Payment Gateway

Integration document

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, Centre for Development of Advanced Computing ('CDAC') and NSDL Database Management Ltd (NDML) on behalf of DIT have created a common infrastructure that can be used by States to offer various services through their 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.

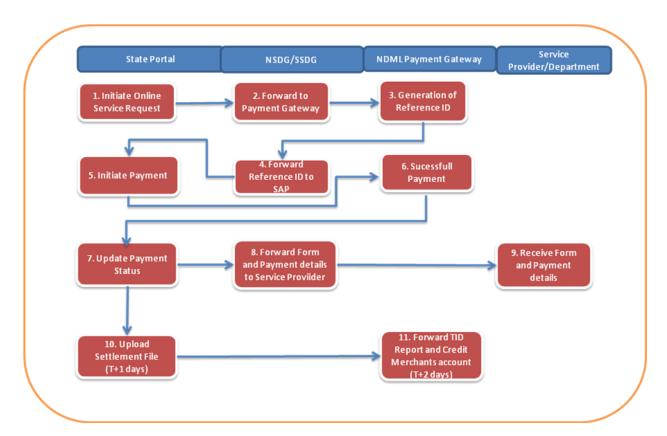## 2. State E-Governance Service Delivery Gateway

The existing Government systems are characterized by islands of legacy systems using heterogeneous platforms and technologies and spread across diverse geographical locations, in varying state of automation. The emergence of many e-governance applications of various departments to provide online services to citizens, businesses and government would require increasing interactions amongst departments and with external agencies at various levels in State Government. Departments would need to develop connectors/adaptors for point to point connections between departments creating a mesh and also tight coupling between applications. This would lead to applications difficult to maintain and upgrade in case of version change and change in government policies and business rules.

The State e-Governance Service Delivery Gateway (SSDG) is an attempt to reduce such point to point connections between departments and provide a standardized interfacing, messaging and routing switch through which various players such as departments, front-end service access providers and back-end service providers can make their applications and data inter-operable. The State e-Governance Service Delivery Gateway (SSDG) aims to achieve a high order of interoperability among autonomous and heterogeneous entities of the states based on a framework of e-Governance Standards. SSDG as a messaging middleware acts as an intelligent hub and routes service requests from a Service Seeker (Service Access Provider) to a Service Provider (typically a back end Government department that puts up its service for electronic delivery) and in return sends the response back to the Service Seeker through the Gateway.

Please refer ANNEXURE II for all documentation details for integration process with NSDG/SSDG.

3. Online Payment Gateway process overview

The State Portal will be integrated with NSDG/SSDG 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 Portals. The portal needs to be registered both with SSDG and Payment gateway for availing the online payment facilities.

Online Payment Gateway Process Flow

The process are 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 the request.

3. The Portal shall establish a TCP connection [in the background] with the NSDG/SSDG system (Refer ANNEXURE II for all documentation details for integration process with NSDG/SSDG.), which in turn initiates a request to the Payment Gateway and receives back a Reference ID from the Payment Gateway. This Payment Reference Number is provided back to the Portal by the NSDG/SSDG System.

4. Portal shall establish direct connection with the Payment Gateway Interface and initiate the payment request.

5. 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.

6. 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.

7. The Payment Gateway shall provide the return response to the designated Portal Return URL received in the initial transaction request.

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.

9. On completion of the payment process, the Portal shall forward the request details through NSDG/SSDG containing the form details, Transaction Id and payment status. This may be done through a Synchronized or Asynchronized call. The Service Provider/Department back office will send a return response through NSDG/SSDG to the Portal.

10. On the next day (T+1), Portal shall upload a Settlement File (refer 'Settlement Workflow' section below) into the Payment Gateway platform.

11. Payment Gateway processes the Settlement File on a batch basis and generates an MIS report – that will include the Order Number; and the Transaction ID generated by the Payment Gateway.

12. This report will contain the successful transactions; and the refunds that would have been initiated by Merchant for specific transactions.

13. Net amount [of charges] will be provided to Merchant with an MIS Report ['**Merchant TID Report'**].

4. Registration Process

All Registration forms for SAP and SP will be provided by the Gateway Service Provider (NSDG / SSDG) to each respective SAP and SP Owners. Every State portal (Service Access Provider – SAP) and the services offered by various departments shall be required to be registered with NSDG/SSDG as well as with Payment Gateway. NSDG/SSDG shall allot a Service Provider ID to the State Portal and Payment Gateway shall allot a unique Merchant Id on enrollment of SAP in Payment Gateway. Similarly, every service offered by the departments shall be registered and allotted a unique service id. Any payment transaction initiated from the State 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, SAP 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/SAP shall execute an agreement with NDML for availing the payment gateway facilities.
2. Registration of Service Access Provider (SAP): SAP shall forward duly filled SAP Enrollment form to NSDG/SSDG. NSDG/SSDG shall register the SAP, allot a Service Provide ID and forward the details to NDML for registration with the Payment Gateway. Payment Gateway shall allot a Merchant ID to the SAP. The merchant ID should be mentioned in all online payment transactions.

