PayGov India

Integration Document for Mobile Application

Contents

1. Overview

Over the past decade, there have been islands of e-Governance initiatives in the country at the National, State, District and even Block level. Government of India (GoI) perceived that if e-Governance was to be speeded up across the various arms of government at the national, state and local government level, a programme-approach would need to be adopted, which must be guided by a common vision, strategy and approach to objectives. With a view to make all Government services accessible to the common man in his locality, through common service delivery outlets and ensure efficiency, transparency & reliability of such services at affordable costs to realise the basic needs of the common man, the National e-Governance Plan (NeGP) was formulated by the GoI, for implementation across the country. NeGP envisages web-enabled anytime, anywhere access to information and services across the country, especially in rural and remote parts of India. Department of Information Technology (DIT) has envisaged common e-Governance infrastructure that will offer end-to-end transactional experience for a citizen which includes accessing various services through internet with payment gateway interface for online payments.

In this regard, NSDL Database Management Ltd (NDML) on behalf of DIT have created a common infrastructure that can be used by States/Departments to offer various services through their mobile application / WAP portals with a facility to make online payment using net banking, credit cards, debit cards and IMPS. This document lays down the procedure for registering with the payment gateway and details of the technical integration with the payment gateway.

<< This space has been intentionally left blank>>

2. Online Payment Gateway process overview

The State / Department Mobile Application will be integrated with PayGov India, the Payment gateway and with the respective Service provider or Department for the purpose of processing the service request. The online payment gateway facilities can be availed by the Citizen as well as by the Citizen Service Centers/Agents for services available at the State / Department Mobile Application.

The online transaction flow is explained as below:

1. The Citizen/Agent (customer) shall have Department's mobile application (Mobile App) installed on his handset. Customer shall open the Mobile App for submitting the online request. e.g. issue of a birth certificate, Payment of Bill. Customer shall fill the online form containing the details as required by the specific service providers [departments]. Based on the service type selected, the Mobile App shall identify the service amount that has to be paid by the customer.
2. Mobile application invokes the mobile browser and makes a call to a designated Department's Central URL [managed by Department on its server, here in after referred to as "Central URL"] passing along certain parameters like, transaction amount, etc.
3. Central URL on receiving the input parameters generates a Unique Transaction Id and creates the request message string as per PayGov India Payment Gateway transaction initiation message specifications
4. In a seamless manner this Central URL will then redirect the user to the underlying PayGov India WAP URL.
5. At the payment gateway, customer shall be displayed various payment options such as Debit Card/ Credit Card/Online Net Banking/IMPS etc. Based on the option selected, customer shall be redirected to the relevant bank/card page to make the payment. Customer shall be required to accordingly provide the relevant authentication details [i.e. User ID/ Card Number/ Password] at the bank's website; and confirm the payment amount.
6. On confirmation of the payment the Customer's account is debited and the Customer is then directed back to the designated Return URL [that was received in the transaction initiation message] within the Mobile Browser.
7. Basis this response, Department shall display an acknowledgement to the customer.

8. Payment gateway shall also generate a **unique Transaction ID** against each order number that is received – which could be displayed to the customer; and used for any queries relating to the transaction.

3. Registration Process

Every State / Department Mobile Application shall be required to be registered with Payment Gateway. Every service offered by the departments shall be registered and allotted a unique service id by the state / Department. Any payment transaction initiated from the State / Department Mobile Application should carry the Merchant id and the Service id allotted by Payment Gateway for which the payment request is initiated by citizen or Agent. The request of only registered merchant ids and service ids will be accepted by the Payment Gateway for further processing. Further, State / Department shall appoint a Nodal Agency/Officer for all interaction with NDML with respect to the payment gateway who would be focal point for all integration and payment/account settlement.

1. State/ Department shall execute an agreement with NDML for availing the payment gateway facilities.
2. Registration of State / Department Mobile Application: State / Department shall forward duly filled Registration forms to NDML for registration with the Payment Gateway. Payment Gateway shall allot a Merchant ID to the State / Department. The merchant ID should be mentioned in all online payment transactions.
3. State / Department shall provide the Bank details for crediting monies collected through payment gateway. Nodal Agency/Officer would maintain a Database of all bank accounts for all the services integrated with the payment gateway with the corresponding Department/Service in which the service fee is to be credited. This information is a pre-requisite for the integration of the payment gateway.

