

PayGov India

Integration Document



This document is confidential to NSDL Database Management Limited (NDML) and Department of Electronics and Information Technology (DeitY). This document contains information and data that NDML considers confidential and proprietary (“Confidential Information”). Confidential Information includes, but is not limited to, the following: Corporate, employee and infrastructure information about NSDL/ NDML, Commercial rates and values, Technology, Process, Administration and Management Information. Any disclosure of Confidential Information to, or use of it by a third party (i.e., a party other than DeitY), will be damaging to NDML. Ownership of all Confidential Information, no matter in what media it resides, remains with NDML.

Contents

1. Overview	3
2. Online Payment Gateway process overview.....	4
3. Registration Process	5
4. Technical Integration with Payment Gateway	5
4.1. <i>Transaction Process</i>	5
4.2. <i>Payment Request</i>	7
4.3. <i>Payment Response</i>	8
4.4. <i>Payment Updation process at Portal end</i>	8
4.5. <i>Key Points for a Successful Integration</i>	10
5. Settlement Process.....	11
5.1. <i>Reconciliation Process [at PayGov]</i>	11
5.2. <i>Merchant TID Report</i>	11
5.3. <i>Refunds Processing</i>	11
6. Next steps.....	13
7. Disputes/ Charge backs	13
ANNEXURE I – Checksum calculation	15

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 Electronics and Information Technology (DeitY) 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 DeitY have created a common infrastructure that can be used by Center/States/Departments to offer various services through their national / state portals with a facility to make online payment using net banking, credit cards and debit cards. This document lays down the procedure for registering with the payment gateway, overall process flow for 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 Portal will be integrated with PayGov, 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 Portals. .

The online transaction flow is explained as below:

1. The Citizen/Agent (customer) shall login to the Portal for submitting the online request. e.g. issue of a birth certificate. Customer shall fill the online form containing the details as required by the specific service providers [departments]. Based on the service type selected, the Portal shall identify the service amount that has to be paid by the customer.
2. The customer shall select the option for Online Payment at the Portal. The Portal shall generate a **Unique Order number** for each request.
3. Portal shall establish direct connection with the Payment Gateway Interface and initiate the payment request.
4. At the payment gateway, customer shall be displayed various payment options such as Debit card/ Credit card/Online net banking etc. Based on the option selected, customer shall be directed to the relevant bank page to make the payment. Customer shall be required to capture the relevant authentication details [i.e. User ID/ Card Number/ Password] at the bank's website; and confirm the payment amount.
5. On confirmation of the payment the Customer's account is debited and the Customer is then directed back to the designated Return URL [RU] at the Portal.
6. The Payment Gateway shall provide the return response to the designated Portal Return URL received in the initial transaction request. Basis this response, portal shall display an acknowledgement to the customer.
7. 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 portal 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 portal. Any payment transaction initiated from the State / Department Portal 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 Portal 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 Portal: State / Department Portal 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 Portal website and payment gateway are described below

4.1. Transaction Process

1. Customer logs-in at the merchant's 'Portal' (website).
2. Portal displays various services that the customer could use, e.g. issue of a birth certificate. The details as required by the specific service providers [departments] are to be captured by the portal.

3. The Portal will decide the specific amount that has to be paid by the customer; and the consumer clicks on 'Make Payment' at the Portal.
4. Portal now establish a connection with the Payment Gateway Interface and initiate the payment [refer the section on Payment Request in section 4.2 below]. At this point, the following key parameters will be provided by the Portal to Payment Gateway
 - a. Unique Order Number [for every request initiated by the Portal]
 - b. Transaction Amount
 - c. Merchant ID [this is unique for each State /Department Portal]
 - d. Service ID [this will be the specific service provider for whom the payment is collected]
5. Return URL [where the payment response is required]
6. At the Payment Gateway; the customer is displayed various 'payment options' that the customer can use for e.g. Credit Cards / Debit Cards / Online Net banking.
7. Customer chooses the payment option and is taken to the relevant bank page. Customer then enters the relevant authentication details [i.e. User ID/ Card Number/ Password] at the bank's website; and then is requested to confirm the payment amount.
8. Customer's account is debited and the Customer is then directed back to the designated Return URL [RU] at the Portal.
9. The Payment Gateway will provide the return response to the designated Portal Return URL received in the initial transaction request. There are two responses provided by the Payment Gateway:
 - a. Browser Response – this is provided to the Return URL through a redirection mode; and can be used by the Portal to display the status of the transaction to the customer.
 - b. Server-to-Server Response – this is provided to the Portal at a fixed Return URL through a TCP connection directly by the payment gateway to the Portal Application. This response can be used by the Portal to update its system and initiate the service delivery to the respective department.
10. 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

- After the customer clicks on PAY [within Portal website], a request needs to be generated by Portal to following payment gateway URL for each payment with the parameters indicated:

[PayGov will provide the URL as part of the integration activities]

