UNIFIED PAYMENTS INTERFACE

Procedural Guidelines

A procedural document that defines the procedural guidelines framed under the provisions of Payment and Settlement System Act, 2007 and are binding to all members of Unified Payments Interface

Version 1.7

October,2019

Index of Revisions in UPI Procedural Guidelines:

Ver.	Page No	Section Title	Changes Made	Date	Justification
1.5	10	Permitted Transaction Types	In subsection Collect Request, below paragraph included: In case of Pull transactions, customer will have option to define the expiry time of collect request (up to 45 days). In case customer has not defined the expiry time, the default time should be taken as 30 minutes. The PSP has to provide an option to customer to define minimum validity of 1 minute, in case customer is selecting expiry time.	28th June, 2016	To include Minimum, default and maximum validity time for Collect request.
1.5	10	Permitted Transaction Types	In subsection Non-Financial transactions, added below paragraph: **Note**: The PSP shall continue to provide option to their customers for raising dispute/complaints using PSP App and adhere to resolve the same within TAT as defined in UPI Operating and Settlement guidelines.	28th June, 2016	Included the mandate for providing option of raising dispute through PSP App and adhere to TAT.
1.5	26	UPI App Considerations – Annexure III	Included below paragraph: i) PSP needs to build App for the at least two platforms i.e. Android and iOS, while for Windows, it will be optional.	28th June, 2016	UPI PSP App on Windows platform made as optional.
1.5	29	Customer Registration Process (Step I) – Annexure IV	Included mandate of Customer Specifies his SIM (in case of Dual Sim) and sending of outbound encrypted SMS to fetch the Mobile No of customer.	28th June, 2016	Eliminating manual data entry of Mobile No and also option to customer to select Sim in case of dual SIM Mobile
1.5	29	Customer Registration Process (Step II) – Annexure IV	Included "Typing the Bank Name" in addition to selecting drop down of Bank names, on PSP App during registration of Bank Account.	28th June, 2016	Providing additional option for customer to type bank name in-addition to selecting from drop down list.
1.5	48	Roles and responsibilities of PSP (Annexure VII)	Included below paragraph: a) PSP should place a moratorium of at least Two (2) Years in case a VPA is deactivated/deregistered by customer.	28th June, 2016	Including mandate of putting "Moratorium of Two Years" for VPA in case of deletion

1.5	54 - 66	Annexure XII to XIV	Included the 3 Annexures viz UPI PSP Role, UPI Broad Security consideration and App checklist	28th June, 2016	To provide clarity on PSP Role, mandating security consideration and standardising the App flow with mandatory functionalities.
1.6	12-13	Guidelines on NPCI Common Library (CL) installation (only in case of separate APK)	Deletion of section titled "Guidelines on NPCI Common Library (CL) installation (only in case of separate APK)" basis UPI Steering Committee approval dated 19thSeptember, 2016.	7th November , 2016	Deletion of section titled "Guidelines on NPCI CL installation in case of separate APK" as the option is not available to member banks as per UPI SCM approval
1.6	18	Liabilities	Deletion of "**Option a** – NPCI provides separate APK for Common Library" under subsection NPCI Liability in case of Common Library (CL)" basis UPI Steering Committee approval dated 19thSeptember, 2016.	7th November , 2016	Deletion of "**Option a** – NPCI provides separate APK for Common Library" under subsection NPCI Liability in case of Common Library (CL)" as per UPI SCM approval.
1.6	68	Annexure XII (UPI PSP Role)	Deletion of text "pilot period" in last paragraph of subsection "9. Embedding of NPCI Library into Banks Mobile banking App and merchant through sdk through banks".	7th November , 2016	Deletion of text "pilot period" in last paragraph of subsection "9. Embedding of NPCI Library into Banks Mobile banking App and merchant through sdk through banks".
1.6	101	Annexure XV	Included the section Annexure XV – Merchant SDK guidelines	7th November , 2016	To provide clarity included Annexure XV titled Merchant SDK guidelines
1.6	105	Annexure XVI	Included the section Annexure XVI – Merchant SDK checklist	28th December , 2016	To provide clarity included Annexure XVI titled Merchant SDK checklist
1.7	113	Annexure XVII	Off Boarding Process	24th Oct 2019	To provide clarity included Annexure XVII on Off Boarding Process
1.8	121	Annexure XX	Bhim *99# &Role and obligation for BHIM Bill Pay	24th Oct 2019	To provide clarity included Annexure XX on BHIM, *99#
1.9	123	Annexure XXI	UPI 2.0 Features	24th Oct 2019	To provide clarity included Annexure XXI on UPI2.0

Contents

Introduction

The Unified Payments Interface (UPI) offers an architecture framework and a set of standard Application Programming Interface (API) specifications to facilitate online payments. It aims to simplify and provide a single interface across all NPCI systems, thereby creating interoperability and superior customer experience.

The key aspects of the Unified Payments Interface are:

a) The payments can be initiated by both, the sender (Pay) & the receiver (Collect).
b) UPI is a mobile first platform.
c) The payments are carried out in a secure manner aligned with the extant RBI guidelines.
d) The payments can be done using Virtual Address, Account Number & Indian Financial System code (IFSC). NPCI may develop other channels to facilitate transactions.
e) The payment uses 1-click 2-factor authentication. Currently the second factor of authorization is UPI PIN. UPI is also capable of accepting biometrics in the future as a factor of authentication.
f) UPI is available through Unstructured Supplementary Services Data (USSD) channel as well. Members live on UPI can avail the same to cater users on feature phones.

Value Proposition of UPI:

a) Simplifying Authentication – UPI can ride on the Biometric Authentication of UIDAI (Trusted Third Party biometric authentication as a utility service) in the future.

b) Simplifying Issuance Infrastructure – The UPI ID addresses in conjunction with mobile as "what you have" factor helps payment providers to create virtual token-less infrastructure.

c) Mobile as Acquiring Infrastructure – Mobile phone as the primary device for payment authorization can completely transform the acquiring infrastructure to be simple, low cost and universal.

d) Enabling 1-click 2-Factor Authentication – UPI enforces 2-FA using mobile (first factor) and UPI PIN (Second factor) which makes all transactions compliant with the existing regulatory guidelines.

e) End-User Friendly - UPI offers payment through QR, Intent, NFC, Bluetooth & other standard protocols, which make the customer checkout process seamless.

f) Flexibility to 3rd Party/Merchant/Developer :- Depending on the business requirements, UPI offers 3rd party/merchants/developers options ranging from simple integration options such as intent/web collect to complex and detail oriented design through SDK and API model.

g) Flexibility for Payment Service Providers (PSPs) - Payment System Providers can build functionality rich mobile apps using UPI.

h) Exponential Innovation – UPI offers Application Programming Interfaces (APIs) that is minimalistic, fully functional, and allowing innovations in user interface, convenience

features, authentication schemes and mobile devices to be brought in without having to change the core API structure.

i) UPI Addresses Existing Challenges: Below table summarizes how UPI solves the limitations of the existing payment systems:

Sl.	Challenge	UPI Offerings	Description
1	Only Push based payment solutions existing in the Ecosystem	Pull Based Mobile transactions enabled via UPI	Existing solutions in the market are limited to push transactions initiated by the payer. **UPI enables push and pull transactions by the payer and payee.**
2	Limited Payment Options	Multiple Payment options available	Customers can pay using multiple identifiers (Aadhaar Number, Virtual Address, Account no & IFS code or mobile number only {Specific to same PSP}). Payment can be requested on one interface and authorized on a different interface.
3	Safety & Security	1 Click 2 Factor Authentication	Single click two factor authentication enabled using Device Fingerprint as the first factor & PIN as second factor of authentication
4	Design/Solution Flexibility	Highly Customizable	Designed to embrace the smartphone boom in India & the inclination of customers to move to digital mobile based solutions. UPI based applications offer a variety of customer experience depending on the business requirement.

Role of NPCI:

NPCI is the owner, network operator, service provider, and coordinator of the UPI Network. NPCI reserves the right to either operate and maintain the UPI Network on its own or provide or operate necessary services through third party service providers.

NPCI also has the right to call for documents relating to architecture, operating model and other technology related aspects to the UPI solution which the bank/PSP is planning to develop/developed. All certification stages will require signoff from concerned UPI team.

NPCI will issue circulars from time to time, to which all banks/ PSP's will have to adhere to.

Entities in UPI:

UPI is unique payment system which works on a two/three/four party model.

There can be maximum four entites consisting of **two PSPs** which will be acting as Interface Providers for the customers/merchants and **two banks** acting as Remitter & Beneficiary Bank. The role of the two PSPs shall be to facilitate the transaction and customer debits and credits happen in the bank accounts.

Bank by definition should broadly perform below mentioned functions/roles, as:-

1) **Payer PSP: -** Under this function a bank can onboard a customer, create his/ her UPI ID, create device binding which is used as a first factor of Authentication , using this customer can enter their UPI PIN to approve a financial transaction or non-financial request where ever necessary.

2) **Payee PSP: -** Under this Function a bank can onboard a customer/merchant & allow them to receive money basis allocated UPI ID or raise a Collect request. It is also known as beneficiary PSP / resolving PSP.

3) **Remitter Bank: -** All UPI users need to have a banking account with a UPI enabled banks. While performing a transaction, the user's bank account will be debited. The remitting bank also holds the responsibility to issue and store the UPI PIN set by the customer.

4) **Beneficiary Bank: -** Any credit going to a UPI user will be credited in his bank account. The bank receiving the funds in a UPI transactions will be acting as a beneficiary bank.

In case of Person to Person transactions, there may be four entities (two PSPs and two Account Providers/Banks).

UPI Transaction Flows:

The UPI transactions flows are outlined in Annexure VI.

UPI Availability:

UPI would be operational and available to all members round-the-clock with 99.9% uptime, excluding periodic maintenance with prior notice and force majeure events such as war and natural calamities. Periodic maintenance of the UPI System would be notified to all members 48 hours in advance unless an emergency or unscheduled maintenance activity.

Membership (UPI Ecosystem)

The UPI ecosystem is designed for banks. Only a banking entity can directly interact with the UPI switch. However, there is a provision for non-banking entities to participate in the UPI ecosystem. They will have to partner with a banking entity (already enabled on UPI) and develop their own PSP. Such PSP's are known as third party applications. The entire operational and financial liability of the third party application lies on the bank.

Membership Requirements:

i. The Payment Service Provider/member should be a regulated entity by RBI under Banking Regulations Act 1949 and should be authorized by RBI for providing mobile banking service.
ii. The member should comply with the Procedural Guidelines, certification requirements operating & risk guidelines and circulars issued by NPCI from time to time.
iii. The bank should be live on IMPS.

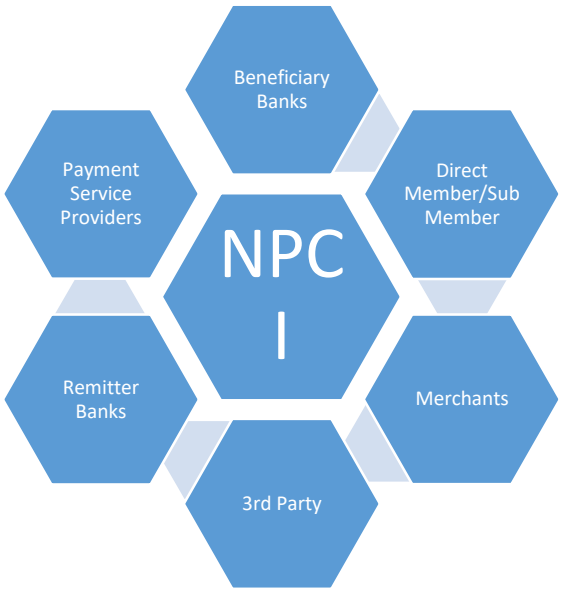
Additionally any bank which intends to participate in UPI as PSP, should ensure that while the bank's technology platform can be outsourced, **its functions 'as a PSP' cannot be outsourced**. This implies that the PSP Bank has an equal ownership of other bank's customer's data as its own customer base. Further the PSP has toprovide an audit report for the Data Center&PSP App by CISA equivalent auditor. The Qualified Security Assessor (QSAs) empanelled by the PCI Council shall conduct such audits at least once annually. The QSA shall verify App & the following:

a. System level Security
b. Network / Data Centre Security
c. Risk tools to be adequate
d. Policy & Procedures
e. Annual Certification process

In addition to the above, the member has to provide a declaration in writing to abide by:

i. All the terms and conditions of Unified Payments Interface Procedural Guidelines & Circulars, notifications, directions issued by NPCI from time to time.
ii. All guidelines issued by relevant authorities from time to time with respect to payment system operations.
iii. AML/KYC guidelines, other stipulations of RBI, as well as guidelines of NPCI issued from time to time

Members in UPI ecosystem:



Banks / Payment banks/ RRB's / UCCB's:

Banks & payment banks having mobile banking license (RBI approval) and enabled on IMPS are eligible for UPI. They can on-board as Issuer only or Issuer & Acquirer. Banks can have more than one PSP app but they should complete their issuer certification before getting on boarded as acquirer. Regional Rural Banks (RRBs) and Co-Operative bankshaving mobile banking license can on-board as issuers only, after going live on IMPS. RRBs can be on boarded as direct member or as sub member through the sponsor banks as issuers only.

Any banking entity mentioned above can play a part under UPI ecosystem. The banking entities have two major roles to play one is as Payment Service provider (PSP's) and another as a Bank (for all debits / credits). The further details related to role of PSP's can be referred from below from specific section pertaining to PSP roles & responsibilities.

3rd party Processors / Entities:

UPI as a frame work also provides feasibility for large technology companies / 3rd party processors /Merchant / Aggregators to connect to banks and provide extensive services to end consumers. The services may include both on-boarding of customers& merchants by PSPs for peer to peer transfer & merchant payment transactions respectively.

Member on-boarding/Certification Process:

There are 3 steps involved in On-boarding banks in UPI:

- **Sandbox testing** - Only banks coming with new vendor for certification needs to undergo Sandbox testing.
- **Certification** - Certification consists of two rounds Comfort and UAT.
- **Documentation** - Documentation includes SLA and NDA and other documents that needs to be executed by bank before go live. In addition to this bank needs to submit App Sec report, VAPT and Server Hardening report mitigating all the vulnerabilities before go live.

Cessation/Termination/Suspension of Service:

A. A member would cease to be a member in any of the following events:

a. If it's banking license is cancelled by RBI.
b. If it stops or suspends payment of its debts generally, ceases to carry on business, or gets in to liquidation
c. If it is put under moratorium or prohibited from accepting fresh deposits
d. If the bank settlement gets in to shortfall of funds in RTGS Settlement account for more than specified number of times as set by NPCI.

