**Your reference: 2015/1400135283X**

**Date: 02 November 2015**

**Writer's direct number: 63302748 / 63302750 (Ms Umarani)**

Patent Application No.: 10201505741R

Title of invention: Hybrid cloud architecture for financial technology application

Applicant(s): MATCHMOVE PAY PTE. LTD.

Naik Shaileshkumar Sumantrai Leow Hsueh Huah

Lord Rainiel Braganza Mangila

Shantanu Gautam

Zheng Ping

Gian Carlo Val Flores Ebao

Sunio Romeo Jr. Sanchez

Poon Ching Man

Hidalgo Paul Wilson Manaois

**SUBJECT: REPLY TO THE SEARCH REPORT AND WRITTEN OPINION**

Dear Sir/Madam,

This is pertains to filing of reply to the Search Report and Written Opinion in relation to the Patent Application filed before IPOS, bearing application number 10201505741R, filed on dated 23/07/2015. We hereinafter filing our response along with amended claims in order to satisfy our Inventive Step (Section 15 of the Patents Act), wherein other two conditions [Novelty (Section 14 of the Patents Act) and Industrial Applicability (Section 16 of the Patents Act)] for patent has been already established.

**In response to observation Box No VI of the written opinion, the Applicant submits the amended claims below:**

**Amended Description:**

1.1 Technical Field

The invention relates to making use of a dynamic validation security token for virtual card payment transactions between a user and a merchant in a merchant transaction in an online or offline transaction for the payment of goods and services. The invention relates to a secure mode of virtual card payment transaction between user and merchant through financial institutions and payment

service providers in the merchant portal using a dynamic validation security token generated online by the card issuer of the user.

1.3 Summary of the payment transaction using a dynamic validation security token invention

The present invention describes the process of getting and making use of a dynamic validation security token provided by the card service provider, payment service provider, financial institution for a more secured virtual payment transaction between the user and the merchant, compared to using a static 3 or 4 digit CVV (Card Verification Value as used by VISA)/CVC (Card Verification Code as used b MasterCard Worldwide)/CID (Unique Card Code as used by American Express)/CSC (Card Security Code as used by American Express)/(CVN as used by China UnionPay) printed on prepaid, credit or debit cards.

1.4 Objects of the payment transaction using a dynamic validation security token invention

It is the primary object of this invention to provide secured virtual payment transaction between user and merchant through the one time usage and generation of a dynamic validation security token provided by the card service provider, payment service provider, financial institution.

Another object of this invention is to provide high levels of security in virtual or internet payment transaction between the user and merchant.

Another object of this invention is to provide a secure mode of virtual payment transaction also referred to as card-not present transactions between user and merchant without multilayered One Time Password (OTP)

In response to observation Box No VII of the written opinion, the Applicant submits that all claims and description are amended and mentioned above for clarity to support the description of the invention. The ‘recipient’ in Claim 1 is amended to merchant; the ‘online portal’ cited in (iv) of Claim 1 is amended to online payment portal. The claim 4 is dependent on claim 1 and 3; claim 5 is dependent on Claim 1, 3 and 4; and Claim 7, 8, and 9 are dependent on Claim 1 and 6.

**Amended Claims:**

1. A process of secured online payment transaction by generating dynamic validation security token via. online payment portal of the user to the merchant wherein the process comprising the steps of:

user logins to the merchant system of merchant portal via Web or Mobile Browser or App Merchant and initiates the online payment for the items purchased by providing the user’s card information into merchant system of merchant portal via. user’s logins, filling up the authentication details to retrieve user’s information in online payment portal via. user logins, user requests dynamic validation security token in the online payment portal’s webpage, a request is sent by the application

system of online payment portal via secured network channel to the processing system of the online payment portal to generate a virtual dynamic validation security token on user's dashboard, after authorisation and verification by the online payment portal a Security token is generated by the processing system of online payment portal and communicated via secured network channel to the Application system of online payment portal and displayed as Dynamic validation security token on user's dashboard system of the Applicant system of online payment portal to use it directly in the submit form of the merchant system, thereafter merchant system sends a request through networks payment infrastructure to processing system of online payment portal, thereby user's online payment portal transfers online payment to merchant portaland user completes online purchase in merchant portal.

2. The process of secured online payment transaction by generating dynamic validation security token as claimed in claim 1, wherein the merchant system comprising of: merchant shopping cart's webpage, checkout form's webpage which allows to enter user's personal information along with the dynamic validation security token, submit form's webpage allows user to initiate a card not present transaction to make online payment to merchant portal for items purchased online.

3. The process of secured online payment transaction by generating dynamic validation security token as claimed in claim 1, wherein the application system loads the relevant configuration displaying user's card information in online payment portal webpage and API's of the Application system communicate and receive information with processing system of online payment portal.

4. The process of secured online payment transaction by generating dynamic validation security token as claimed in claim 1 and 3, wherein the application system loads the relevant configuration displaying user's card information in online payment portal webpage, allows API's through secured network channel to send user's request for dynamic validation security token.

5. The process of secured online payment transaction by generating dynamic validation security token as claimed in claim 1, 3 and 4, wherein Application system of online payment portal through API's receives dynamic validation security token generated by processing system of online payment portal through secured network channel and displayed on user's dashboard system.

6. The process of secured online payment transaction by generating dynamic validation security token as claimed in claim 1, wherein the process comprising of: Generate Token which receives API request from the application system of online payment portal and generates security token; and time based counter initialized to validate security token to be sent to application system of online payment

portal through secured network channel and to validate payment transaction authorized by merchant system of merchant portal to online payment portal.

7. The process of secured online payment transaction by generating dynamic validation security token as claimed in claim 1 and 6, wherein the processing system of online payment portal performs the following steps with the help of open loop channel,

i. processing system of online payment portal receives authorisation request from merchant system of merchant portal through networks payment infrastructure;

ii. processing system sends the authorisation request to online payment portal;

iii. online payment portal verifies user's card information;

iv. processing system of online payment portal validates the security token generated sent to Application system of online payment portal through secured network channel;

v. online payment portal releases online payment to merchant portal through secured network channel;

thereby processing system of online payment portal communicates through secure network channel to merchant system of merchant portal and displayed in merchant portal webpage as the transaction successful.

8. The process of secured online payment transaction by generating dynamic validation security token as claimed in claim 1 and 6, wherein the processing system of online payment portal performs the following steps with the help of closed loop channel,

i. processing system of online payment portal receives authorisation request from merchant system of merchant portal through networks payment infrastructure;

ii. processing system validates the security token generated sent to Application system of online payment portal through secured network channel;

iii. online payment portal makes online payment to merchant portal through secured network channel;

thereby processing system of online payment portal communicates through secure network channel to merchant system of merchant portal and displayed in merchant portal webpage as transaction successful.

9. The process of secured online payment transaction by generating dynamic validation security token as claimed in claim 1 and 6, wherein the processing system of online payment portal does the following: when Dynamic validation security token has expired / doesn't match the token (if any) associated with the card at that point in time; validation conditions are not met; authorisation request

is rejected; thereby processing system of online payment portal communicates through secured network channel to merchant system of merchant portal and displayed in merchant portal webpage as transaction failure.