Annexure I

1. Merchant initiated transactions for merchant payments

The merchant initiated transactions for merchant payment is a two-step process:

1. Generate OTP before transaction
2. Make payment to merchant using OTP

1.1 Generate OTP before transaction

The customer shall get OTP from his Issuing Bank, before the transaction. OTP Generation is a two-factor authentication process. Customer can get OTP using any of the following ways from the bank:

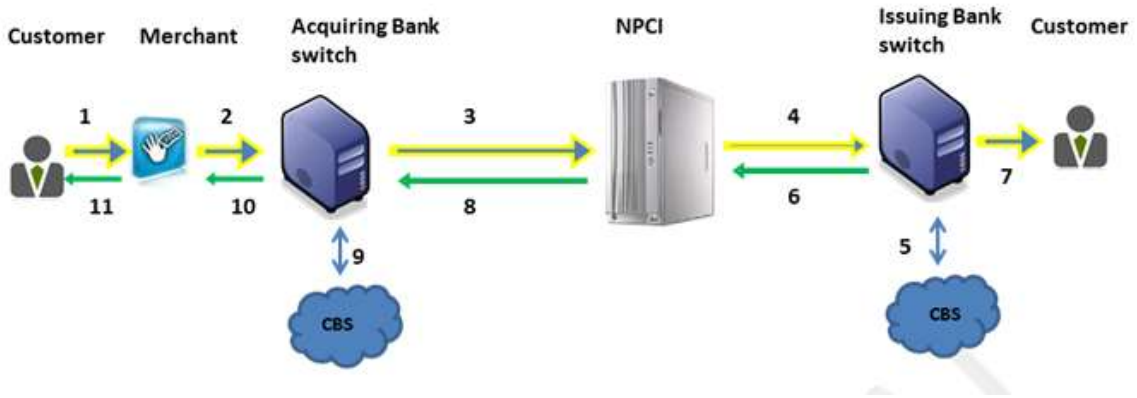
1. Use the Bank's mobile banking application option 'Generate OTP'
    a. Enter customer MMID, and M-PIN
    b. Bank shall authenticate this information and provide an OTP, that the customer can use for making payment
2. Use Bank's phone banking
    a. Bank provides the option to generate OTP on their phone banking IVR
    b. Customer calls the Bank phone banking IVR from his registered mobile number
    c. IVR recognizes the mobile number from which customer is calling automatically
    d. IVR prompts customer to enter MMID, and M-PIN
    e. Information is validated at Bank, and provides OTP to customer
3. Use Bank's Web / WAP site
    a. Customer accesses Bank's secure Web/WAP site, and visits 'Generate OTP' page
    b. Customer enters mobile number, MMID, and M-PIN
    c. Bank authenticates this information, and provides OTP
4. Use ATM
    a. Customer accesses ATM using ATM credentials and visits the screen 'Generate OTP'
    b. Customer enters mobile number, MMID, and M-PIN
    c. Bank authenticates this information, and provides OTP

1.1.1 OTP validity

1) Only one OTP is valid at a time, even if user has generated multiple OTP's. The last OTP generated will override all other OTPs
2) OTP should be valid only for one transaction – successful or failure.
3) It should be valid for maximum 60 minutes
4) OTP is 6-digit numeric
5) Transaction limit will be 50,000/- for OTP generated, or as decided by the bank

1.2 Make merchant payment using OTP

The transaction flow is as follows:



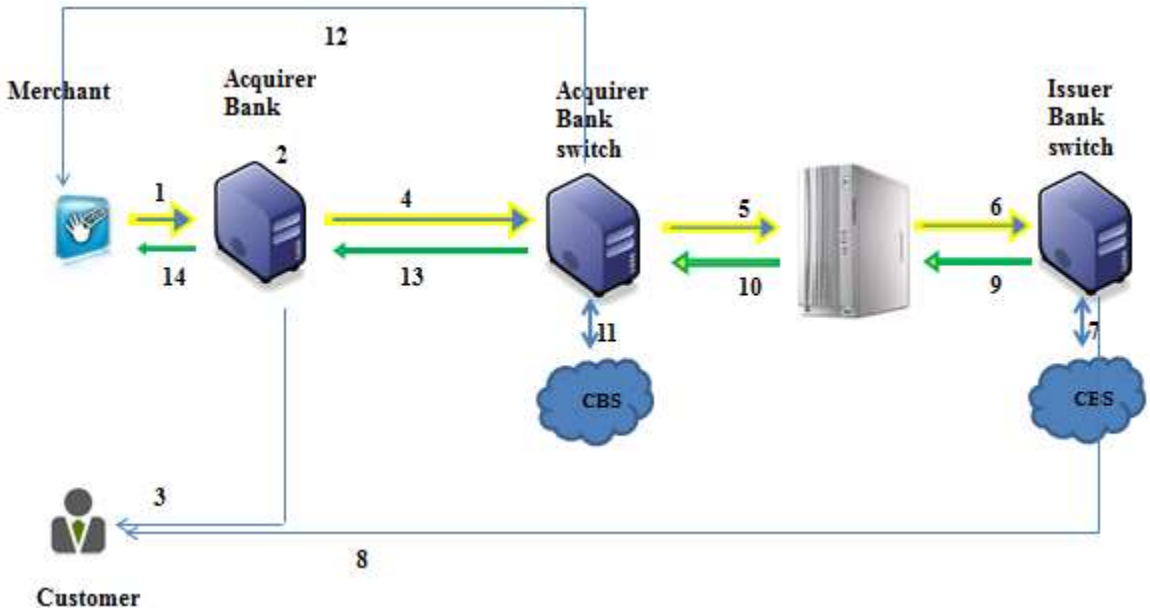
1. The customer can initiate the transaction through merchant application. Merchant application could be based on Web, IVR, or mobile handheld application. Customer enters following information for payment
    a. Customer mobile number
    b. Customer MMID
    c. Amount
    d. OTP
2. The transaction is forwarded by merchant application to acquiring bank switch. The information sent by merchant application includes above payment information by customer, as well as merchant mobile number and MMID
3. The Acquiring Bank validates merchant credentials (this includes merchant mobile number, MMID, and may be IP address, username, password, etc as may be provided by acquiring bank to merchant for authentication of merchant) and sends the transaction to NPCI
4. NPCI validates the request, and based on the NBIN (part of MMID), NPCI identifies the issuing bank and sends the transaction to the same for debit from the customer account
5. The issuing bank verifies the customer details, fetches the account number and debits the customer account (based on customer mobile number, customer MMID, amount, and OTP)
6. The issuing bank sends the transaction response to NPCI
7. The issuing bank sends an SMS confirmation to the customer informing him of the debit
8. NPCI sends this response to the acquiring bank
9. Acquiring bank based on the response received, credits the merchant account
10. Acquiring bank sends the transaction response to merchant application
11. Merchant application sends the transaction response to customer via SMS