B. NPCI may terminate/suspend the UPI membership under any one or more of the following circumstances:

a. The member has failed to comply with or violated provisions of either the UPI or any other NPCI products.

b. The member commits material breach of the UPI or any other related product Procedural Guidelines and which remains un-remedied for 30 days after giving notice.
c. The RTGS settlement account with RBI of the member is closed or frozen.
d. The member bank is amalgamated or merged with another member bank or
e. Steps have been initiated for winding up the business of the member.
f. Suspension or cancellation of RTGS membership.
g. Suspension/Cancellation of Mobile Banking Approval by RBI.

Process of Termination/Suspension of UPI Membership:

- NPCI informs the member in writing regarding termination/suspension of its membership from the UPI network citing the reason for termination/suspension. Once the bank is terminated still they are supposed to accept /reject disputes as per the TAT i.e. 180 days.
- If NPCI is of the opinion that the non-compliance/violation is not curable, NPCI may suspend/terminate the UPI membership with immediate effect. However, the member would be given an opportunity to appeal and post decisional hearing within thirty days and will be communicated the order confirming or revoking the termination passed earlier.
- If the non-compliance/violation is capable of remedy but cannot be reasonably cured within thirty (30) days, the termination/suspension will not be effective if the member in default commences cure of the breach within thirty (30) days and thereafter, diligently peruses such cure to the completion within sixty (60) days of such notice of violation.
- On revocation of termination of membership order the entity should be entitled to apply for membership afresh. However, no automatic restoration of membership to UPI will be granted by NPCI.

Withdrawal of Service:

Any Member may withdraw from using the UPI service in the following ways:

- The UPI member would have to submit in writing for its withdrawal from UPI along with the reasons, serving a notice period of ninety (90) days.
- NPCI will take minimum of fifteen (15) working days from the date of receipt of request to process the withdrawal request for the member and to inform the date of termination of UPI network to the members.
- The amount deposited as collateral deposit for the Net Debit Cap (NDC) will be returned (only principal amount) to the member after the adjustment of the disputes, if any, which may arise for the settlement/obligations to any other member after ninety (90) days from the date of withdrawal. However, this may change post implementation of UPI Settlement Guarantee mechanism (SGM) or a consolidated SGM subject to all requisite approvals being in place.
- NPCI will inform all the other members regarding the withdrawal and the date of closure of UPI services for the particular member so that they can settle their adjustments/obligations

with the member. Members will notify the sub-members of the same and will also be responsible for settling the adjustments/obligations on their behalf.

- If a sub-member withdraws from UPI, the sub-member would have to submit in writing through the sponsor bank for the withdrawal and the reasons. The daily transaction limit, which is allotted for the sub-member would be released and added to the overall limit of the sponsor member.
- In case the Steering Committee approves the re-joining of member, the member would have to go through the complete process of joining UPI again. If sponsor bank wants to withdraw from sponsoring the sub-member, it must serve a thirty (30) days' advance notice to NPCI.

Off boarding:

The off boarding process is outlined in Annexure XVII.

Models in UPI

Broadly the models for 3rd party can be segregated basis architecture as primary factors:-

1) Model dependent on bank architecture.
2) Model independent of bank architecture.

Further segregation for both categories are mentioned below, which should be followed by banks while implementation of models:-

Additionally for every model mentioned under this section, PSP's/ banks has to provide all the documentation & relevant solution to NPCI well in advance for validations at NPCI level. It will be up to NPCI's discretion to approve the solution basis internal feedback.

Model Dependent on Bank Architecture:-

In this scenario, bank connects with NPCI through NPCI NET and routes the specific transaction for each merchant. The merchant will interact with the bank network through secure medium as per bank's internal policy. This integration should support both Collect & Pay type of transaction along with the relevant non-financial transactions. The hosting of services should be at the banks data centre.

In addition to above NPCI may request additional clarifications & documentations for any model mentioned below to ensure sanctity of UPI.

The liability/responsibility of each transaction in this case is on the bank /PSP which can't be outsourced to any other entity. The below mentioned models are approved by NPCI for merchants/third party entities to enter UPI ecosystem:-

a) Single PSP model (SDK).
b) Multiple bank model (API approach)
c) Service App model.

d) Web / Mobile app based Collect.
e) QR/intent etc. based approach.

Single PSP Model (SDK model).

Adoption of UPI payment by merchants and third party app providers has enabled the growth of UPI by integrating PSP SDK into their app. This entails bank to share the Common Library (CL) in a secured wrapper within PSP SDK (Software development kit). The PSP bank SDK integrated in the app connects to the bank PSP server for UPI related functions on secure channel. For more details, please refer to circular 15, 15A & 15B.

The banks engaging in deep integration with third party app provider should note the following;

A. Customer data storage

a. Customer Data (including customer consented data):

The customer data can be defined as Customer's name, customer's mobile number, residential address, email ID, gender, location details (entered by customer); device details such as App id, IMEI number, transaction related details – UPI ID, Transaction reference Number (RRN), transaction id, time stamp, beneficiary UPI ID, beneficiary account number and beneficiary Core Banking system (CBS) name resolved by beneficiary's PSP (stored for subsequent transaction enablement) etc. All the UPI transaction data should be stored in the app providers' end in encrypted format.

b. Customer payment sensitive data:

Classified as customer account details (such as Account number) customer payment authentication data (such as device fingerprinting) required for authentication as first factor. This data can be only stored in PSP bank systems. Some of the data like account number, can be shown in masked format to the customer on the app as per existing UPI PG. Last 6 digits of the Debit Card, Expiry date of the debit card, UPI PIN, Issuer OTP should not be stored.

B. Roles & Responsibilities of the PSP in Single SDK model:

The broad roles and responsibilities of the PSPs in single SDK model are outlined in Annexure – IX

Multiple bank model (API approach)

This approach enables multi-bank PSP's to partner with a single 3rd party, in which a large merchant/tech player (referred as "third party app provider") having an access to large customer base, can connect to UPI system through multiple PSP banks. In the multi-bank Application Programming Interface (API) arrangement, NPCI shall provide the NPCI Common Library (CL) directly for integration to the third party app provider on behalf of PSP banks. The App connects to PSP bank systems through third party app provider's system using API on secure channel.

For initiation, the third party app provider needs to write to NPCI with the names of participating banks (up to maximum of 5 banks). The letter should also include the details of existing user base and volume commitment.

The participating banks must note the following:

A. Storing customer data by app provider systems in Multi-bank model:

We classify the data into two types, namely 'Customer data' and 'Customer payment sensitive data':

1. **Customer Data (including customer consented data)**:
   The customer data can be defined as Customer's name, customer's mobile number, residential address, email ID, gender, location details (entered by customer); device details such as App id, IMEI number, transaction related details – UPI ID, RRN, transaction id, time stamp, beneficiary UPI ID, beneficiary account number and beneficiary CBS name resolved by beneficiary's PSP (stored for subsequent transaction enablement) etc. **The UPI transaction data should be stored in the app providers system in encrypted format.**

2. **Customer payment sensitive data**:
   Classified as customer account details (such as Account number) customer payment authentication data (such as device fingerprinting) required for authentication as first factor. **This data can be only stored in PSP bank systems.** Some of the data like account number, can be shown in masked format to the customer on the app. **Last 6 digits of the Debit Card, Expiry date of the debit card, UPI PIN, Issuer OTP should not be stored.**

B. Roles & Responsibilities of the PSP in Multiple bank/API model:

The broad roles and responsibilities of the PSPs in multiple bank/API model are outlined in *Annexure - X*

Service App Model (Using Remote Procedural Call)

RPC stands for Remote procedural call, the said protocol will help merchant to integrate easily with any UPI PSP/ UPI compliant app. This integration is a deep integration within a merchant App & UPI PSP / UPI compliant app based on correct source authentication method; like client –server based architecture. The service app should be hosted within bank premises &Technology Service Provider (TSP)/ASP could provide tech solution to PSP Bank on this.

- Merchant app will interact securely with another which is already stored on a mobile device. Merchant will tie with any acquiring PSP & get the Secret keys to interact with the PSP/ compliant apps. Below is the customer journey expected:-
- Customer will go to merchant App selects the goods which is for example has tied up with bank A for payment through UPI.
- If Customer device already contains bank A PSP app / UPI Compliant Apps Customer will be prompt as PAY via UPI.
- On clicking the same the authorization keys will do its validation & call the PSP /Complaint app.
- On successful authorization between merchant app & PSP app, customer will be directed towards CL (Common Library) page embed into PSP / compliant app, where customer inputs the UPI pin.
- On successful transaction customer will get both success on Service App / UPI complaint app & merchant app for confirmation of goods.

Interoperability:

It is also necessary that interoperability should still be there in form of intent or collect calls & UPI_ID creation should not be forced on customer.

Liability &Responsibility:-

- Liability /Ownership in this method based transaction remains with UPI compliant / Service app which is being called by the merchant app as the CL holding entity will be UPI compliant / Service app.
- This works on client &server based architecture where merchant app will work like a client & Service app will work like server.

Web/Mobile Application Based Collect

Under this model 3rd party / merchant will interact with PSP bank infrastructure to collect payment through UPI. The customer will access website / mobile app / browser of merchant for making payment. The customer needs to select UPI as the payment mode and enter his/her UPI ID. A collect request will be raised towards the ID and the user will authorize to complete the payment.

QR/Intent Based Model

Under this model 3rd party / merchant will interact with PSP bank infrastructure to generate a unique transaction reference number (tr) & accordingly QR / intent request will be generated by merchant on their website / mobile application respectively. User will be displayed all UPI compliant applications on his mobile phone and proceed to pay with the same.

Model Independent of Bank Architecture:-

Under this category a 3rd party can connect to NPCI UPI central switch basis below mentioned conditions.

- The 3rd party processor should already have NPCINET connectivity for other products of NPCI.
- Only collect based transaction will be permitted to these entities.
- MCC Mapping has to be as per the nature of business done by end merchant, the same has to be authenticate / approved by sponsor bank before moving into production environment.
- 3rd party should not initiate preapproved Debit transaction &ReqPay type: Pay from direct integrated network.3rd party have to get certified by NPCI for UPI with defined Scope for this model & will have to provide Audit reports.

Sponsor bank / Acquiring bank (Requirements, Role & Responsibilities)

- Sponsor bank has to provide intent letter to NPCI for the said integration.
- Sponsor bank should submit PSP handle creation form to NPCI.
- Dispute & Operational activities has to be carried out by sponsor bank, bank may also permit 3rd party to carry out activities on RGCS portals.
- MCC for merchants has to be confirmed & approved by sponsor bank.
- Settlement for the transactions will be happening through sponsor banks RTGS Account.

- Liability of such transaction will be taken by Sponsor bank.

Customer on-boarding in UPI

The individual bank account holder is the most essential factor under UPI ecosystem. The customers are offered a standard flow across all bank from on boarding of a customer till completing a UPI financial transaction.

Customers can be on boarded using below tools:-

1) BHIM Mobile Application.
2) UPI Bank PSP Apps.
3) UPI Compliant Apps (3rd party Apps).
4) *99# (USSD).
5) Mobile banking apps of each bank.

The above tools covers complete gambit of mobile devices in India & also covers both user base of customer connected to mobile data & customer not connected to mobile data.

Customer Registration:

All banks willing to avail UPI services are required to ensure safe and secure registration process for their customers. The registration process should be complied with the guidelines issued by the RBI/NPCI from time to time.

For remitting customers opting for mobile phones to initiate UPI transaction, mobile banking registration is mandatory. For Collect requests, the transactions may be initiated from non-mobile channels; however authorization of the transaction needs to occur at Mobile channel only. Mobile banking registration is mandatory for the Payer.

UPI service should be provided to customers registered for mobile banking service if it is initiated from Mobile App. The PSP registration process should allow the customer to generate/obtain his virtual address with the PSP through the registration process. It is however, also possible for a Bank joining UPI only as an Issuer, to provide Virtual addresses to its customer base by default.

The customer shall be providing banking details to be mapped against this virtual address through the defined process. These fields available shall form the local mapper at the PSP end for which it may have the customer agree to specific 'Terms & Conditions'.

The User Interface (UI) guidelines are only for reference purposes. PSPs are free to innovate the user experience part. The guidelines related to steps with regard to customer registration on PSP App are outlined in ***Annexure IV***.

Customer Complaints:

In case of any customer complaints regarding non-refund for failed transactions and/or non-credit for successful transactions shall be dealt by the PSP/Bank. Any complaint about credit not being given to a beneficiary should be dealt with conclusively and bilaterally by the remitting and beneficiary banks as per the guidelines circulated by NPCI from time to time.

In case of any complaints related to UPI transactions, the first point of contact for customer will be the customer's PSP. Customer's PSP has to mandatorily provide option in their App to raise dispute/complaint by providing transaction reference/Id number. However, if customer decides to

approach his/her remitter/beneficiary bank instead, the respective banks shall entertain all such requests and help to resolve the complaint to the customer's satisfaction. The PSP must provide to customers, the option of checking the current status of a transaction in the PSP App.

For complaints pertaining to the P2M it is mandatory for acquiring banks to take up the matter with merchant and check the status of the TXN i.e. if the goods/services are fulfilled.

PSP Management

Payment Service Providers (PSPs)

Payment Service Providers will be entities which are allowed to acquire customers and provide payment (credit/debit) services to individuals or entities. Payment Service Providers are the entities that provide for the Front-end/App for the customer. It should be a regulated entity by RBI under Banking Regulations Act 1949 and should be authorized by RBI for providing mobile banking service.

PSP will provide an App to the customers which will use the UPI libraries facilitating payments. The PSP App can be used by own bank's customers or other bank's customers. The customer can use any PSP app he desires and can start doing transactions securely. This will help customers who's bank does not offer mobile banking Apps or offer feature-limited mobile apps.

In UPI, it is mandatory for the PSP to come on-board as Issuer at the time of on-boarding. It should have the functionality of initiating both Push & Pull transactions and have the NPCI Libraries embedded into its App. It cannot come directly as an Acquirer without being an Issuer.

The PSP shall support the below transactions:

a) Financial transactions including Virtual Address based Push & Collect Requests, Account & IFSC based Pushand Mobile & MMID based Push Requests.

b) Non-Financial transactions including Mobile Banking Registration, Set & Change PIN, OTP Request and Balance Enquiry.

c) The PSP shall also provide on the PSP App the functionality of "Check Transaction Status" and an option to the customer for Raising Dispute/Complaint through the PSP App itself.

- ✓ The customer should be able to raise a dispute/complaint through the PSP App by selecting transactions from their past transactions history and/or by entering any other unique reference such as transaction id no.
- ✓ After the due diligence by the PSP, the dispute can be registered in the NPCI back-office system.

PSP App Implementation Guidelines:

There will be two approaches to develop and deploy for UPI App. The details related to both the approaches are outlined in ***Annexure III***.

NPCI Libraries:

NPCI Libraries area set of utilities which are embedded in the PSP App. These libraries are available for all major mobile operating systems viz. Android, iOS & Windows.

These libraries allow secure capture of credentials like OTP, PIN, Biometrics etc. The secured credentials are always captured by the NPCI libraries which use Public Key Infrastructure (PKI) Encryption.

