device, and wherein the payment server manages a certificate for validating the pair of encryption keys.

19. The POS terminal as claimed in claim 12, wherein the payment server validates the payment transaction at the POS terminal by facilitating an interaction between a validated pair of encryption keys.

20. The POS terminal as claimed in claim 12, wherein the merchant defined transaction code indicates the payment transaction to be at least one of: an authentication transaction, a purchase transaction, a refund transaction, a void transaction, and a purchase with cashback transaction.