Title

Payment transaction using a dynamic validation security token

1. Description of the payment transaction using a dynamic validation security token invention

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 recipient 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 recipient 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.

1.2 Background of the payment transaction using a dynamic validation security token invention

There is a rapid and significant increase in online transactions between the user and the merchant portals worldwide as witnessed by the explosive growth of online internet ecommerce/merchant portals such as Amazon.com in USA and Taobao in China. The user logs into the merchant portal to buy certain items and makes online payments through the payment service provider, card service provider or the financial institutions. During payment transaction, the user first logs at the merchant portal and after entering his personal information, he logs to the payment portal, where the user is able to retrieve virtual card information and also request the generation of a dynamic validation security token to enter in the merchant checkout form and initiate a transaction. Some of the payment service providers, card service providers, financial institutions provide two step verification for online payment transaction. Card not present transactions or online transactions have inherent risks and there is an increase in fraud rate related to credit or debit cards for online transactions. Traditionally to counter fraud, an OTP (One Time Password) is required to authenticate the transaction. OTPs traditionally have an issue with delivery failures due to network coverage. Besides OTP also have an associated cost on SMS delivery, absorbed by the card issuers. Therefore there is a need for a more secured online payment transactions with or without the use of an OTP, which is more reliable and economical compared to the present OTP for online transactions. Further there is a need of secured user friendly payment transactions between the user, merchant portal, payment service provider and the financial institutions.

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 recipient, 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 recipient 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 recipient.

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 recipient without multi-layered One Time Password (OTP).

Another object of this invention is to provide a secure online payment transaction which is reliable and economical compared to the present OTP required online payment transactions.

Another object of this invention is to provide user friendly payment transactions between the user, merchant portal, payment service provider and the financial institutions.

Another object of this invention is to provide one time generation (dynamic) and one time usage of the CVV/CID/CVC/CSC/CVN for each transaction with a time limit (for example, 10 minutes set for one transaction and user will need to re-generate a new security token as the original has expired).

1.5 Brief Description of Accompanied Drawings of the payment transaction using a dynamic validation security token invention

The present invention will be described in more detail hereinafter with the aid of the description which relates to preferred embodiments of the invention explained with reference to the accompanying schematic drawings, in which:

The most illustrative drawing is Figure 1. Figure 1 explains the payment transaction through the use of a dynamic validation security token invention.

In Figure 1 the user logins the merchant portal webpage through Web/Mobile Browser/App Merchant (1). The merchant system (17) of merchant portal webpage / application consists of information of merchant portal, links for the goods selected through Merchant Shopping Cart (2), Checkout form (2) webpage/ application allows user to enter his personal information, card information comprising of Card number, Name on card, Expiry date and the Security token in the respective fields of the webpage, Submit Form (12) allows users to initiate a card not present transaction for making online payment to merchant portal for the goods selected through Merchant Shopping Cart (2). The card service provider/online payment service provider/financial institution portal hereinafter referred to as online payment portal. The user logins the web/mobile browser/app merchant webpage for virtual payment transaction (4) and enters the Application system (18) of online payment portal webpage. After authentication(5) with his credentials for the online payment portal, he is able to access information necessary to complete a card not present transaction, User enter Card Details (6), and initiate a request to generate a Dynamic Validation Security Token (7). The Application System (18) of online payment portal sends the request to the Processing System (19) of online payment portal through secured network channel (8). The Processing System (19) of the payment portal which generates the Dynamic validation security token for user transaction request contains Generate Token (9), Initiate countdown (10) and communicates the Dynamic validation security token through secured network channel (11) back to the Application system (18) of online payment portal. The authorisation request from merchant system (17) of merchant portal is communicated via secured network channel (13) to the Processing System (19) of online payment portal. The Validate Transaction (14) and Expire Token (16) of Application system (18) of payment portal is based on outcome of the transaction. The success or failure of online payment transaction processed by the Processing System (19) of online payment portal is communicated through secured network channel (15) to the merchant system (17) of merchant portal.

1.6 Detailed Description of the Preferred Embodiment of the payment transaction using a dynamic validation security token invention

The most illustrative drawing is Figure 1. Figure 1 explains the online payment transaction through the use of a dynamic validation security token invention.

The user logins the merchant system of merchant portal webpage through Web/Mobile Browser/ App Merchant (1) and decides to purchase goods through online shopping. The user selects the items to be purchased in Merchant Shopping Cart (2) webpage of merchant system and selects the Checkout form (3) webpage of merchant system and fills user's personal information, delivery address in the respective fields. Further user is required to enter user's

card information like Name on card, Card number, Card expiry date and online security password in the respective fields of Checkout form (3) webpage of the merchant system.