3. Registration of Service: SAP shall forward duly filled SP Service Enrolment form to NSDG/SSDG for registration of service. NSDG/SSDG shall register the service, allot a Service ID to each service and forward the details to NDML for registration of service in Payment Gateway. The service id should be mentioned in all online payment transaction.

4. State shall provide the Bank details for crediting monies collected through payment gateway. Nodal Agency/Officer would maintain a Database of all Government 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. Please Refer Annexure III.

Please refer ANNEXURE II for all documentation details for integration process with NSDG/SSDG.

5. Technical Integration with Payment Gateway

Key aspects of the integration between the Portal website and payment gateway are described below

5.1. Transaction Process

1. Customer logs-in at the 'Portal' website.

2. Portal displays the various services that the customer could use, eg. 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 paid by the customer; and the consumer clicks on 'Make Payment' at the Portal.

4. At this point, the Portal establishes a TCP connection [in the background] with the NSDG/SSDG system (Refer ANNEXURE II for all documentation details for integration process with NSDG/SSDG.), which in turn initiates a request to the payment gateway and receives back a Payment Reference Number from Payment Gateway. This Payment Reference Number is provided back to the Portal.

5. Portal will now establish a connection with the Payment Gateway Interface and initiate the payment [refer the section on Payment Request in section 4 below]. At this point, the following key parameters will be provided by the Portal to Payment Gateway
    a. Reference ID [provided by Payment Gateway through NSDG/SSDG Connector]
    b. Unique Order Number [for every request initiated by the Portal]
    c. Transaction Amount
    d. Merchant ID [this is unique for each State Portal]
    e. Service ID [this will be the specific service provider for whom the payment is collected]

6. Return URL [where the payment response is required]

7. At the Payment Gateway; the customer is displayed various 'payment options' that the customer can use for e.g. Credit Cards / Debit Cards / Online Netbanking / Cash Cards.

8. 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.

9. Customer's account is debited and the Customer is then directed back to the designated Return URL [RU] at the Portal.

10. 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.

11. 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.

5.2. 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:

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
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	2375613	SAP (State Portal) Unique Order ID/ Transaction ID
AdditionalInfo2	XYZ	Service ID [will vary as per the service provider or department]
AdditionalInfo3	NA	Fixed Value
AdditionalInfo4	NA	Fixed Value
AdditionalInfo5	NA	Fixed Value
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|2375613|XYZ|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|2375613|XYZ|NA|NA|NA|NA|NA|http://www.domain.com/response.jsp|3712345678

In addition to the 'msg' parameter, portal also needs to pass the following two parameters with fixed values

hidRequestId=PGIME1000

hidOperation=ME100

- **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|12-12-2010 16:08:56|0300|NA| 2375613|XYZ |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.

- **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	Cancel 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.

5.3. Settlement File Upload

Portal Administrator can settle transactions through the Payment Gateway Merchant Interface. The Settlement requests can be initiated through the upload of a Settlement File into the Payment Gateway Merchant Interface.

- ***Settlement - Definition***

The Portal would 'settle' those transactions where the status is successfully received by the Portal and customer has been provided the requested services. Through the 'settlement' process, Portal effectively claims monies for the successful transactions where transaction acknowledgement has been generated on the previous day.

- **Settlement process workflow**

The following process should be followed at the Portal end for settlement of transactions:

1. Portal to pick up all the records for the previous day where transaction status was SUCCESS. Previous day – should be defined based on the timestamp of the transaction provided by Payment Gateway.

2. Create a file in the standard format [refer format below] and upload into the 'Settlement File Upload' option in the Payment Gateway Merchant Interface.

3. Payment Gateway processes the uploaded settlement file on a batch basis. If there are any records in the Settlement File are found to be invalid for any reason Payment Gateway Ops would work with Portal Operations team to resolve such cases.