4. Technical Integration with Payment Gateway

Key aspects of the integration between the Mobile Application and payment gateway are described below.

4.1. Transaction Process

1. The Citizen/Agent (customer) shall have Department's mobile application (Mobile App) installed on his handset. Customer shall open the Mobile App for submitting the online request. e.g. issue of a birth certificate, Payment of Bill. Customer shall fill the online form containing the details as required by the specific service providers [departments]. Based on the service type selected, the Mobile App shall identify the service amount that has to be paid by the customer.
2. Mobile application invokes the mobile browser and makes a call to a designated Department's Central URL [managed by Department on its server, here in after referred to as "Central URL"] passing along certain parameters like, transaction amount, etc.
3. Central URL on receiving the input parameters generates a Unique Transaction Id and creates the request message string as per PayGov India Payment Gateway transaction initiation message specifications
4. In a seamless manner this Central URL will then redirect the user to the underlying PayGov India WAP URL.
5. At the payment gateway, customer shall be displayed various payment options such as Debit Card/ Credit Card/Online Net Banking/IMPS etc. Based on the option selected, customer shall be redirected to the relevant bank/card page to make the payment. Customer shall be required to accordingly provide the relevant authentication details [i.e. User ID/ Card Number/ Password] at the bank's website; and confirm the payment amount.
6. On confirmation of the payment the Customer's account is debited and the Customer is then directed back to the designated Return URL [that was received in the transaction initiation message] within the Mobile Browser.
7. Basis this response, Department shall display an acknowledgement to the customer.

Payment gateway also generates a **unique Transaction ID** against each order number that is received – this could be displayed to the customer; and used for any queries relating to the transaction.

4.2. Payment Request

- A request needs to be generated for payment gateway URL for each payment with the parameters indicated:

[Payment Gateway Request URL will be provided after setup.]

MERCHANT		
Parameter	**Sample Value**	**Description**
MerchantID	ABCD	To be provided after setup
CustomerID	123456789012	State/ Department system's Unique Order ID
TxnAmount	100.00	Transaction Amount
CurrencyType	INR	Fixed Value (max length 3)
TypeField1	R	Fixed Value (max length 1)
SecurityID	abcd	To be provided after setup
TypeField2	F	Fixed Value (max length 1)
AdditionalInfo1	XYZ	Service ID [will vary as per the service provider or department]
RU	http://www.domain.com/response.jsp	Return URL where the payment gateway response is to be received by Merchant

- **Payment Request Message description**

MerchantID|CustomerID|NA|TxnAmount|NA|NA|NA|CurrencyType|NA|TypeField1|SecurityID|NA|NA|TypeField2|AdditionalInfo1|AdditionalInfo2|AdditionalInfo3|AdditionalInfo4|AdditionalInfo5|NA|NA|RU

- **Sample message for checksum value generation**

ABCD|123456789012|NA|100.00|NA|NA|NA|INR|NA|R|abcd|NA|NA|F|123456789012|XYZ|NA|NA|NA|NA|NA|http://www.domain.com/response.jsp

Assume the checksum value generated was:
0F142D19B0720BB2F7680CDF85CFA46FDF8B698EFB9A73C04EDFDB11805619C6

- **Sample Txn Initiation Message to be sent to payment gateway URL as parameter 'msg'**
  ABCD|123456789012|NA|100.00|NA|NA|NA|INR|NA|R|abcd|NA|NA|F|123456789012|XYZ|NA|NA|NA|NA|NA|http://www.domain.com/response.jsp|0F142D19B0720BB2F7680CDF85CFA46FDF8B698EFB9A73C04EDFDB11805619C6

4.3. Payment Response

The payment response is sent to the Return URL [RU] specified dynamically by Department for each transaction. This response is a **browser** response and the message will be posted to the Return URL as a parameter - **msg**