NPCI will be using PKI to encrypt the PIN using NPCI Public Key which will be stored locally in the libraries. This encrypted block will be sent to NPCI where NPCI will decrypt using NPCI Private Key. Then NPCI will encrypt it using the Issuer's Public Key and send it to the issuing bank which will decrypt & validate with its Private Key. The Issuer Bank has to mandatorily decrypt the PIN and/or any other data using HSM only.

In case the Remitter Bank & Payer PSP are same entities, then the PSP may send pre-approved transaction to NPCI and need not use NPCI Libraries. In this case, NPCI will process only the Credit Request as the debit has already been taken care of by the Remitter Bank/Payer PSP. If the PSP uses NPCI Libraries, then NPCI will necessarily process both the Debit Request & the Credit Request even though the payer PSP and Remitter Bank are same entities.

In case the Remitter Bank & Payer PSP are different entities, then the Payer PSP has to mandatorily use NPCI Libraries to capture the PIN. In this case, NPCI will process both the Debit Request & the Credit Request.

Note: The PSPs/Banks may route ONUS transactions basis their internal processes.

Addresses Allowed:

Transactions can be done using Mobile Number& MMID, Account Number & IFS Code and Virtual Payment Address. The PSP shall mandatorily provide for the Virtual address based Push & Pull transactions and Account number and IFS Code based Push transactions.

Sl. No.	Particulars	Global Address	UPI ID (Virtual Address)
1	Identifiers Allowed	A/C No & IFS code	name@psp
2	Database	NPCI Mapper	PSP Local Mapper
3	Address Resolution & Responsibility	NPCI	Respective PSP

The PSPs will resolve the virtual addresses where the address will be mapped against the Account Number & IFSC/Mobile No & MMID stored at the PSP end. Virtual Addresses are always required to be issued by the PSP in the below format and ensure that customer is uniquely identified by the PSP:

username@psp

NOTE: UPI ID are only accepted in lower case only. UPI ID should be forwarded by PSP to NPCI in lower case only.

Username: It can be a unique name within PSP setup which the customer desires to have or can be provided by the PSP.

PSP: It will be provided to PSP by NPCI at the time of on-boarding process. PSPs can request the desired "PSP" name to NPCI and NPCI will allocate it to them provided, the "PSP" name has not already been taken by other PSP and it does not resemble in any way to any other PSP. The underlying principle for the "PSP" name will be an easy identification of the PSP by the customer and other users. It is desirable that Banks requesting PSP name should have registered/trademark/existing domain names. The maximum cap per bank will be 3 PSP handles. Any changes in this regard shall be governed by the Steering Committee direction/decision.

Permitted Transaction Types:

a) Financial Transactions: UPI supports the following financial transactions viz.

   a. *Pay Request*: A Pay Request is a transaction where the initiating customer is pushing funds to the beneficiary using Account Number/IFS Code, Mobile No/MMID, and UPI ID known as Virtual Address etc.
   b. *Collect Request*: A Collect Request is a transaction where the customer is pulling funds from the remitter by using UPI ID known as Virtual Address. In case of Pull transactions, customer will have option to define the expiry time of collect request (up to 45 days). In case customer has not defined the expiry time, the default time should be taken as 30 minutes. The PSP has to provide an option to customer to define minimum validity of 1 minute, in case customer is selecting expiry time.

b) Non-Financial Transactions: UPI supports the following non-financial transactions viz.

   a. Mobile Banking Registration
   b. Generate One Time Password (OTP)
   c. Set/Change UPI PIN
   d. Check Transaction Status

Note: The PSP shall continue to provide option to their customers for raising dispute/complaints using PSP App and adhere to resolve the same within TAT as defined in UPI Operating and Settlement guidelines.

Authorization

All financial transactions follow mandatory two factor authentication process. The first factor is validated by the PSP & the second factor is validated by the Issuer Bank.

- For non-biometric based authentication, the second factor will be a **four digit or six digit numeric UPI PIN.**

Below table represents the summary of the twofactor authentication in the first and subsequent transaction:

Authentication	First TXN	Authorised by	Subsequent TXN	Authorised by
1st Factor	Mobile Number	Issuer	Device Fingerprint	PSP
2nd Factor	UPIPIN /Biometrics*	Issuer	UPIPIN /Biometrics*	Issuer

***** *In case of Biometric, authentication will be done by UIDAI and on the basis of that, Issuer will debit the customer's account*

The PSP also checks the veracity of the person registering on its App.

Mobile Banking Registration Transaction:

Mobile Banking registration transaction allows the customer to register for mobile banking service with his Issuer Bank through UPI. It will be possible only if the mobile number (which is to be registered) is registered with the Issuer Bank for SMS Alerts/mobile alerts & not for Mobile Banking services. This service won't allow the customer to change or modify any existing number. It will only elevate the mobile number registered for receiving alerts to full-fledged mobile banking services. The customer requires details like last six digits of debit card, expiry date and an OTP to authenticate for this transaction. This transaction is to be facilitated only through PSP App. The steps related to Mobile Banking registration, Set/Change PIN and Generate OTP through PSP App are outlined in ***Annexure V*.**

PSP Role

The UPI PSP roles are outlined in **Annexure -XII**

PSP Liability:

The onus of validation of the first factor of authentication of customer credentials including Mobile device fingerprinting or any other material information which identifies the customer lies with the PSP. Only after proper validation of the customer identification and customer authorization credentials, the PSP will offer UPI services and allow the account to be operated under UPI.

The PSP shall be liable whether for any loss or corruption (whether direct or indirect) of data or information. The PSP will be liable for loss on account of breach of data (whether loss is direct or indirect) even if such loss was in the contemplation of the system participants or was wholly foreseeable. The PSP shall be fully liable for any loss of data or any loss arising out of breach of data whether due to wilful misconduct of PSP's representatives or arising out of gross negligence

or misconduct, etc., as such liabilities pose significant risk. **NPCI will in no way be liable for the same.**

The PSP's liability in case of claims against **NPCI resulting from breach of data or compromise of first factor or incorrect authentication of first factor shall be unlimited.**

The PSP **shall indemnify NPCI against** all costs, damages, expenses, liabilities, and losses (including but not limited to any direct, indirect or consequential losses, loss of profit, loss of reputation and all interest, penalties and legal costs (calculated on a full indemnity basis) and all other professional costs and expenses) suffered or incurred by NPCI arising out of or in connection with:

a) Breach of Data or corruption of data or information whether due to any system failure or negligent performance or non-performance of PSP or its employees, agents, representatives etc. or for any reason whatsoever solely attributable to the PSP.
b) Compromise of first factor or incorrect authentication of first factor due to act(s) of omission of commission of the PSP.

PSP Best Practices

1. If UPI Pin is not set, then application should force customer to set the UPI PIN. The flag of UPI Pin is provided in the response of List Account request.
2. **Multilingual Languages in Application** – Similar to BHIM application, there should be availability of regional languages which shall help in better penetration of the application.
3. **Pay using Contact details** – Saved contact numbers can be utilized to send money or raise collect requests where the mobile number can be prefixed to **@UPI** handle as UPI ID or can be checked whether the mobile number is available with the same PSP.
4. **Limitation of UPI ID (VPA) creation** – PSP applications need to restrict the creation of excess UPI ID's for a single user. This is also compulsory for blocking and spamming of the customers.
5. **Blocking unwanted collect initiators** – Customers should have the option to block UPI ID's to restrict any future collect requests from the same user.
6. **SPAM/Block marking** – Marking a user SPAM/Block in case the user receives collect requests from spurious users.
7. **Marking "Verified Merchants" for whitelisted merchants** – All the merchant UPI ID's which are whitelisted under List Verified Address Entity needs to be represented as Verified Merchants to the customers when they receive a collect request from them on PSP App.
8. **Account+IFSC option available for UPI enabled banks** – Whenever customer selects Account+IFSC as the payment mode, user should be shown the list of banks LIVE on UPI to restrict the user from entering account details of banks which are not LIVE in UPI and in turn reduce business declines.
9. **Gallery Read of QR code** – The Scan N Pay tab should have an option to read the QR from the gallery of the phone to help the customer scan and pay to the QR's which are shared to the user.
10. **Transaction History Download** – Application should have the option to download the transaction history of the customer.
11. **Alert notification** - PSP Applications can also provide alert notifications to the customers (payer) before the collect requests gets expired (approx. 15 minutes before).
12. **Beneficiary name** - Displaying the name of beneficiary customer in Bold to avoid wrong transfers (applicable for UPI ID based transfers)

13. **Deemed transaction Status** – Customers transaction history should be updated basis of the TCC/RET where the transactions needs to be marked as Successful or Declined accordingly and separate notification has to be sent to the customer.
14. **Application Password Security** –
    a. Constant password disabled (user cannot use same password, in case they change the password or does a forget password)
    b. Simple password disabled (user cannot use passwords like 1234, 2222, etc. which are easy to guess)
15. PSP App to force customer to set UPI PIN, in case UPI PIN is not set.
16. Banks to maintain the uptime for their UPI Application server and CBS.
17. 24*7 Helpdesk Monitoring from the PSP bank side to reduce the number of declines.
18. Bank to populate reason of decline in front end app as just like Bharat Interface for Money App (BHIM) with all the proper details.
19. Bank to show the clear reasons of decline for the list account i.e. BR (account linked with multiple customer ids), B2 (account linked with multiple names e.g. Joint account, Karta account etc.), B3 (Transaction not permitted to the account).

Customer Convenience/Handling Grievance:

a. If a customer is trying to Set/Change UPI PIN on any PSP applications and the transaction fails with the RC 'ZM'(Invalid UPI PIN due to violation of policies while setting/changing PIN) then the Issuing bank can send an SMS to its customer describing the policies of the bank while setting/changing UPI PIN. This shall also reduce the Business Declines for Invalid UPI PIN. This procedure can also be followed for all declined transactions which can be used as an information to the customers.
b. Customer Call Centers/Branch Help desk can be more proactive and helpful to the customers visiting/calling them for their grievance. This shall reduce the dependency of the customers on NPCI and the complaints will be closed more efficiently and immediately. This shall also increase and maintain the trust of the customers on their member banks.
c. Member banks are processing the reversals on continuous basis, it shall also be helpful if the banks process the reconciliation on T+0 BASIS.
d. Processing of Deemed Approved Transactions to be done on T+0 or latest by T+1 BASIS.
e. Only Genuine cases (e.g. Closed Account etc.) to be raised as RET otherwise the same can be termed as Transaction Credit Confirmation(TCC).

Best Practices to be followed to reduce the Customer Complaints:

a. As more and more customers are getting on boarded on UPI, it is ideal that customer should receive both credit and debit SMS/App notifications irrespective of the transaction ticket size.
b. Separate SMS to be sent to the customers for all Successful Debit & Credit Reversals.
c. App notifications to be sent for Deemed Approved transactions or when the TCC/RET is raised and responded.
d. After resolution of the Customer Complaints raised on the PSP applications, notifications describing the status of the complaints should be sent for the same.

e. Customer Complaints should be uploaded in RGCS and responded on same day to further enhance the customer experience.

Standardization of SMS Formats and App Notifications:

a. SMS/App notifications can be standardized for an enhanced customer experience on any of the UPI Applications. Through this, customers will not get confused and will have a clear understanding about the messages received to them.
b. Banks needs to educate customers for UPI PIN. Customers are using the application PIN as UPI PIN as well. Banks need to send a SMS/PSP App notification about their 4/6 digit UPI PIN.

Roles & Responsibilities

Roles & Responsibilities of the PSP:

The roles and responsibilities of the PSP are outlined in ***Annexure - VII***

Roles & Responsibilities of the Sub-members:

The roles and responsibilities of the sub-members are outlined in ***Annexure - VIII***

Broad Roles & Responsibilities of the Technology Service Provider (TSP):

The broad roles and responsibilities of the TSPs are outlined in ***Annexure - XI***

Settlement

Settlement of UPI transactions and Reports availability:

The details related to Settlement of UPI transactions and its report availability are outlined in **Annexurel**.

Settlement Guarantee Mechanism

Principle of Settlement Guarantee Fund (SGF)

These provisions are based on Principles for Financial Market Infrastructure of Bank for International Settlements.

As per NPCI risk management framework it maintains SGF for an amount that is arrived at using the following principles:

The system should have adequate funds for settlement to cover the shortfall in a member participant bank's RTGS Account.

The maximum duration is arrived at by taking into consideration all RTGS holidays by having sufficient funds for meeting at least two (2) settlement obligations on the very day of settlement.

SGF= {(1st HNDP* + 2nd HNDP** from the remaining cycles) from a specified time period} * 2

Constitution of UPI SGF

The SGF will have the following components:

Line of Credit:

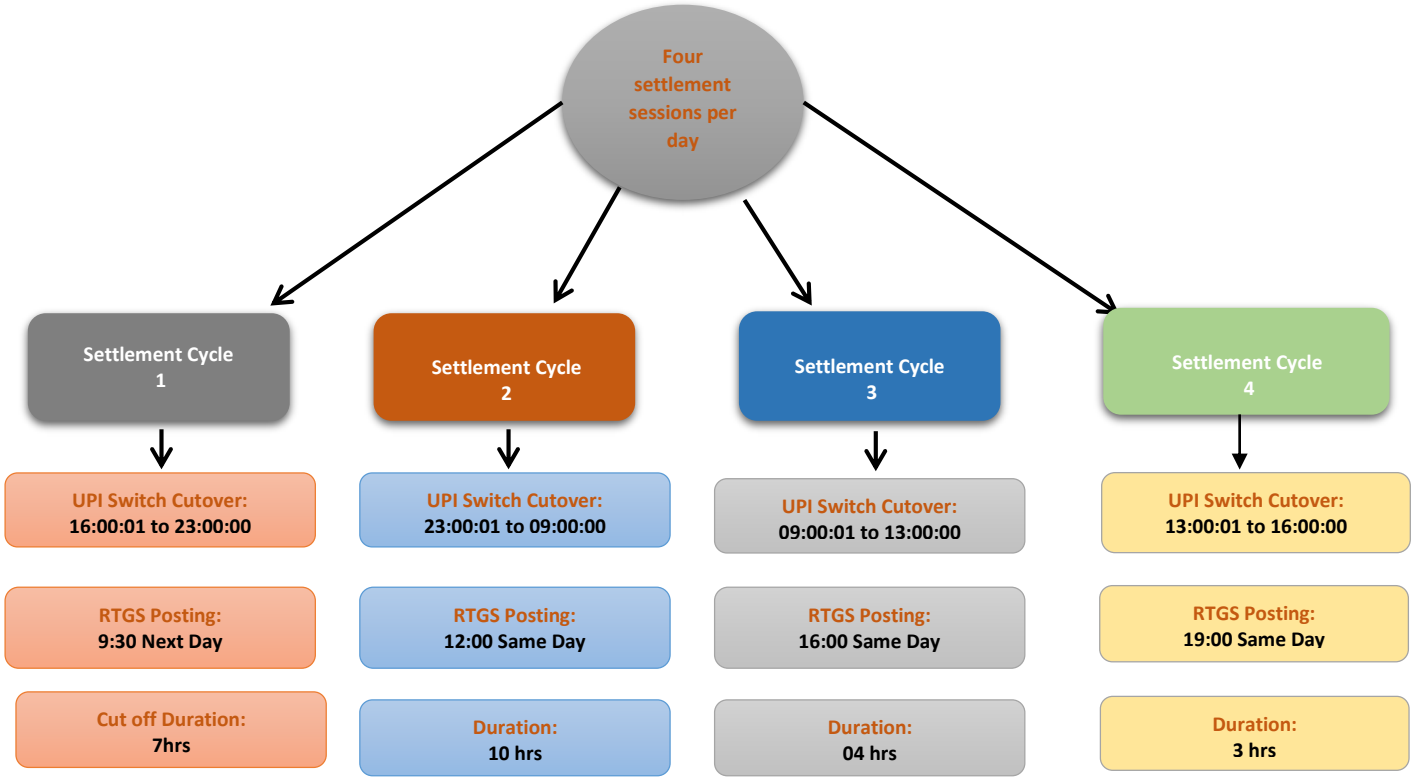
100% of the SGF, NPCI will establish a LoC arrangement with multiple banks and invoke this facility only in the event of settlement default by a member bank.