- **Format of the settlement file will be as follows:**

  txn_id,customer_id,txn_amount(Rs.Ps),txn_date

Field Name	Notes
txn_id	Payment Gateway Transaction ID received in the Payment Response

customer_id	Will be the value set in 'txtCustomerID' in the Payment Request
txn_amount	Transaction Amount; in Rs.Ps format [for e.g., 500.00]
txn_date	Transaction Date in YYYYMMDD format

For example:

MICI9011234567,34895634895,500.00,20090731

- **Sample Settlement File Naming Convention:** MerchantID_Settlement_yyyymmddhhmmss.txt

Notes:

1. File is to be uploaded as a .txt file; values should be separated with 'comma'
2. The settlement file must **not** contain any column headers
3. All fields are mandatory in the settlement file
4. Settlement File Name can take maximum of 50 characters without spaces
5. Only transactions older than current date can be settled

5.4. Merchant TID Report

The payment gateway shall generate a Merchant TID report which can be downloaded by the portal by logging to the Payment Gateway PG Interface. The TID report provides a summary of:

1. Settled Transactions
2. Refund Transactions
3. 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.

5.5. Refund Processing

The Portal administrator can initiate a refund for a transaction through the Payment Gateway Merchant Interface. The Transaction Refund requests can be initiated through the upload of a Refund File into the Payment Gateway Merchant Interface.

- **Refund process workflow**

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

1. Create a file in the standard format [refer format below] and upload into the 'Upload Refund/Cancellation File' option in the Payment Gateway Merchant Interface.
2. Payment Gateway processes the uploaded refund file on a batch basis; and provides a Validation Report that can be downloaded by the merchant through the 'Download Validation Report' option.
3. Refunds that are successfully received are then processed with each of the banks as per the workflow defined with the banks.
4. Refund – a transaction that is already settled for the merchant. Part of the transaction amount can also be refunded by the merchant.
5. Cancellation – a transaction that is not settled for the merchant. Only the entire transaction amount can be cancelled by the merchant.
6. Refunds made by the merchant can be viewed through the 'Refund Report' option.
7. 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	Payment Gateway 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 eg 100.00 will be 10000]
refund_amount	Amount to be refunded; in paise format

For example:

MUTI0803612345,20080731,6012345,100000,100000

- **Sample Refund File Naming Convention:** MerchantID_Refund_yyyymmddhhmmss.txt

Notes:

1. File is to be uploaded as a .txt file
2. Values should be separated with 'comma' delimiter
3. The refund file must **not** contain any column headers
4. All fields are mandatory in the refund file
5. Refund File Name can take maximum of 50 characters without spaces

5.6. 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.

5.7.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 120 characters. A 'NULL' value will not be accepted for any parameter.
5.	Disallowed characters	The following characters are disallowed in the parameters that are sent to Payment Gateway: < > % ; ' " ^ ` & ? = \\ 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.

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 logic/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|12-12-200416:08:56|0300|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|12-12-200416:08:56|0300|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.

ANNEXURE II – Links to NSDG / SSDG Integration Documentation

1. Main Links to Manuals - http://nsdg.cdacmumbai.in/administration/Manuals.jsp

2. Java Connector Cook Book -

   http://nsdg.cdacmumbai.in/administration/manual/JavaConnectorCookBook.pdf

3. Java Connector Manual -

   http://nsdg.cdacmumbai.in/administration/manual/Java%20Connector%20Manual.pdf

4. DotNet Connector Cook Book -

   http://nsdg.cdacmumbai.in/administration/manual/DotNetConnectorCookBook.pdf

5. DotNet Connector Manual -

   http://nsdg.cdacmumbai.in/administration/manual/DotNet%20Connector%20Manual.pdf

6. FAQ - http://nsdg.cdacmumbai.in/administration/faq.jsp

Kindly note the connector components (jar/dll) as per operating environment (Java/DotNet) of SAP/SP will be provided by NSDG/SSDG integration team.

ANNEXURE III

Date:

To,
NSDL Database Management Ltd
4th Floor, Trade World, A wing,
Kamala Mills Compound
Lower Parel, Mumbai 400013

Subject: Transfer of monies for transactions done through NDML payment gateway services

Dear Sir/ Madam,

This is to inform you that remittance of transactions done using NDML payment gateway services should be transferred to the below mentioned account details as per our requirement:

SP ID (Allotted by NSDG/SSDG) _____

Name of the Bank: _____

Account Title (Beneficiary Name): _____

Account Number: _____

Branch Name: _____

Branch City: _____

IFS Code: _____ MICR Number: _____

For Service Name: _____ provided by

Organization/Department Name: _____ Of

State: _____

Please arrange to have the necessary done at the earliest.

Sincerely,

<< Designation >>

<< Company Seal >>

[This letter should have the bankers Stamp / Sign / Date clearly indicating that the beneficiary details are correct]