The card service provider/online payment service provider/financial institution portal hereinafter referred to as online payment portal. The user then logins to the online payment portal webpage through Web/Mobile Browser/App (4) by a secured network channel. The user enters information related to authentication (5), and is able to access Card Details (6) along with expiry date, Name on Card and Billing information in the online payment portal webpage. The user clicks on 'Get dynamic validation security token'(7) button displayed in online payment portal webpage. The Application system (18) of online payment portal loads the relevant configurations and initiates an API request to the processing system of online payment portal through secure network channel (8) with a request of dynamic validation security token generation(9). The processing system (19) of online payment portal on receiving the API request (8), checks if there are any active security tokens associated with the card number and validates the same. After checking, a new security token is generated and associated with the card (9) and a subsequent counter is initialized (10) with pre-set duration to validate the security token. This security token generated (9) is communicated through secure network channel (11) to the application system (18) of online payment portal and displayed as Dynamic validation security token on user's dashboard system. This Dynamic validation security token is entered in the checkout form where the 3 or 4 digit CVV/CSC/CID is required and transaction is initiated by clicking the Submit Form (12) webpage of the merchant system (17) of merchant portal.

The processing system (19) of the online payment portal is ready to receive, process and authorize transactions either by open loop or closed loop payment channels from merchant system (17) of merchant portal via networks payment infrastructure (13). In open loop transactions the authorisation request is routed via networks payment infrastructure (13) to processing system (19) of online payment portal and the processing system (19) of online payment sends the authorisation request to online payment portal. Upon receiving the authorisation request, the online payment portal verifies the user's card information like Name on card, Card number, Card expiry date, Address, Account Balance, etc. and validates back to the processing system (19) of online payment portal. In closed loop transactions authorisation process request is directly sent from merchant system (17) of merchant portal via the networks payment infrastructure (13) to processing system (19) of online payment portal. To validate (14) the security token, the processing system (19) of online payment portal checks if there is any active security token associated with the card number used in the transaction. In case of active security token present, if the rest of the transaction is validated, the active security token is used to authorize the transaction , and the authorisation request is complete. The required amount is deducted from online payment portal of the user and paid to the merchant portal. The processing system (19) of online payment portal communicates through secured network channel (15) to the merchant system (17) of merchant portal and displayed in merchant portal webpage as transaction successful and user has successfully made online

payment transaction for his online purchase in the merchant portal. After the transaction the security token expires (16).

In case the active token is expired then validation conditions are not met, the authorisation request is rejected then the processing system (19) of online payment portal communicates through secured network channel (15) to the merchant system (17) of merchant portal and displayed in merchant portal webpage as transaction failure and user has to initiate new request for a dynamic validation security token to the online payment portal for online [payment transaction.

While the present invention has been described in connection with the preferred embodiments of the various figures, it is to be understood that other similar embodiments may be used or modifications or additions may be made to the described embodiment for performing the same function of the present invention without deviating there from. Therefore, the present invention should not be limited to any single embodiment, but rather construed in breadth and scope in accordance with the recitation of the appended claims.

2. Claims of the payment transaction using a dynamic validation security token invention

We claim:

2.1 A process of secured online payment transaction by online payment portal of the user to the recipient wherein the process does the following:

i. the 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 entering the user's card information in the merchant system of merchant portal webpage;
ii. the user logins the application system of online payment portal webpage by secured network via Web or Mobile Browser or App and fills the authentication information to retrieve user's card information;
iii. the user clicks the 'Get dynamic validation security token' displayed in the webpage;
iv a request is sent by the application system of online portal via secured network channel to the processing system of the online payment portal;
v. 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;
vi. the Security Token displayed as Dynamic validation security token on user's dashboard system of the Applicant system of online payment portal;
vii. the user enters the Dynamic validation security token in the Submit Form of the merchant system webpage;
viii. authorisation request from the merchant system is communicated through networks payment infrastructure to processing system of online payment portal;
ix. after authorisation and verification by the online payment portal.

thereby user's online payment portal releases online payment to merchant portal and user completes online purchase in merchant portal.

2.2 The merchant system of merchant portal as claimed in the process of Claim 2.1 comprising of Merchant Shopping Cart's webpage wherein the items are selected by the user to be purchased; Checkout form's webpage allows user to fill user's personal information including virtual card information along with the Dynamic 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.

2.3 The Application system of online payment portal as claimed in the process of Claim 2.1 comprising of webpage to enter user's authentication; user's card information displayed in

online payment portal webpage; and relevant configurations and API's to communicate and receive information with processing system of online payment portal.

2.4 The Application system of online payment portal as claimed in the process of Claim 2.1 and 2.3 wherein Application system of online payment portal loads the relevant configurations, initiates an API request to the processing system of the online payment portal through secured network channel with a request of a dynamic validation security token generation.

2.5 The Application system of online payment portal as claimed in the process of Claim 2.1, 2.3 and 2.4 wherein Application system of online payment portal receives dynamic validation security token generated by processing system of online payment portal through secured network channel and displayed on user's dashboard system.

2.6 The processing system of online payment portal as claimed in the process of Claim 2.1 comprising of Generate Token which receives API request from 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.

2.7 The processing system of online payment portal as claimed in the process of Claim 2.1 and 2.6 wherein open loop channel of processing system of online payment portal does the following:

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.

2.8 The processing system of online payment portal as claimed in the process of Claim 2.1 and 2.6 wherein closed loop channel of processing system of online payment portal does the following:

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 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 transaction successful.

2.9. The processing system of online payment portal as claimed in the process of Claim 2.1 and 2.6 wherein 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.