**HNDP: Highest Net Debit Position

A transaction is received at NPCI for routing to beneficiary bank only after debiting the remitting customer's account. Therefore, the risk of a remittance being made with the remitting customer not having adequate funds does not arise. Once the transaction reaches the beneficiary bank, it would be treated as "good fund" and the beneficiary bank should credit the beneficiary's account immediately. Thus, it would be a real-time money transfer system from the customer's point of view. However, from the members' perspective, interbank settlement of debiting the sending bank and crediting the beneficiary bank/PPI would take place on a net basis four times a day on RTGS working days

- However, a separate cycle-wise Daily Settlement Report (DSR) would be provided to all members
- On Sundays and other public holidays, only DSR would contain the complete business day transactions i.e. 23:00 hrs. To 23:00 hrs.
- Member's net position (payable or receivable) would get computed after every transaction
- Member's net position after every transaction should be within the "Net Debit Cap (NDC)" prescribed for each member basis on SGM.
- Threshold for a member would be the amount decided for member as per SGM criteria.
- Four settlement sessions would be applicable for UPI on RTGS working day throughout a week in the following manner

Four settlement sessions for UPI



Note:

- All UPI members should download the respective settlement files as shown in the above figure* (The settlement timings are subject to change based on RBI approvals which will be informed as and when to all the member banks via circular)
- Members must perform reconciliation on T+0 and T+1 basis
- The above cycles change on Monday. For settlement, please follow the timings and details mentioned in the above diagram
- UPI members should have a separate operations and reconciliation team to handle the day-to-day activities proactively and efficiently.

Loss Sharing Mechanism

In the event of a member bank failing to meet its settlement obligations on the settlement date and thereafter, the surviving participating member banks will make contribution towards sharing of loss in accordance with the procedure of loss sharing mechanism.

- The loss will be equivalent to the net debit obligation of the defaulting member participating bank(s) + Charges

- Keeping in view the PFMI guidelines (enunciated earlier) the loss will be shared by all the surviving member participating bank(s)

- The share of loss shall be related to the risk exposure (transaction limit) set for the participating bank(s)

- The contribution would be same for the banks in a particular exposure group.

Compliance and Regulations

Perceived Risks & Mitigation:

Sl.	Perceived Risks	Risk Mitigation
1	Secure Customer Registration	The customer will be sent an SMS by the Payment Service Provider while registering the customer to ascertain the veracity of the customer. The PSP also does the device fingerprinting through an automated outward encrypted SMS (Mobile number to PSP system) which hard binds the Mobile number with the device. This ensures that the transactions originating from the Hard bound device are secured at the first step itself. This outward SMS being sent should be encrypted and should not have any customer intervention. The system should provide for sustainability through the Mobile Operating System and App upgrades.
2	Application security	The PSP application shall be certified by NPCI and the NPCI Utility / Libraries embedded in the application for entering sensitive data such as; Biometric credentials, PIN and One Time Password (OTP).
3	Transaction Level Security	a) Transaction is secured with the Authorization which is split between the Payment Service Provider & the Issuing Bank. The device fingerprinting of the mobile device serves as the first factor.
		b) Customer enters the UPI PIN **or** the Bio-metrics as the 2nd factor of authentication.
4	Security while handling the PIN	The PIN is always entered by the customer on the NPCI Library (which is embedded into the Parent PSP App while certification) which is invoked while entering the PIN for an interoperable transaction. The PIN traverses over the secure channel from UPI to the Issuing bank basis the PKI encryption where PIN is encrypted using the Public key at the UPI and the Issuing bank decrypts at its end using its Private key.

5	Settlement Risk	The settlement of the UPI transactions shall be done under the respective products only already complying with the Settlement Guarantee Mechanism framework and hence there is no incremental settlement risk.
6	Unsolicited Pull requests to the customer	The end customer is in complete control of transaction and has to enter authentication details to initiate a debit to his bank account.

Fees & Charges:

It would be charged and configured in the system. Fees may be revised periodically based on the discussions and consultation with the Steering Committee. The details related to pricing structure(as an example) to be implemented in UPI are outlined in **AnnexureII**.

Pending Dues:

All members should clear all pending dues such as fines, settlement dues, and other liabilities within the stipulated time provided by NPCI. Failure to settle all dues within the stipulated time may result in suspension/termination of the member from further participation.

UPI Steering Committee:

UPI Steering committee shall comprise of representatives from IMPS Steering Committee members& any other committee as may be decided by the competent authority from time to time. The Committee is constituted to discuss and deliberate on business, operational, and technical issues of the UPI network. The committee is also subject to reconstitution on a case/need basis from time to time. The extant Procedural Guidelines document shall be read in conjunction with and as an extension of the products under which the UPI transactions are processed/settled. The UPI Steering Committee may invite industry experts for insights on a need basis. The committee would meet at least once in a quarter. The list of members and the calendar of meetings in a year would be published on NPCI's website in the beginning of the calendar year.

Fines:

NPCI reserves the right to impose penalty on the members for violating the guidelines. Penalty may include imposing fines as decided from time to time by the UPI Steering Committee or suspending/terminating end-to-end (host-to-host) connectivity of the member for frequent violations of these guidelines.

NPCI reserves the right to either notify the member or impose penalty on the member depending on the member's past record. No fine would be imposed, if the rectification is done within the stipulated time provided by NPCI. Failure to abide by UPI Procedural Guidelines would also be subject to Steering Committee recommendations/legal action.

Indemnification:

Including NPCI, it is binding on all members participating in the UPI network to defend, indemnify, and protect themselves from all loss and liabilities, if any, arising out of the following:

a) Member's failure to perform its duties and responsibilities as per UPI PG
b) Malfunctioning of member's equipment/systems
c) Fraud or negligence on the part of a member
d) Unauthorized access to UPI network

Member's software, hardware, or any other equipment violates copyright and patent laws.

Liabilities:

a) NPCI will take the responsibility of the security of data when the data reaches UPI and is in NPCI Network. When the data is outside the reach of UPI and NPCI Network, its security & authenticity will be the responsibility of the entity on whose possession the data is.

b) Security & integrity of the data will be the responsibility of the PSP/Bank even in cases where the Bank/PSP & the outsourced technology service providers are different entities. Therefore, it is recommended that the PSP/bank does full due diligence of the outsourced technology service provider as they are dealing with sensitive customer data.

c) NPCI Common Library (CL).

NPCI provides SDK to embed into Bank / Merchant App – This is an integrated approach wherein the Bank / PSP embeds the Common Library in the Merchant App through an SDK. In this case, the Customer downloads a single app of merchant or PSP. In all such cases, the Banks/PSPs shall own the full liability should the Common library be compromised.

Audit

Audit by RBI: The Reserve Bank may, for the purpose of carrying out its functions under the Payment and Settlement System Act, 2007 conduct or get conducted audits and inspections of PSP and it shall be the duty of the PSP to assist the Reserve Bank of India to carry out such audit or inspection, as the case may be.

Audit by NPCI/NPCI appointed external agency: NPCI reserves the right to audit the UPI related systems (including hardware and software) of the members as and when considered necessary either by self or by appointed external agency. Additionally, each member should conduct its annual internal audits and its processing agent, if any, to comply with the UPI Procedural Guidelines. Members would be required to submit the audit report annually to NPCI.

Intellectual Property Rights:

NPCI will own, hold, possess, and acquire the intellectual property rights to UPI and related assets.

Prohibition to use UPI Logo/Trademark/Network

- Upon termination of the UPI membership, the member should abstain from further use of the UPI Trademark with immediate effect. Failure to comply Shall entitle NPCI to seek appropriate reliefs/remedies through legal recourse

- Members that have been suspended from UPI membership would not be able to use the UPI for any transactions

- Any pending dispute pertaining to transaction errors not resolved before the member is suspended will be retrieved from the respective member's settlement account even after the date of suspension

- The suspended member would not disclose any information regarding the UPI network or any knowledge gained through participation in the UPI network to outsiders. Failure to comply with the same would be treated as breach of trust and could invite legal penalties.

Amendments to the Procedural Guidelines

NPCI will issue amendments to the UPI-PG from time to time by way of circular. Revised versions of UPI-PG may also be issued incorporating new provisions periodically.

Summary of circulars

Circular No.	Circular Name	Summary	Date of Issue
1	Enablement of UPI for thousand employees	UPI Member banks are advised to open up their apps to internal staff (at least 1000). This will ensure that the bank customers can use their own apps with their own accounts (onus linking) and also evolve ways to have the apps of other banks shared with their internal employee for (off us linking). The testing will include downloading the app, creating a profile, adding account and performing UPI transactions.	14th July, 2016
2	Prerequisites for UPI customer launch	Compliance and mandatory requirements for banks to go live on UPI: 1. UPI enablement of 1000 employees 2. Confirmation of 5000 plus successful transactions 3. Completion of 3rd party audit 4. Call centre activation 5. user manual/instruction section on bank's website	22nd July, 2016
3	Daily reconciliation of UPI transactions	UPI Member banks are advised to implement automated recon process for seamless reconciliation. The daily recon process at banks helps to identify customer service issues, frauds, system issues and this has been seen evidently in other payment system operated by NPCI. Banks are also advised to refer **operating and settlement guidelines version 1.0.**	2nd August, 2016
4	Compliance with NPCI circulars and Procedural Guidelines of UPI	Member banks are advised to confirm on compliance of Circular No. 1, 2 and 3 issued by NPCI	12th August, 2016

5	Security considerations on UPI - Immediate Actions	UPI Member banks are advised that in case of use of Mobile numbers as the UPI ID by the end customer, the PSPs may permit only the same Mobile number to be opted as UPI ID by the customer for which the sms has been sent at the time of registration. This is important step towards containing any fraud risk. UPI PSP Apps should also provide an option to the customer for resetting his App Login password/PIN	6th September, 2016
6	Implementation of FRM in UPI	Member banks are informed about the implementation of FRM in UPI with the rule that if a customer performs "5 successful financial transactions in 24 hours" or a cumulative value "exceeds Rs. 1lac" on debit side then NPCI/UPI shall decline the transaction basis the alert. NPCI shall be maintaining the negative list of Mobile numbers for which the transactions shall be blocked at UPI. Banks may report mobile nos. to NPCI and NPCI shall add such mobile nos. to the negative list	15th September, 2016
7	UPI Usability enhancements	Member banks are advised to follow the below points: 1. banks to route all meta APIs including onus transactions to NPCI 2. Banks to change the reference of MPIN to UPI PIN 3. Member banks to enable the dynamic QR code reading/writing functionality in the PSP app 4. Member banks to whitelist the large merchants 5. MCC of collections and interchange for unreserved ticketing/LIC 6. Deemed approved concept in UPI for credit timeout 7. Separate response codes for list account 8. Blocking spam collect functionality in PSP app 9. Alert for first time collect	19th October, 2016

8	Addendum to circular for implementing UPPI 1.5 changes	Banks were advised to provide the usage of ATM PIN in addition to existing factors. NPCI to progress to make the requisite changes in this regard. Member banks to make the changes in their UPI PSP app flow to capture ATM PIN on NPCI common library. issuer banks to identify the full card number and validate the pin by sending message to EFT switch operated by the bank	15th November, 2016
9	UPI Daily reconciliation and dispute handling	Member banks are advised to download "UPI settlement files and raw data files" from NPCI portal on daily basis after every settlement cycle. Member Banks should also do a three way reconciliation using bank's UPI switch data, CBS data and UPI raw data. Member banks should consider UPI raw data file as the base file for reconciliation. Member banks should ensure to handle 'exceptional scenarios' as per the NPCI 'Operating & Settlement guidelines'. Member banks should raise the customer complaints received on PSP App and also respond to complaints raised by other PSPs as per compliance defined in UPI 'Operating and settlement guidelines'	1st December, 2016
10	Recommendations to simplify UPI PSP apps for seamless customer on boarding	Member banks are suggested to enhance the PSP flow for increasing the usability by dual sim handling, simple customer on boarding and account additions. Hiring of professional agencies and analysis of customer dropouts are also suggested as one of the measures to member banks	1st December, 2016
11	Urgent enablement of reading/generating dynamic QR code	UPI member banks are advised to implement the functionality of generating & reading dynamic QR code in PSP Apps.	7th December,2016
12	Revision in benchmarking criteria of UPI system/interface of member banks.	UPI member banks are advised to process the volume/s of 5millionper day & 500 TPS including the system with core banking system	8th December,2016

13	Compliance to merchant on boarding and SDK guidelines checklist	Approval received from the steering committee & subsequent discussion with the member banks under the aegis of IBA, NPCI issued broad compliance guidelines on the merchant integration and SDK checklist to be followed.	8th December,2016
14	Unified Payments Interfaces compliance and requirement for the member banks	UPI member banks are advised to implement the below: 1. Implementation of separate settlement for UPI. 2. Implementation of deemed approval. 3. Implementation of generating UPI PIN using ATM PIN.	4th January,2017
15	UPI Merchant SDK: Specific requirements & Compliance	Compliance to merchant On boarding& SDK guidelines checklist.	18th January,2017
16	UPI,IMPS& *99# - Revision in interchange fee & MDR (1st Jan to 31st Mar 2017)	Post de-monetization, an attempt to accelerate digital payments has been made. Hence, NPCI through the ecosystem members has discussed the need of revising the existing pricing (interchange fee & MDR) for its products UPI, IMPS and *99#	21st February 2017
17	a. Compliance for successful debit reversals b. Handling deemed approved transactions and reconciliation	A) Non-processing of online reversals for declined transactions has led to increase in customer complaints. Hence implemented 4 additional test cases and new response code for proper understanding of declined transactions B) All member banks to send us an undertaking informing that bank is performing daily reconciliation	09th March 2017
18	Bank Compliances to enable UPI Merchant Ecosystem	Circular briefs about following product functions and essentials for merchant payments: a) Functional uniformity in QR based merchant solutions b) Uniformity in Android intent function in UPI Payments c) Implementation of Manage & List VAE APIs d) Other specific requirements to ensure seamless merchant payments e) Merchant on boarding related standardizations	20th March 2017