- **Response Message description:**

  MerchantID|CustomerID|TxnReferenceNo|BankReferenceNo|TxnAmount|BankID|BankMerchantID|TxnType|CurrencyName|ItemCode|SecurityType|SecurityID|SecurityPassword|TxnDate|AuthStatus|SettlementType|AdditionalInfo1|AdditionalInfo2|AdditionalInfo3|AdditionalInfo4|AdditionalInfo5|AdditionalInfo6|AdditionalInfo7|ErrorStatus|ErrorDescription|CheckSum

- **Sample Response Message**

  ABCD|123456789012|MSBI0412001668|NA|0000100.00|SBI|22270726|NA|INR|NA|NA|NA|NA|25-12-2012 16:08:56|0300|NA|123456789012|XYZ|NA|NA|NA|NA|NA|NA|NA|53058B5321A528E90F63D614AED5641D4DE05C622D68747B0CB848600F9863E8

☐ Please note – MERCHANTID and the CHECKSUM KEY would be provided at the time of integration. Refer ANNEXURE I for a detailed description of the Checksum Key and related process.

4.4. Payment Updation process at Department's end

Department's Return URL will receive the browser response and display an acknowledgement to the customer.

Department will receive the server-to-server response and do the system updation at its end. The following process should be followed at Department's end for receiving and processing the payment response:

(a) Receive and Read the Payment Response message – msg at the Return URL

(b) Generate the 'checksum value' for the Payment Response and validate it with the 'checksum value' received in the Payment Response. If they match; proceed to step (c) below; else display a Payment Rejection message to the customer.

(c) Update the original record in the merchant system based on the 'AuthStatus' field received in the Payment Response. Refer the table below for various values that are received in the AuthStatus field, and the related Transaction Status. The updation to the original record must be done as follows:

Successful transaction [AuthStatus – 0300]

Update <record> set STATUS = 'SUCCESS' where ORIGINALSTATUS='PENDING' and ORDERNUMBER=' 1073234' and TRANSACTIONAMOUNT='2400.30'

Failure transaction [AuthStatus – other than 0300]

Update <record> set STATUS = 'FAILURE' where ORIGINALSTATUS='PENDING' and ORDERNUMBER=' 1073234' and TRANSACTIONAMOUNT='2400.30'

(d) The above updation process ensures the following:

- ☐ Only the original record is updated [through the Unique Order Number]
- ☐ The record is updated only once [for original status=PENDING]
- ☐ The record is updated for the same 'Transaction Amount' that was initiated by the merchant.

- **Authorization status**

AuthStatus	Status Reason	Proposed Transaction Status
"0300"	Success	Successful Transaction
"0399"	Invalid Authentication at Bank	Cancel Transaction
"NA"	Invalid Input in the Request Message	Cancel Transaction
"0002"	Payment Gateway is waiting for Response from Bank	Pending Transaction
"0001"	Error at Payment Gateway	Cancel Transaction

For all AuthStatus that is not a Success, an ErrorDescription would be provided in the Payment Response.

4.5. Key Points for a Successful Integration

Payment Request

No	Area	Description
1.	Secure Payment Gateway Desk URL	Always use "https" for the Payment gateway URL where the request will be posted.
2.	POST method	* Always Use "POST" method * Variables must be sent as HIDDEN values
3.	Referral URL	Always call the Payment Gateway production URL from the Referral URL only; which needs be shared at the time of integration.
4.	Length of parameters	Each parameter field should not be more than 100 characters. A 'NULL' value will not be accepted for any parameter.
5.	Special characters	The following characters are allowed in the parameters that are sent to Payment Gateway: space, hyphen, underscore, dot and @ Please note special characters by default are not enabled for the parameter values; they have to be enabled on request. Also it is important to note that not all special characters can be enabled.
6.	Transaction Amount	In the test phase of your integration, only Rs. 2 can be used as a transaction amount.

Payment Response

No	Area	Description
1.	Checksum Validation	Always validate the checksum before updating the transaction response
2.	Verify whether the updation is as per the process specified in the interface document	☐ Only the original record is updated [through the Unique Order Number] ☐ The record is updated only once [for original status=PENDING] ☐ The record is updated for the same 'Transaction Amount' that was initiated by the merchant.

