CLAIMS

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

receiving, by a payment 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 by encrypting information comprising a merchant ID, merchant details, and a dynamic token,

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, a notification to a merchant device, wherein the notification includes the scanned machine-readable code and the transaction amount received from the customer device;

receiving, by the payment server, a purchase request from the merchant device, wherein:

the purchase request includes a merchant defined transaction code and the transaction amount, and

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

validating, by the payment server, 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.

2. The method as claimed in claim 1, further comprising:

managing, by the payment server, the application; and

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

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

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

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

4. The method as claimed in claim 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.

5. The method as claimed in claim 1, 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.

6. The method as claimed in claim 1, 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.

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

a memory comprising stored instructions; and

a processor configured to execute the stored instruction and thereby cause the

payment server to:

receive 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 by encrypting information comprising a merchant ID, merchant details, and a dynamic token,

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 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; and

receive a purchase request from the merchant device, wherein:

the purchase request includes a merchant defined transaction code 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 account with the transaction amount.

8. The payment server as claimed in claim 7, wherein the payment server is further caused to:

manage the application; and

enable a payment option in the application.

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

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

manage a certificate for validating the pair of encryption keys.

10. The payment server as claimed in claim 9, wherein the payment server is further caused to:

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

11. The payment server as claimed in claim 7, 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.

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

a memory comprising stored instructions; and

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

generate a machine-readable code, wherein:

the machine-readable code 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 to a customer, wherein:

the machine-readable code is scanned by an application in the customer device,

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 and the transaction amount to a payment server,

the payment server sends a notification that includes the scanned machine-readable code 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.

13. The POS terminal as claimed in claim 12, 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.

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.