19	Continuance of the existing interchange structure for RuPay, UPI, IMPS & *99#	As mentioned in Circular 16, the existing interchange structure for merchant transaction and P2P transaction shall continue as per the existing structure	31st March 2017
20	Assigning exclusive MCC for Life Insurance Corporation of India (LIC)	MCC "6529" has been exclusively reserved for LIC	25th April 2017
21	Usage of BHIM by bank's UPI PSP App	UPI member banks are advised to use the brand 'BHIM' in conjunction with their own 'UPI PSP' at their own discretion including the BHIM Logo which will avail the benefit of popularity of BHIM app	08 June 2017
22	Launch of Referral and Merchant Cashback scheme for BHIM users	To promote the usage of digital payments through BHIM and *99#, GOI has launched 2 schemes namely (a) Referral bonus scheme for individuals and (b) Cashback scheme for merchants along with all relevant details	June 14, 2017
23	UPI OC Migration from Service Tax to GST 18%	It is informed to the member banks that upon Migration of GST from 1st July, 2017, the existing service tax rate applied at 15% will be charged to GST rate at 18% for all transactions from 1st July, 2017 (as per NPCI business day cut off time)	June 14, 2017
24	Corporate Disbursement through UPI	To remove the check of 20 transactions with cumulative amount of Rs. 1,00,000 for corporate disbursements. The check is on a 24 hour period for a Unique mobile number and Org ID	July 5, 2017
25	Discontinuing Services on USSD 1.0 system	NPCI decided to discontinue USSD 1.0 from 01st August 2017 and continue with USSD 2.0	June 30th , 2017
26	UPI Customer complaint handling process	Complaint Management document which explains the process to handle UPI customer complaints and best practices	
27	Inclusion of UPI Banks in BHIM Merchant Cashback and Referral Bonus Scheme	Revision in BHIM merchant cashback scheme and Customer referral Bonus scheme. The scheme is being extended to 31st March 2018	August 18, 2017
28	Scanning UPI credentials	All UPI PSP apps to scan & pay using both UPI QR & Bharat QR(integrated with UPI	August 18, 2017

	integrated in Bharat QR through UPI PSP application	credentials).NPCI has released the technical specifications to scan/read UPI credentials from Bharat QR.	
29	To reduce the high technical declines and business declines	TD to be less than 1% and customer awareness by banks to bring down the BD%	August 19, 2017
30	Upgrading UPI from TLS 1.0 to TLS 1.2 (To be treated as circular 30)	NPCI has decided to migrate from TLS 1.0 to TLS 1.2 Version from 1st Nov, 17 post which NPCI will only receive request and respond on TLS 1.2 version.	--
31	Inclusion of UPI Banks in BHIM Merchant Cashback and Referral Bonus Scheme	Confirmation of Inclusion of BHIM in their PSP name and other changes as per circular received on before 1st September 2017 for the scheme go live. Banks need to confirm this enablement by 20th of every month to be part of the scheme	September 7th, 2017
32	UPI - Multibank model (API Approach)	This circular broadly outlines the guidelines related to; a. Data Security b. Audit & Compliances c. Customer service d. Allocation of UPI_ID. E. Risk & liabilities defined. It also reinstates the PSP Bank's Ownership and Responsibility with respect to similar 3rd party provider.	15th September 2017
15 B	Single PSP Model Merchant Integration (Addendum circular 15B)	This bears reference to UPI Operating Circular 15 & 15A issued by NPCI in the past and procedures related to merchant integrations for UPI payments. This circular broadly outlines the guidelines related to; a. Data Security b. Audit & Compliances c. Customer service.	15th September, 2017
33	Multiple bank model (API Approach)	Large merchant/ tech player having a huge issuing base can enter the UPI ecosystem through multiple PSP apps. PSP apps shall be liable for settlement and operational aspects.	15th September, 2017
34	Compliances related to MCCs in UPI and guidelines for merchant on-boarded	All acquiring banks to ensure correct MCC is populated for the merchant they have acquired as per ISO standards. Banks acquiring aggregators must ensure visibility for the same. MCC 4900 (Utility) to include electricity, water and gas bills.	October 11th, 2017

	through Aggregator		
35	Guidelines for positioning of UPI/BHIM logo as payment mode at merchant location (offline and online)	Merchants providing pay by UPI/BHIM as an payment option should display the payment option prominently and above other UPI options. Transactions done via using the UPI/BHIM option should be free of any additional details being asked to the customer.	October 11, 2017
36	Pricing Circular	Reference available with Member banks	
37	Banks PSP apps and third party apps compliance to UPI Deep linking specs 1.5.1	Bank apps and third party apps are failing to comply with UPI deep linking specs 1.5.1*. As a result non-compliant apps is discouraging merchant to adopt UPI. *(Deeplinking specs will be revised from time to time and will be circulated to banks. Banks must be compliant on latest deep linking specs always.)	01st November, 2017
38	UPI – RRC "Refund/Return Reversal Confirmation"	Handling and controls to be built for credit adjustments/ returns by the customer banks	01st November, 2017
39	Efficient implementation for merchant on-boarding on UPI	Existing and proposed process to handle merchant transactions in UPI where Acquiring PSP and merchant bank is same. The proposed process shall help in handling deemed approved transaction.	20th November, 2017
40	UPI – Complaints handling process	To explain handling and controls to be built in for various types of customer complaints	23rd November, 2017
41	Process to handle chargeback for wrong account transfers	The process to handle wrong credits in UPI & IMPS which are initiated by remitting bank customers due to typo errors and resulting in wrong transfers	15th December 2017
42	Enhanced penalty for not updating TCC, RET, DRC & RRC after T+1 working days	Few banks are not updating the status in RGCS even T+1 working days for deemed approved, un-responded reversal, credit adjustments & returns which are resulting in customer complaints	15th December 2017
43	Standardization of the Account statement	To distinguish the transactions, certain important transaction parameters like remitter/beneficiary details, mode of	5th January 2018

	narration on Unified Payments Interface(UPI)	payments & purpose of the transaction should be made available in the passbook.	
44	1.Balance Enquiry optional in UPI for PSP & 3rd party apps 2.No storage of account balance by PSP or 3rd party apps	1.PSPs & 3rd party apps under SDK model shall provide balance enquiry as an optional feature 2. Customer account balance shall not be stored by PSP, 3rd party players or 3rd party apps for any purposes. The storage is not permitted.	11th January ,2018
45	1. Implementation of new response/error codes. 2.Best practices to reduce- "DA" Txn, "Unsuccessful debit reversals" and "overall declines"	To explain the process to reduce deemed approved * debit timeout transactions (requiring DRC) in UPI. This shall help to reduce operational work, avoid customer complaints and enhance positive user experience.	12th February 2018
46	BHIM UPI branding at all UPI enabled apps and merchants.	UPI ecosystem comprises of multiple UPI applications which are owned by the banks and 3rd party UPI enabled Apps. All UPI enabled apps may change name to BHIM <App name> UPI App	23rd February 2018
15C	Guidelines on interoperability features for all BHIM UPI Apps	Circular is in continuation to Circular 15, 15A & 15B to have mandatory features for interoperability across all BHIM UPI Apps	16th March 2018
47	Extension and modification of BHIM/BHIM UPI incentive/cashback scheme for individuals and cashback scheme for merchants.	The revised BHIM scheme has been implemented by Govt. of India for BHIM & BHIM UPI App users.	24th April 2018
48	Foreign Inward Remittance (FIR) through Unified Payment Interface (UPI)	To process the domestic leg of FIR in to bank account using UPI	9th May 2018

49	Onboarding banks with no retail presence as an acquirer only in UPI	Banks which cater to Corporate/Institutions and have no retail presence are now allowed to be on boarded on UPI as an acquirer only. The same is approved by SCM Members. (No Retail App).	11th June 2018
50	Introduction of Bill Pay functionality (BBPS) on BHIM App	NPCI has operationalized the Bill Payment functionality in BHIM, through BBPS platform w.e.f. 25th May, 2018. This functionality is allowed to those banks which are live in BBPS as customer OU and live in BHIM as Issuers.	11th June 2018
51	UPI – Process for scheduling maintenance activities & SMS alerts to customers	UPI has seen significant growth in number of financial transactions in the recent months. While this indicates that UPI is being adopted as a preferred payment method, it also necessitates that customer experience on UPI transactions is seamless	27th June 2018
52	Modification of BHIM incentive scheme for individuals and withdrawal of BHIM incentive scheme for merchants	The revised BHIM scheme provides incentive only to the new BHIM app users and no other incentive shall be applicable. Under the BHIM cashback scheme of Individuals the incentive shall be paid only to the new users of BHIM app as per the defined requisites.	17th July 2018
53	Compliance to the Sec 42A, Rule 3 and 7 of Information Technology Act,2000	Under section 15.3 of the UPI Agreement, member banks are obliged to ensure compliance with laws on data protection under Information Technology Act, 2008 and rules framed thereunder. Member banks to comply with section 43A of IT Act, 2000 and the IT Rules, 2011 which deal with data protection of sensitive personal data.	17th July 2018
54	Regarding removal of Pay to Aadhaar functionality in UPI and IMPS	Aadhaar number is a sensitive information and the revised framework about its usage in the payment landscape is still evolving. With this background, 'Pay to Aadhaar' functionality in both UPI and IMPS shall be removed from 31st August 2018 by member banks, PSP/3rd PSPs.	17th July 2018
55	Blocking of transaction between same bank account in UPI	Transactions initiated through methods like same 1) UPI ID to same UPI ID, 2) UPI ID to Account IFSC and 3) One UPI ID to Other UPI ID but with both IDs having the same underlying account will be blocked by 1st August, 2018 at NPCI. Also PSPs/banks should block the 1st and 2nd method at their end.	19th July 2018

56	Roll out of the features of Unified Payments Interface (UPI) 2.0	Description of below UPI 2.0 functionality : · One time mandate with block functionality ·Over-draft(OD) account as an underlying account in UPI ·Invoice in the inbox (View & Pay) · Signed Intent/QR	14th August 2018
57	Changes in PSP & Customer communication to prevent fraudulent transaction	To reduce fraudulent transaction following changes have mandated for bank/PSP level. ·Standardization of SMS sent to customers for a collect request · Masking of Account number ·Disabling UPI services via customer facing channels ·PSP apps to add payment confirmation page before transaction authorization	20th August 2018
58	Parent PSP app to support interoperability compliance for their P2M only Apps in case of Non-exclusive handles (Exclusion for Apps providing only P2M services)	To an extension to Circular No. 15C · Only P2M apps having non-exclusive handles will be applied under this circular · If no such UPI enabled apps are present in the phone, then the merchant app should give provision to download the Parent app · Parent PSP App (acquiring app) to cater the interoperability features.	28th August 2018
59	Change of Production IP of RGCS for UPI	Migrated to a new advanced and high end server to improve the RGCS Performance in UPI and informed bank to use new IP	23th August 2018
60	NRE to NRE account transfer by IMPS and UPI	Crediting/debiting non-resident accounts in UPI & IMPS for domestic transactions	15th October 2018
61	UPI Transaction frequency limit revised to 10 transactions for	Frequency of P2P transactions per bank account has been revised to 10 for the span of 24 hours.	22nd October 2018

	P2P, w.e.f October 21,2018		
62	UPI Pricing for transactions through linked OD account	a. Pricing remains same for Secured OD b. Revised pricing is applicable for Unsecured OD	04th December 2018
63	Migration from UPI 1.0 to 2.0 by 31st March 2019	i. All member banks to complete certification for UPI 2.0, latest by 31st March 2019 ii. All new banks to be on-boarded on UPI 2.0 iii. UPI central switch shall continue to support both UPI versions up to 31st March 2019	07th January 2019
64	Pricing applicable for Mandate & Industry Program	Applicable pricing for the mandate functionality along with interchange and industry program is tabularized	23rd January 2019
65	Change in cutover cycles in UPI	To bring in further efficiencies in settlement process. Change in cutover cycle has been advised	24th January 2019
66	Minimum Net Debit Cap (NDC) of Rs 2.5 lakhs for Sub Member banks in UPI &IMPS	The minimum NDC limit across UPI and IMPS to be maintained at 2.5 lakhs for existing member and sub member banks. The proportion of 10:90 in NDC limits across UPI & IMPS shall be applicable only at sponsor banks end not at beneficiary	22nd February 2019
67	Revision in UPI switching fees for P2P & P2M.	Revised charges inswitching fees for P2P transactions and P2M transactions	22nd March 2019
67A	UPI Pricing – Addendum to UPI Circular 67	Revised charges for switching fees ,interchange and PSP fees in case of UPI	16th May 2019
68	Levy of sub charge by merchants and channel partners prohibited in UPI	a) UPI must be treated at par with any other debit payment modes such as debit card, NEFT Net banking at all times. b) No sub charge to be levied to customers for UPI Transaction. c) Any convenience fees if charged must be mentioned upfront to the customer on the	16th May 2019

		merchant payment of page prior to selection of payment mode. d) Such Convenience fees must be consistent for available debit payment modes (i.e net banking, Debit card and UPI etc.) e) NPCI reserves the right to take appropriate actions against the sponsor bank for any act of non-compliance to the above stated.	
69	Pricing Circular	Reference available with Member banks	
70	Introduction of P2PM category in UPI for unorganized or small merchants	Introducing a new category "P2PM" in UPI which caters small merchants and unorganized retail sector with low value ticket size. These merchants to be on boarded with a new MCC 7407 by the acquiring PSP's	17th June 2019
71	Enhancement of UPI per transaction limit to Rs 2 lakhs for UPI based ASBA	All members and PSP banks live on UPI 2.0 mandate block functionality should maintain the per transaction limit of Rs 2lakhs for UPI based ASBA transactions with purpose code 01 with MCC 6211.	21st June 2019
72	Pricing Circular	Reference available with Member banks	
73	Payer APP behaviour for intent based transaction on UPI	Guidelines for intent and a reference to OC 15C	19th Sep 2019
74	UPI Compliance Guidelines	The banks and stakeholders including not limited to TPAP's etc. are requested to comply to the below circuto the below circulars. a)Functional&Interoperable compliances b)Risk/Infosec compliances c)Technology &Operation compliances d)Pricing ,commercial&limits in UPI e)Settlement ,Reconciliation &Disputes f)Branding related compliances.	19th September 2019

Fraud Risk Management operating circular

Sr. No.	Date	Circular No.	Subject
1	26April 2017	RMD-028	Measures for creating VPA basis sensitive information by merchant & corporates
2	20 June 2018	RMD-079	Duplicate SIM Issuance Fraud in Mobile Banking/ Mobile Payments
3	27 June 2018	RMD-122	Duplicate SIM Issuance fraud in mobile banking mobile payments
4	12 Nov 2018	RMD-327	Mandatory features to be implemented by PSP's
5	08 Dec 2018	RMD-014	Security Recommendations for UPI ecosystem
6	27 Dec 2018	RMD-015	Mandatory features to be implemented by PSP's & TPAP's – To avoid SMS Spoofing issues
7	10 Jan 2019	RMD-015A	Addendum to RMD 15
8	30 Jan 2019	RMD-018	Risk and Compliance framework for ecosystem
9	18 April 2019	RMD-OC-1-19/20	Restrictions on BHIM UPI Transactions- Mandatory mitigating requirements

Annexure – I (Settlement & Reports)

UPI Settlement & Reports Availability:

All transactions processed through UPI switch shall be settled through RTGS. Settlement files (DSR & Raw files) shall be made available in RGCS.