MERCHANT		
Parameter	Sample Value	Description
MerchantID	ABCD	To be provided after setup
CustomerID	123456789012	Payment Reference ID [this is the id provided by Payment Gateway to NSDG/SSDG. If NSDG/SSDG is not applicable, then State/ Department Portal's Unique Order ID to be passed.
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	5630147521	State/ Department Portal's Unique Order ID
AdditionalInfo2	Service1	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|5630147521|Service
1|NA|NA|NA|NA|NA|http://www.domain.com/response.jsp

Assume the checksum value generated was 3712345678

- **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|5630147521|Service
1|NA|NA|NA|NA|NA|http://www.domain.com/response.jsp|3712345678

4.3. Payment Response

The payment response is sent to the Return URL [RU] specified dynamically by Portal for each transaction. This response is a **browser** response and the message will be posted to the Portal's 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|30-12-2012
16:08:56|0300|NA|5630147521|Service1|NA|NA|NA|NA|NA|NA|NA|3734835005

- 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 Portal end

Portal will receive the browser response and display an acknowledgement to the customer.

Portal will receive the server-to-server response and do the system updation at its end. The following process should be followed at Portal 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 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	<input type="checkbox"/> Only the original record is updated [through the Unique Order Number] <input type="checkbox"/> The record is updated only once [for original status=PENDING] <input type="checkbox"/> The record is updated for the same 'Transaction Amount' that was initiated by the merchant.

5. Settlement Process

5.1. Reconciliation Process [at PayGov]

- On the next working day of transactions, PayGov will reconcile the online transactions with the credits received based on the batch files received from the bank(s).
- After reconciling, PayGov will generate an MIS report – that will include the Order Number; and the Transaction ID generated by PayGov.
- This report will contain the successful transactions; and the refunds that would have been initiated by Merchant for specific transactions.
- Net amount [of PayGov Charges] will be provided to Merchant with an MIS Report [**'Merchant TID Report'**].

5.2. Merchant TID Report

The merchant will be able to login to the Merchant Interface and download a daily Merchant TID Report. This report provides a summary of:

- Settled Transactions
- Refund Transactions
- Chargeback Transactions

In addition to providing details as mentioned above, the Merchant TID Report gives an overall summary with respect to the 'Net Credit' amount.

5.3. Refunds Processing

Refunds [if any] to be identified by merchant and should be initiated with PayGov.

Refund process workflow

The following process should be followed at the merchant end for processing refunds:

- (a) Create a file in the standard format [refer format below] and provide the same to PayGov
- (b) PayGov processes the refund file on a batch basis.
- (c) Refunds that are successfully received are then processed with each of the banks as per the workflow defined with the banks.

Refund – a transaction that is already settled for the merchant. Part of the transaction amount can also be refunded by the merchant.

Cancellation – a transaction that is not settled for the merchant. Only the entire transaction amount can be cancelled by the merchant.

- (d) Refunds successfully processed will be displayed as a deduction in the next 'Merchant TID Report' that is generated for the merchant.

Format of the refund file will be as follows:

txn_id,txn_date,customer_id,txn_amount(Paise format),refund_amount(Paise format)

Field Name	Notes
txn_id	PayGov Transaction ID received in the Payment Response
txn_date	Transaction Date in YYYYMMDD format
customer_id	Will be the value set in 'txtCustomerID' in the Payment Request
txn_amount	Transaction Amount; in paise format [for e.g. 100.00 will be 10000]
refund_amount	Amount to be refunded; in paise format

For example:

MUTI0803612345,20130731,6012345,100000,100000

Sample Refund File Naming Convention: MerchantID_Refund_yyyymmddhhmmss.txt

Notes:

- File should be a .txt file
- Values should be separated with 'comma' delimiter
- The refund file must **not** contain any column headers
- All fields are mandatory in the refund file
- Refund File Name can take maximum of 50 characters without spaces

6. Next steps

- Merchant to confirm the integration process and discuss any clarifications required.
- Merchant to confirm their tech platform; parameters for the integration along with validation information.
- Merchant to confirm the Referral URL to be used for the test phase.
- Merchant to provide Nodal Bank Letter for payout related setup.
- PayGov to initiate the technical integration development at its end.
- PayGov to share the URL for testing/UAT post completion of the development.
- Merchant to provide a UAT signoff.
- Merchant to confirm their Referral URL to be setup for production phase.
- Merchant to provide Operations Contact Matrix for the process.
- PayGov to complete the go-live related setup.
- PayGov to confirm go-live readiness to merchant.
- Go live.

7. 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 Portal 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 Portal of the dispute request notice along with all the relevant details of the transaction [including Portal Order number, Transaction Date, Transaction Amount, Payment Gateway Transaction Reference Number].
5. Based on this intimation, Portal shall verify the dispute request based on its internal process. Portal will need to provide Payment Gateway with a response within three working days with the following:
 - Success Updation Screenshot – this screenshot could be from Portal 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 Portal determines that this transaction can be reversed to the cardholder account; Portal to initiate the refund transaction as per the process defined in Section 3 above.

6. Based on the response from the Portal, 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 Portal; 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|12-12-2004|16:08:56|0300|NA|NA|NA|NA|NA|NA|NA|NA|NA|NA|NA|NA|3734835005

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|12-12-2004|16:08:56|0300|NA|NA|NA|NA|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.