5. Disputes/ Charge backs

Potentially, as per the card associations [Visa/ Mastercard] guidelines, cardholders can dispute a charge [generally within 180 days of the transaction date] that they see against their credit/debit card. The card holder would raise this dispute to the issuing bank on grounds that he/she did not do the transaction; or that the Department has not rendered the services for the specific charge.

This process is briefly described below:

1. Customer raises a dispute with the concerned bank.
2. The issuing bank would in turn raise the dispute request with the Acquiring Bank.
3. Acquiring Bank will inform Payment Gateway about the dispute request notice [Payment Gateway needs to revert to the acquiring Bank within Seven working days after receipt of this request].
4. Payment Gateway shall immediately intimate the Department of the dispute request notice along with all the relevant details of the transaction [including Department's Order number, Transaction Date, Transaction Amount, Payment Gateway Transaction Reference Number].
5. Based on this intimation, Department shall verify the dispute request based on its internal process. Department will need to provide Payment Gateway with a response within three working days with the following:

    - Success Updation Screenshot – this screenshot could be from Department's system and could indicate the details of the customer where the credit has been provided against the purchase. Payment Gateway will provide this screenshot along with the transaction details to the acquiring bank for addressing copy request/ chargeback requests.

    - Cancellation approval – in case the Department determines that this transaction can be reversed to the cardholder account; Department to initiate the refund transaction as per the process defined in Section 3 above.

6. Based on the response from the Department, Payment Gateway will respond to the Acquiring Bank about the copy request/ chargeback notice.

7. All disputes would be resolved in accordance with the rules/policies laid down by Visa/ Mastercard/ American Express/ Diners in this regard.

8. For any chargebacks that are received and debited by the acquiring bank, Payment Gateway would intimate and pass on these chargebacks to Department; and this amount will be deducted in the Merchant TID report.

ANNEXURE I – Checksum calculation

The checksum is an important part while receiving messages from Payment Gateway. When the merchant receives the response from Payment Gateway, a new checksum is generated at the merchant site to verify the received one. Any differences in the checksum imply that the messages have been modified or received erroneously.

Payment Gateway will provide a checksum component to the merchant to generate the checksum. The Checksum component will require a message string and common string, i.e. password (Payment Gateway and the merchant would share a common password to generate the checksum) to generate checksum.

msg – Checksum will be required for this message and has to be validated by the merchant.

Payment Response string

MerchantID|CustomerID|TxnReferenceNo|BankReferenceNo|TxnAmount|BankID|BankMerchantID|TxnType|CurrencyName|ItemCode|SecurityType|SecurityID|SecurityPassword|TxnDate|AuthStatus|SettlementType|AdditionalInfo1|AdditionalInfo2|AdditionalInfo3|AdditionalInfo4|AdditionalInfo5|AdditionalInfo6|AdditionalInfo7|ErrorStatus|ErrorDescription|CheckSum

Checksum will be calculated for the string -

MerchantID|CustomerID|TxnReferenceNo|BankReferenceNo|TxnAmount|BankID|BankMerchantID|TxnType|CurrencyName|ItemCode|SecurityType|SecurityID|SecurityPassword|TxnDate|AuthStatus|SettlementType|AdditionalInfo1|AdditionalInfo2|AdditionalInfo3|AdditionalInfo4|AdditionalInfo5|AdditionalInfo6|AdditionalInfo7|ErrorStatus|ErrorDescription

For example, suppose the Response message for a particular transaction is as follows:

MERCHANTID|1073234|MSBI0412001234|NA|00002400.30|SBI|22230123|NA|INR|NA|NA|NA|NA|12-12-2012
16:08:56|0300|NA|NA|NA|NA|NA|NA|NA|NA|NA|7A1007FB37E10FEE721C59436BD4BEAD93BB315FF6B55B3679222363F40BA29F

Following checksum string will be passed to checksum component with checksum key

MERCHANTID|1073234|MSBI0412001234|NA|00002400.30|SBI|22230123|NA|INR|NA|NA|NA|NA|12-12-2012 16:08:56|0300|NA|NA|NA|NA|NA|NA|NA|NA|NA|checksumkey

Calculated checksum value at the merchant end should be 3734835005 as in response message. This should be matched and then the transaction should be taken for further processing at the merchant's end.