Note:

- The settlement cycles are subject to revisions from time to time.
- All UPI members should download the respective settlement files.
- Members must perform reconciliation as per the guidelines issued by NPCI from time to time.
- The Settlement cycles and timings shall be as prescribed by NPCI from time to time.
- UPI members should have a separate operations and reconciliation team to handle the day-to-day activities proactively and efficiently.

At the end of the each cutover time and completion of Settlement file generation, NDC limit would be refreshed, the net receivable or payable of each member would be generated, and a daily settlement report would be prepared and sent to all members through a Secure File Transfer Protocol (SFTP) and made available in RGCS application.

Currently, NDC Limits are allotted to banks in IMPS as per the SGM policy. For UPI transactions, banks will be assigned a specific percentage of their existing IMPS NDC Limits as prescribed and as approved by the respective governance bodies.

Please note:

- The net settlement amount would include transaction and settlement fees payable between the banks & PSPs (Interchange Fee & PSP Fee) and NPCI (Switching Fee).
- NPCI has obtained Type D RTGS membership and provides settlement service to banks. It would be free to revise the settlement charges based on business needs.
- NPCI will act as a settlement agency and will arrange the necessary interbank settlement of credits and debits to the banks' respective RTGS Settlement Accounts with RBI as per approval received from RBI vide letter DAD/RTGS/626/24.02.001/2011-12 dated Oct 24, 2011.
- It will be the members' responsibility to verify accuracy of the Daily Settlement Reports with member pool accounts, banks switch file, CBS files etc.
- In case of net debit, a member has an obligation towards other members. Therefore, members are advised to ensure strict compliance to the RTGS operational instructions of RBI in this connection. Any failure to maintain the required balance in the RTGS settlement account would attract action as deemed fit by NPCI.
- New members before participating in UPI should issue letter of authority to RBI authorizing net debit/credit for UPI related transaction in their respective RBI accounts by NPCI, duly approved by their respective boards. This is applicable to the members who are not live on IMPS.
- A member failing to meet its daily settlement obligation more than two times in a month would be debarred from membership.

Reports Availability:

UPI would provide the following daily reports in DMS / RGCS application format round-the-clock:

- Raw data file (made available on all 365 days – 24/7 in RGCS)
- Net settlement report (NTSL)/Daily Settlement Report (DSR) (Will be made available on all NPCI settlement days – please refer NPCI settlement holidays list published every year)
- Adjustment reports – Raised & Received (made available on all 365 days – 24/7 in RGCS)
- GST Reports – (Made available on monthly basis in RGCS)
- Any other reports as may be relevant

Members will be provided with the following reports:

Adjustment to Settlement:

Discrepancies relating to reconciliation/adjustment done by members, based on reports furnished by UPI are the responsibility of the participating members. Such discrepancies should be resolved by members as per the settlement procedures set forth in the UPI Procedural Guidelines. The following points explain the switching fee adjustments:

- NPCI determines the amount of service fees its members owe for using UPI services.
- As a service provider, NPCI would maintain an account with a member participating in the UPI network.

AUTH Settlement:

NPCI shall process the settlement for all approved & deemed approved transactions (RC-00 & RB) as per the settlement cycles.

Settlement of Adjustments:

NPCI shall settle all adjustments once a day in 1C after netting the same (adjustments raised less adjustments received).

Annexure – II (Pricing Example)

UPI Merchant Interchange Compliance:

In case of merchant transactions, it is the ownership of Acquiring Bank to populate the correct Merchant Category Code (MCC code), under which merchant is set-up. The UPI system will calculate and settle the Interchange between Acquiring Bank and Issuer bank basis MCC code populated. Merchant Category Code should flow in all the transactions from Acquiring Bank. The acquiring bank may have compliances built in for deviations, if any, basis various parameters such as velocity checks. In case of merchant pushes the P2P then compliance rule of MDR/Interchange will be applicable.

In case of P2P transactions, the interchange will be basis "Default MCC" populated in P2P debit leg. P2P MCC code cannot be used for merchant transactions.

NPCI will issue circular regarding changes in UPI Fees from time to time as per decisionstaken in Steering Committee Meeting.

1) Example of a Merchant UPI transaction for Fees calculation(the below is just an indicator and are subject to changes):

Transaction Amount	Rs. 75,000
Merchant Name	Flipkart
Flipkart's Acquirer Bank	ICICI Bank
Customer PSP	HDFC PayZapp (HDFC Bank)
Customer Issuing Bank	Axis Bank

Particulars	**Details**	**Paid By**	**Paid to**
Charges to Customer	If yes, to the customer by merchant	NA	
Transaction Amount	Rs. 75,000	Axis Bank	ICICI Bank
UPI Switching Fee	Rs.30.1(Ad valorem charges equally divided between acquiring PSP and issuer)	Axis Bank, ICICI Bank	NPCI
Interchange Fee	Rs. 50 (max cap) @ 0.15%	ICICI Bank	Axis Bank

PSP Fee	50 paise	ICICI Bank	HDFC Bank
MDR	Rs. 100 (max cap) @ 0.30%	Flipkart	ICICI Bank
Total Charges to Axis Bank (excl. Trnx Amountand GST)	Rs.15.05		
Total Charges to ICICI Bank (excl. Trnx Amountand GST)	Rs.65.55		

2) Example of a Person to Person transaction for Fees calculation:

Transaction Amount	Rs. 75,000
Payer PSP	HDFC PayZapp (HDFC Bank)
Payer's Remitter Bank	Axis Bank
Payee PSP	SBI Buddy (State Bank of India)
Payee Beneficiary Bank	ICICI Bank

Particulars	**Details**	**Paid By**	**Paid to**
Charges to Payer	If yes, to the customer by the Remitter Bank	NA	
Transaction Amount	Rs. 75,000	Axis Bank	ICICI Bank
UPI Switching Fee	50 paise	Axis Bank	NPCI
Interchange Fee	Rs. 5	Axis Bank	ICICI Bank
PSP Fee	50 paise	Axis Bank	HDFC Bank
Total Charges to Axis Bank (excl. Trnx Amount)	Rs. 6.00 (Switching + Interchange + PSP Fee)		
Total Charges to ICICI Bank	NIL		

(The Bank/PSP names used here above are for representation purposes only)

Annexure –III (PSP App Considerations)

UPI App Considerations:

There can be two approaches defined to distribute UPI compliant apps:

1. **Independent mode** - Bank developing a separate UPI app, and/or converting their existing Mobile Banking application to be extended to facilitate UPI services.

2. **Embedded mode** - The UPI compliant app/module is embedded in other (merchant) apps by bank giving the binary/SDK to the merchant to integrate into their apps. Note that merchants may choose to include more than one UPI compliant apps from different banks.

Following are the boundary conditions which bank needs to keep in mind while developing and distributing the UPI app with any of the above listed approaches.

Boundary Conditions:

a) While bank may engage third party development for the PSP mobile app, the PSP central application must be managed and secured as per RBI guidelines on banking systems.

b) PSP Central Application must reside in Bank's own Data Centre and in under no condition, the PSP customer data to be shared with Merchant App.

c) Under no condition the libraries given by NPCI to bank should be handed over as it is to merchant. The libraries must be integrated into Bank's app and then handed over to merchant (if option 2 i.e. Embedded mode is chosen)

d) The customer data regarding the payment (account mappings and credentials) details required as per the UPI architecture and specification should be visible to, and residing only in the bank's UPI systems.

e) The merchant app should not have visibility of the sensitive account/credential data captured by UPI app.

f) The responsibility of the functionality mentioned for the PSP app in the guidelines shall remain with bank. The bank must have the mechanism to certify the PSP app with aligned merchant app and with proper invocation by any other app on the phone for payments. (The iOS and Android all versions supported from Day 0)

g) The choice of which bank UPI app to be downloaded and used for payments (during transaction flow) would reside with customer. With above options the customer may decide to download his choice bank's PSP app and make all payments through his mobile purchase using this app.

h) The customer can also have multiple PSP apps. Under no circumstances, one UPI app (embedded or independent) must interfere with another UPI app when installing, running, etc. Once the customer selects "Pay by UPI", all the UPI apps on the phone should pop up allowing him/her to select a preferred UPI app as explained ahead.

i) PSP needs to build App for the at least two platforms i.e. Android and iOS, while for Windows, it will be optional.

UPI App functionality:

a) The UPI app shall be invoked by embedded merchant app or any other app intends to initiate the payments when customer has selected "Pay by UPI". The mechanism of invoking the PSP app shall be same or similar in both the methods either internal or external.
b) When an intent / call is made by merchant for payment through UPI, UPI enabled Apps installed / embedded on the mobile application and where the customer has registered and

set UPI PIN should be mandatorily shown to user, so that the customer can select the UPI App of his choice to pay the merchant.

c) The central PSP system must have mechanism to authenticate the merchant before proceeding for the payment transaction.

d) Merchant Initiated Intent:

1. Banks that are offering the merchant PSP integrated App, should have an intent call OR other such enablement basis OS capabilities on the phone to call other PSP Apps.
2. The banks can embed its SDK in the merchant App for intent call. This is to ensure call is made to their central system by 'their code' and additional authentication.

Process:

- In case of transactions initiated through merchant App, merchant will get transaction ID from their respective PSPs before initiating the transaction. The following process will be followed to ensure that proper merchant is initiating the transaction.
- On the merchant App when the customer selects the "Pay by UPI" option, the merchant will initiate request to its Acquiring Bank seeking a "Reference ID".
- In response the Acquiring Bank will provide "Reference ID" linked to transaction Amount to that merchant.
- Merchant App initiates an intent call with that "Reference ID" to the UPI enabled PSP App on the Mobile.
- The transaction comes from UPI enabled App to UPI system.
- UPI forwards to the Acquiring PSP for translation of merchant Virtual ID to actual Bank account details.
- Acquiring PSP before doing translation, will validate the "Reference ID" and amount for the Merchant.
- If reference ID matches, only then the further process will continue, otherwise transaction will be declined.
- Onus and liability of validating the transaction is with acquirer PSP.

e) Banks can tie up with the merchants for seamless download of the independent PSP app along with the download of the merchant app.

f) The UPI app should use the published intent invocation mechanism which can be used by any app on the phone.

- All applications on the mobile must only interact with UPI application (embedded or independent) via general deep linking spec (Android Intent, iOS URL Scheme, Windows URI Scheme etc.)
- When the customer is checking out to make payment and selects "Pay by UPI", it should open up options of entering Virtual address and/or invoke all the UPI certified Apps on the customer's mobile phone, so that customer can make payment through his/her preferred App.

g) Bank must ensure to conduct the independent IS audit for the built PSP app and the backend system.

h) The UPI app on the customer handset must not store any customer data unless encrypted. No authentication parameters should ever be stored on the UPI app or on UPI backend system.
i) PSP Bank must have the mechanism by means of hotlist the registered user's phone if lost/compromised with X hours of information by automated (self-service) means (e.g., ATM, internet banking, IVRS, etc.) as well as assisted means (call center, branch complaint, etc.).
j) Whenever acquiring a merchant/entities, bank must whitelist their payment address in the central UPI system (verified merchant address) so that whenever payments are made to verified merchant addresses, PSP application can show "address verified" icon/color. This is critical to minimize phishing attacks by imitating payment requests from well-known merchants/entities.

PSP app must show the transaction details (amount, transaction reference details, address to which payment is being made, clear indication if the merchant address is whitelisted in UPI system, and the payment confirmation details post payment) during and after the transaction is done for all recent transactions. PSP may also have the option of showing the last ten financial transactions in the "Transaction History" option. However, it is optional.

UPI Payment Options Standardization:

The PSP App has to mandatorily have an option of "*Pay by UPI*". Once the customer selects the "*Pay by UPI*" option on PSP App, the PSP App will initiate intent call to other PSP Apps present on Mobile device and the other option of entering the Virtual address is available, basis which a collect call is placed.

UPI Options on Merchant Application:

Merchants providing UPI option in their payment page shall use the standard terms and icons provided by NPCI like:

- ***Pay by UPI***

Icon/ Branding:

NPCI shall provide NPCI-UPI icons with standard functions like:

- Size of icons (Small/Large)
- Font
- Color usage etc.

This is critical to ensure common brand is used across websites and applications enabled with UPI.

Deep linking URL Spec:

NPCI has published the standard deep-linking URL spec (for intent/QR) from merchant application to PSP application.

For all the merchant transactions that are completed, the PSPs should send their customers a confirmation on the transaction along with 'Merchant Name' being send mandatorily.

Annexure –IV (Customer Registration Process)

Customer Registration Process on PSP App:

Step – I PSP Profile Creation (Registration):

1. The Customer discovers the PSP App on the platform specific App Store. The PSP is responsible for customer education.
2. Customer downloads the PSP application. Application has NPCI libraries embedded into it. Customer starts the configuration process
3. Customer specifies his choice of SIM which he wants to register on a dual sim device (in a single sim device, PSP app automatically fetches the mobile number and proceeds). An outward encrypted SMS from Customer's SIM should go to PSP server to fetch the Mobile Number of the customer. This SMS should be automated without the intervention of the customer. Through this process, the PSP shall not only do the device hard binding, but also strongly bind the Mobile Number with the device. This process has to be mandatorily followed.
4. The PSP app will request customers to enter further details. Then user is provided with the option of creating his UPI ID (Virtual Address) in the specified format.
5. The PSP may provide any additional features like App login credentials etc.

Step – II Registration for Bank Account:

1. The customer logs in to the PSP application & selects the option - "Add a Bank".
2. The customer specifies / selects the bank name with whom he is having the account with (This could be done through a drop down menu or by typing the bank name, of the banks certified on UPI & available in the PSP app).
3. This request is generated from the same mobile number registered by the customer during the registration process i.e. Step-I. The Mobile number "registered and authenticated" by the PSP also becomes the carrier of the information.
4. The Issuer Bank sends the account details including Account Number & IFSC registered for that mobile Number in a masked format to UPI. UPI sends this to the PSP which in turn passes this information to the PSP App.
5. The PSP stores the account details received by the Issuer Bank in its database. In this stage, the PSP Database contains the information such as Mobile Number of the customer, Virtual Address of the customer, Name of Customer on PSP App and Account no, Account & IFSC mapped to the Address, Device ID etc.
6. If the user has not setup UPI PIN, they can request UPI PIN to be setup during the account adding process. The user requests UPI PIN to be setup for the account.