Annexure II

1. Process Flow

- Merchant representative initiates transaction via SMS, IVR, mobile app, USSD, or WAP site
- Merchant initiates transaction using mobile application or web interface, enters customer mobile number for transaction initiation, MMID or bank name, and amount to be received
- Customer receives IVR call on his mobile number, and is informed about the merchant name, amount and how he wishes to pay
- Customer is prompted to enter M-PIN, or OTP
- Customer enters M-PIN, or OTP
- Customer receives confirmation SMS
- Merchant receives confirmation SMS

2. Transaction Flow



1. Merchant initiates transaction from his mobile
2. Request is received by Acquirer Bank Mobile POS platform
3. Acquirer Bank platform initiates IVR call and captures customer M-PIN or OTP
4. Request is sent to Acquirer Bank switch
5. Acquirer bank switch sends request to IMPS switch
6. IMPS switch sends request to Issuer Bank

7. Issuer Bank debits customer account
8. Issuer Bank sends confirmation SMS to customer
9. Issuer Bank sends response back to IMPS switch
10. IMPS switch sends response back to Acquirer Bank
11. Acquirer Bank credits merchant account
12. Acquirer Bank sends confirmation SMS to merchant mobile number (that initiated transaction)
13. Acquirer Bank sends response to Acquirer Bank Mobile POS platform
14. Acquirer Bank Platform sends response back to merchant

3. Transaction Limit

- Using M-PIN, customer can make payment up to Rs 5,000/- to merchant
- Above Rs 5,000/- customer needs to enter OTP. If OTP was generated through encrypted mobile banking application, transaction limit shall be as defined by the Bank, and if OTP is generated through unencrypted channel, transaction limit shall be Rs 5,000/-.

4. Security

Following guidelines shall be applicable for security of M-PIN captured by Acquiring Bank

- M-PIN shall be captured over IVR call
- Two-factor authentication – IVR call shall be made to customer mobile number registered with the Bank. Customer needs to enter M-PIN during IVR call. If the mobile number of the customer is not registered with the Issuing Bank, then the transaction will be declined
- Customer is informed about the merchant name and amount of transaction during the call. Customer shall have facility to reject the call if transaction details are not proper
- Transaction limit shall be Rs 5,000/- using M-PIN
- For higher transaction limit, customer needs to enter OTP generated through encrypted means
- M-PIN or OTP shall be captured by Acquiring Bank only
- From Acquiring Bank, M-PIN or OTP shall be encrypted with Triple-DES using HSM, same logic as NFS. This shall be decrypted at NPCI HSM, encrypted again at NPCI HSM with Issuing bank key, and decrypted at Issuing bank (preferably using HSM, but HSM not required mandatorily)
- This transaction flow is similar to card-not-present transaction over IVR, hence all relevant security protocols should be employed as they are employed for protection of card data traveling on IVR
- Acquiring Bank shall not store M-PIN or OTP captured during IVR call

5. Benefits

- This solution can be used very effectively for over-the-counter payments between customer and merchant and can help bring many merchants use electronic payments for receiving funds from their customers.
- From customer education point of view, this solution is very simple as well, as there will be standard process irrespective of the customer Bank.
- Currently, for OTP generation, customer needs to follow the process as defined by the Bank, and that is different for different Banks. Instead of OTP, we are asking the customer to enter his M-PIN only, this eliminates the requirement for the customer to generate OTP beforehand, hence making the transaction process easier for the customer.