Step –III Generate UPI PIN:

1. The customer logs into the PSP application and selects the option to “Generate UPI PIN”.
2. An OTP Request is generated by the PSP to UPI for the newly added account. UPI requests an OTP to the Issuer Bank on the basis of the account details entered by the customer. Then the issuing banks sends the OTP over SMS.
3. The customer is asked to enter the last 6 digits of Debit card number, expiry date, OTP in base 64 encoding. The new/preferred UPI PIN is also provided.
4. The issuing bank will only allow the UPI PIN to be set after validating both factors - Card details / OTP.
5. The PSP application sends it to the UPI and UPI sends it to Issuer bank by encrypting it with the public key using PKI.
6. The bank completes the request by decrypting the same with its Private Key and confirms the setting of the UPI PIN to UPI
7. UPI passes this information to the PSP which in turns notifies the customer.

The above mentioned steps are the broad guidelines under which the PSP needs to provide the facility of Customer Registration. However, the PSP is free to tweak the User Experience as long as it provides the above specified functionalities.

The PSP shall also provide the facility of change/update the mobile number registered with it by the customer at the time of registration after proper validations.

Annexure –V (Flows of Non-Financial Transactions)

PROCESS FLOWS OF NON-FINANCIAL TRANSACTIONS

A. Mobile Banking Registration Transaction

In case of a customer who has not been registered for mobile banking and has to generate UPI PIN:

Steps:

1. Customer initiates Mobile Banking registration process with PSP app.
2. Customer selects the bank account which he has registered in PSP App.
3. An OTP request is triggered by the PSP to NPCI along with the Account details, Mobile Number (captured during Profile creation) & Bank name. NPCI routes the request to the issuing bank.
4. Issuer Bank sends the OTP after proper validations at their end.
5. Customer enters the OTP (received in Step-4) into the PSP app along with last 6 digits of his debit card number & expiry date which is base 64 encoded prior to sending. The customer also enters the new UPI PIN of his choice.
6. PSP sends this transaction to NPCI & NPCI sends this to the Issuer Bank for verification
7. Issuer Bank validates all the details and confirms to NPCI with the relevant response
8. NPCI informs the same to the Payer PSP
9. Payer PSP confirms to the customer that the Mobile Banking Registration was successful

B. Set UPI PIN Transaction:

Set UPI PIN transaction allows the customer to set or change his UPI PIN using any PSP through UPI. For this, the customer requires details like last six digits of debit card, expiry date and OTP to authenticate. This transaction is to be facilitated only through PSP App.

Steps:

1. The customer logs in to the PSP application and selects the option to “Generate UPI PIN”
2. An OTP Request is generated by the PSP to UPI for the newly added account.
3. An OTP request is initiated to the Issuer Bank on the basis of the account details entered by the customer. The Issuer Bank sends the OTP in the registered mobile number
4. The customer enters the last 6 digits of Debit card number, expiry date, OTP – which is base 64 encoded. The desired/preferred UPI PIN is also provided in library.
5. The PSP application sends it to the UPI
6. UPI sends it to Issuer bank by encrypting it
7. The Issuer Bank decrypts it, verifies the details and sets the UPI PIN as requested and responds to UPI
8. UPI confirms the same to the Initiating PSP
9. PSP App confirms the setting up of new UPI PIN to the customer

C. Generate OTP Transaction:

Generate OTP transaction allows the customer to generate an OTP for any transaction related to UPI & his Issuer Bank. This transaction is triggered in Mobile Banking registration & Set UPI PIN transactions automatically. Below is the process flow:

1. Customer selects “Generate OTP” option in the PSP App
2. PSP App sends a Generate OTP request to UPI along with customers registered details like Account no, Mobile No and other details
3. UPI sends the same to the Issuer Bank

4. Issuer Bank sends the OTP to the customer in the registered Mobile Number.

Please note that for all the non-financial transactions where OTP is required as one input, this OTP has to be sent by the Issuer Bank to the customer through its own existing systems.

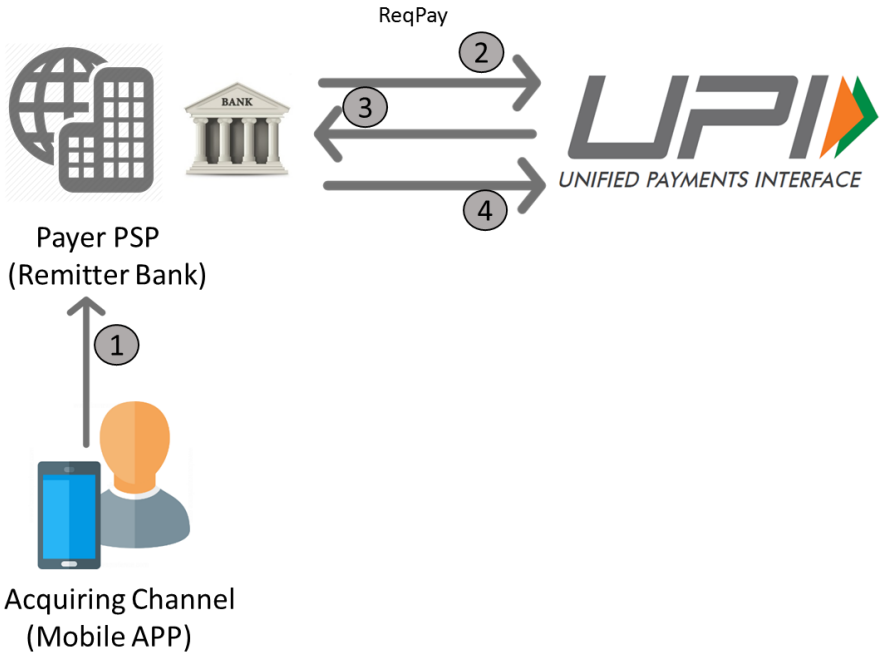
Annexure -VI (Flows of Financial Transactions)

PROCESS FLOWS FOR FINANCIAL TRANSACTIONS:

A. Transaction Flow when NPCI Libraries are used:

For Pay request & Collect Request initiated/authorised from Payer PSP App which is different from the Remitter Bank, NPCI libraries will be used for capturing the auth credentials.

1. Transaction is initiated from PSP App. Customer enters the relevant details and authorizes by entering the authorization credential (UPI PIN)
2. Payer PSP encrypts it using NPCI Public Key libraries & sends it to UPI
3. UPI decrypts it using NPCI Private Key sends it to the Remitter Bank by encrypting it with Bank's Public Key
4. Remitter Bank decrypts it using its Private Key & validates it, debits the customer's account and responds to UPI

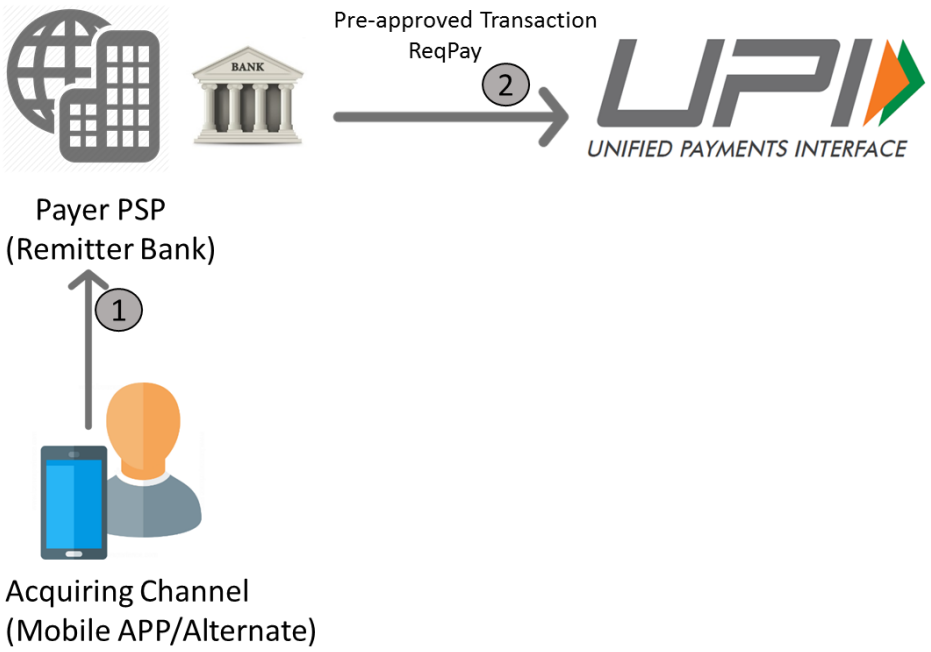


For illustration purposes, Step 3 & 4 is not provided in the process flows for non pre-approved transactions

B. Transaction Flow when NPCI Libraries are not used:

For transactions initiated from alternate channels, NPCI libraries will not be used for capturing the auth credentials and the bank can send it as pre-approved transactions(good funds) where the role of UPI wil be to process the Credit request. It can be initiated in cases where the Payer PSP &Remitter Bank are same entity. Below is the sample process flow.

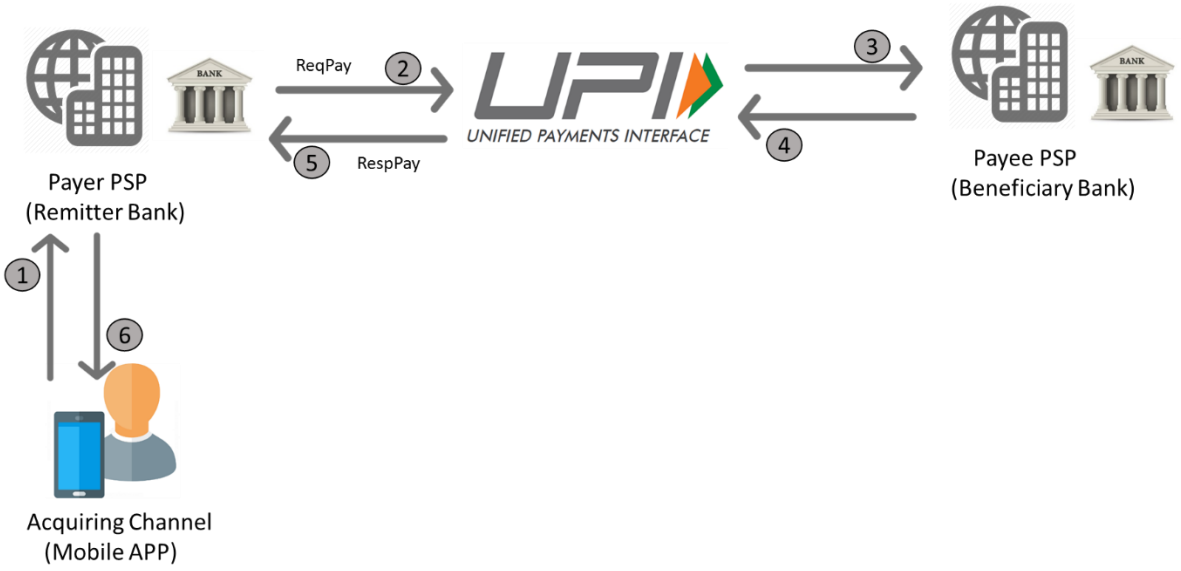
1. Transaction is initiated from PSP App. Customer enters the relevant details and authorizes the transaction. Remitter Bank debits the customer's account.
2. Payer PSP sends this transaction to UPI for processing the credit request.



C. Push Transactions with Mobile Number & MMID:

Steps:

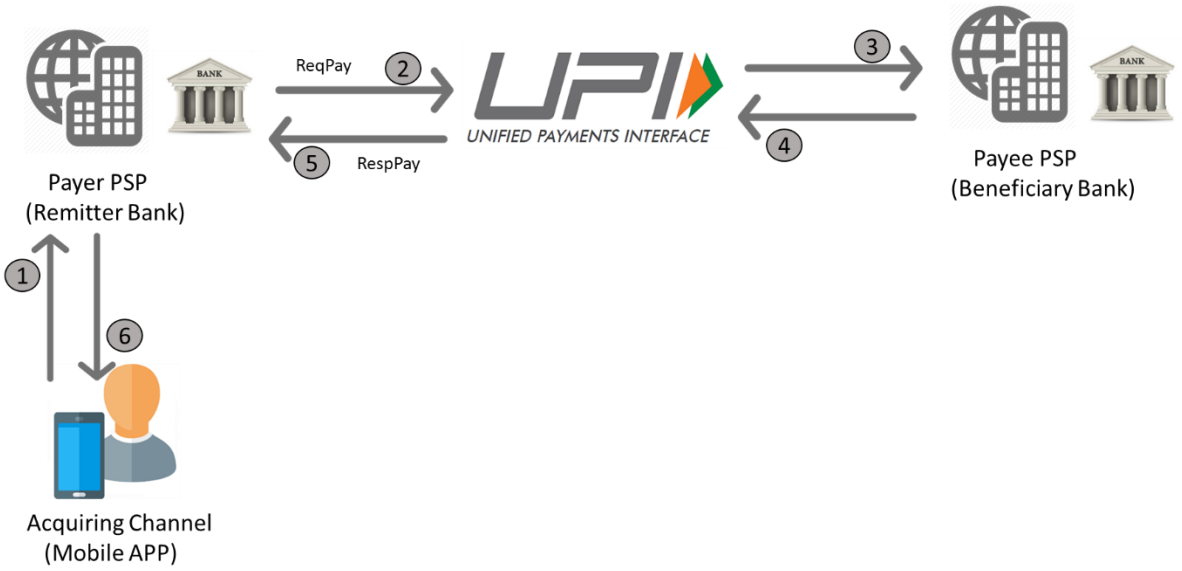
1. Payer enters the Mobile Number & MMID of the Payee in the PSP app and authorizes the payment by entering the UPI PIN.
2. Remitter Bank debits the customer account and sends the transaction to UPI along with the Payer account details and the Mobile Number & MMID of the Payee
3. UPI sends this transaction to the Beneficiary Bank
4. Beneficiary Bank credits the Payee account and responds to UPI
5. UPI responds to the Payer PSP for the successful transaction
6. Payer PSP confirms the same to the customer



D. Push Transactions with Account Number & IFSC:

Steps:

1. Payer enters the Account Number & IFSC of the Payee in the PSP app and authorizes the payment by entering the UPI PIN.
2. Remitter Bank debits the customer account and sends the transaction to UPI along with the Payer account details and the Account Number & IFSC of the Payee
3. UPI sends this transaction to the Beneficiary Bank
4. Beneficiary Bank credits the Payee account and responds to UPI
5. UPI responds to the Payer PSP for the successful transaction
6. Payer PSP confirms the same to the customer

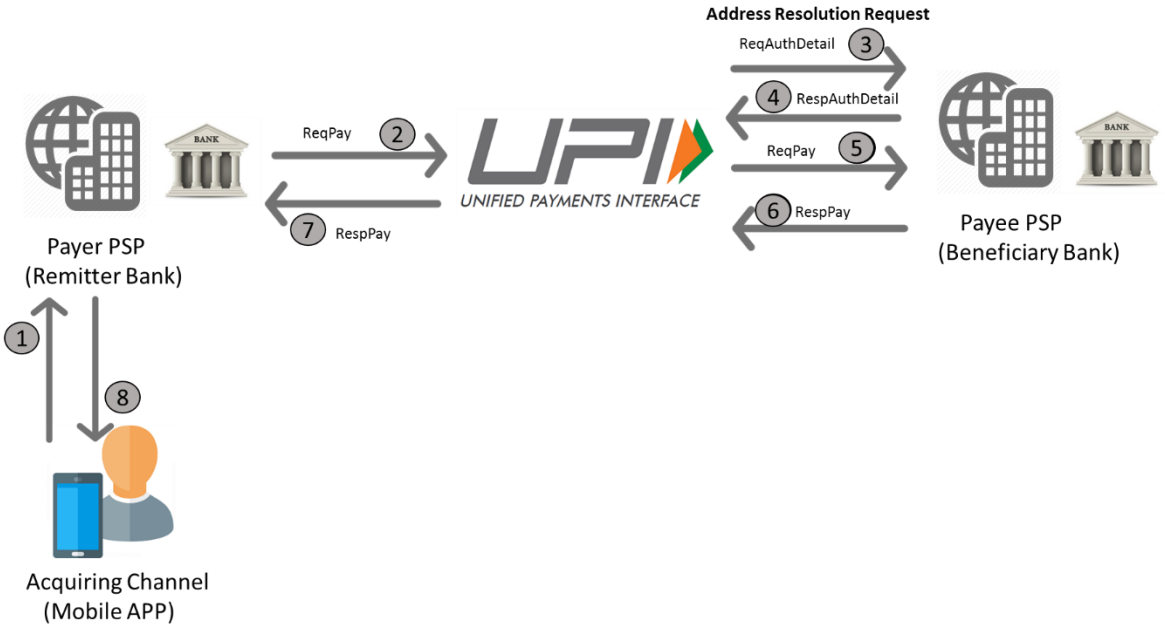


E. Transactions with UPI ID (Virtual Address)

TWO PARTY MODEL: (Payer PSP & Remitter Bank are one entity and Payee PSP & Beneficiary Bank are also one entity)

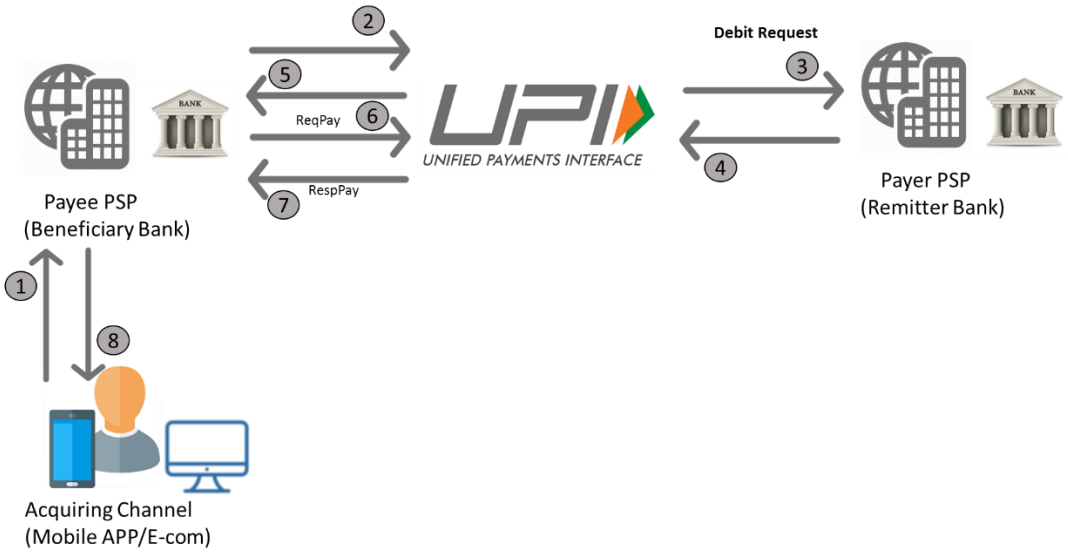
Pay Request:

1. Customer initiates a pay Request by entering the UPI ID of the Payee and UPI PIN
2. Payer PSP/Remitter Bank debits the customer's account & sends the *ReqPay* message to UPI
3. UPI routes it to the respective Payee PSP and send *ReqAuthDetails* message
4. Payee PSP identifies the Address and responds back with *RespAuthDetails* message.
5. UPI sends a credit request to the Beneficiary Bank.
6. Beneficiary Bank credits the customer's account & responds successful credit to UPI
7. UPI sends a successful confirmation to the Payer PSP
8. Payer PSP sends the confirmation to the customer



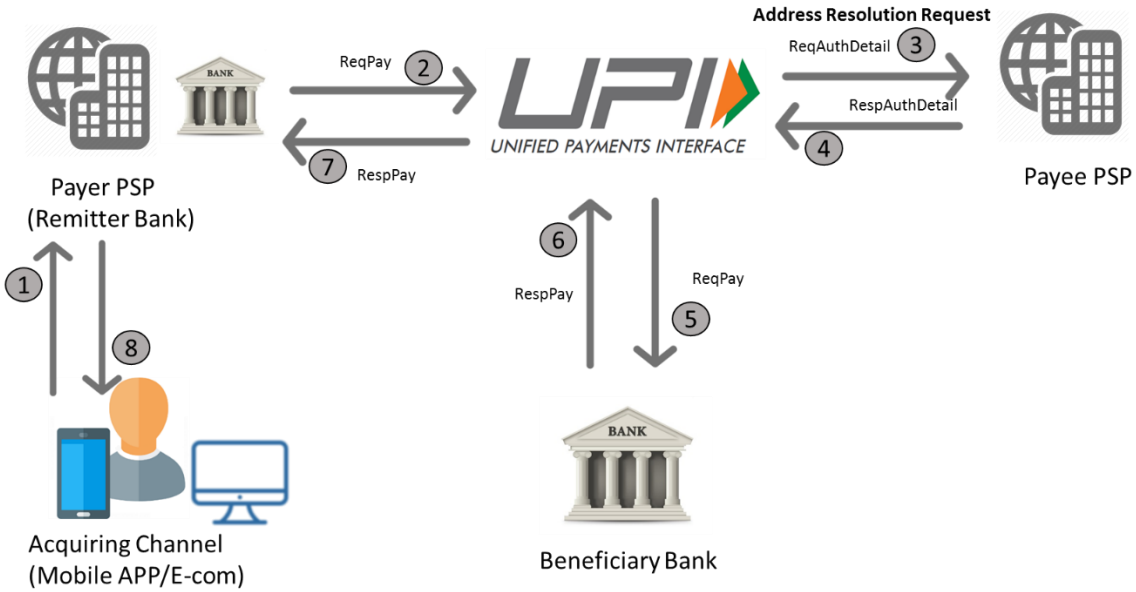
Collect Request:

1. Customer sends a Collect Request by entering the UPI ID of the Payer.
2. Payee PSP sends the *ReqPay* message to UPI
3. UPI routes it to the respective Payer PSP basis resolution of the handle
4. Payer PSP/Remitter Bank sends a notification to the Payer customer for authorization. Customer enters the UPI PIN & confirms the payment. Payer PSP debits the Payer's account and sends the *RespAuthDetails* message to UPI
5. UPI sends a Credit Request to Beneficiary Bank
6. Beneficiary Bank credits the customer's account & responds successful credit to UPI
7. UPI sends the *RespPay* message to Payee PSP
8. Payee PSP sends the confirmation to the customer



Three Party Model (Push: Remitter Bank & Payer PSP are one entity, Payee Bank & Beneficiary Bank are separate entities)

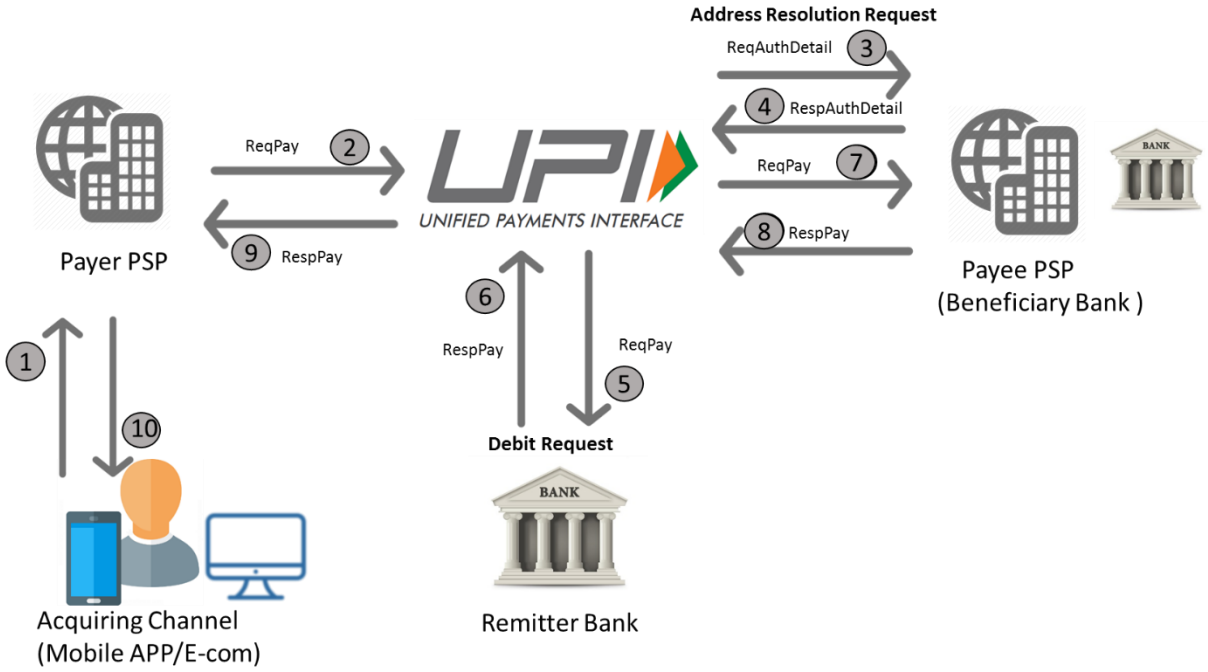
1. Customer initiates a Pay Request by entering the UPI ID of the Payee and UPI PIN.
2. Payer PSP/Remitter Bank debits the customer's account & sends the same to UPI
3. UPI routes it to the respective Payee PSP
4. Payee PSP identifies the Address and sends the relevant account information to UPI
5. UPI sends a credit request to the Beneficiary Bank
6. Beneficiary Bank credits the customer's account & responds successful credit to UPI
7. UPI sends the same to Payer PSP
8. Payer PSP sends a successful confirmation of the transaction to the customer



Three Party Model

(Push : Remitter Bank & Payer PSP are separate entities, Payee Bank & Beneficiary Bank are one enty)

1. Customer initiates a Pay Request by entering the UPI ID of the Payee and UPI PIN.
2. Payer PSP sends the Request Pay along with customer's credentials to UPI
3. UPI sends address resolution request (ReqAuthDetails) to payee PSP.
4. Payee PSP identifies the Address and sends the relevant account information to UPI
5. UPI sends the debit request to remitter bank.
6. Remitter bank sends the response after debiting the customer account
7. UPI sends a credit request to the Beneficiary Bank
8. Beneficiary Bank credits the customer's account and responds successful credit to UPI
9. UPI sends the same to Payer PSP
10. Payer PSP sends a successful confirmation of the transaction to the customer

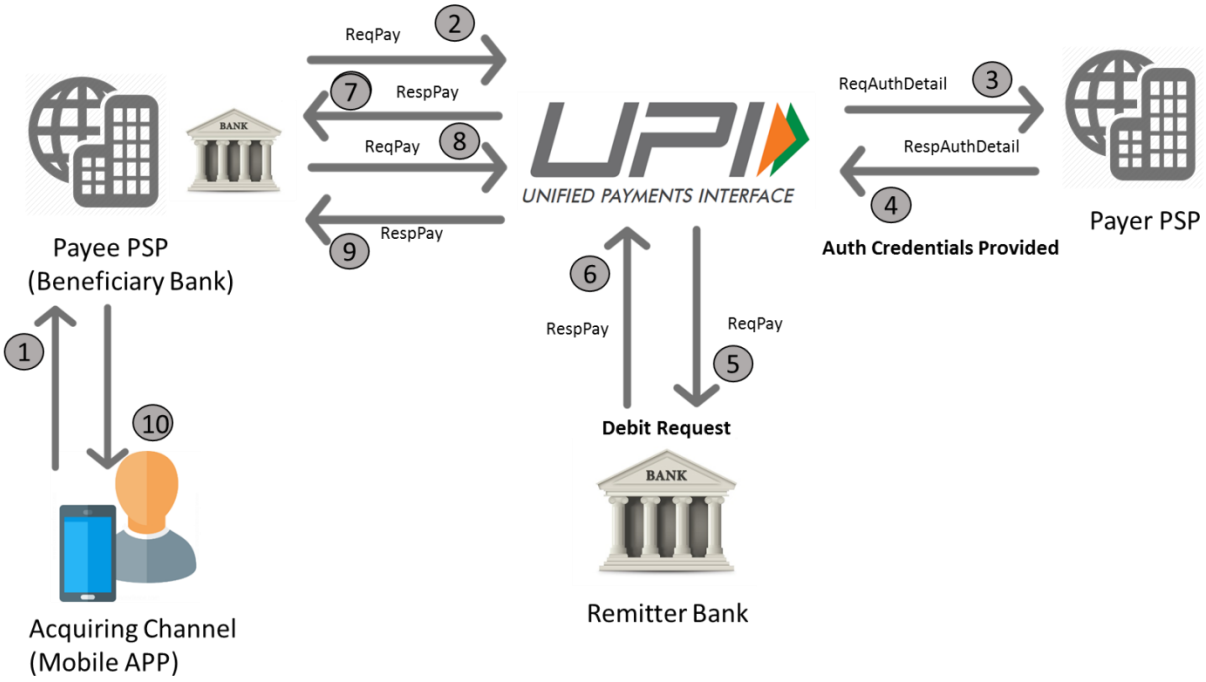


Three Party Model

(Pull : Remitter Bank & Payer PSP are separate entities, Payee Bank & Beneficiary Bank are one entity entity)

1. Customer sends a Collect Request by entering the UPI ID of the Payer.
2. Payee PSP sends the same to UPI
3. UPI sends it to the respective Payer PSP for address resolution and authorization
4. Payer PSP sends a notification to the Payer customer for authorization. Customer enters the UPI PIN & confirms the payment. Payer PSP sends the same to UPI
5. UPI sends the debit request to remitter bank.

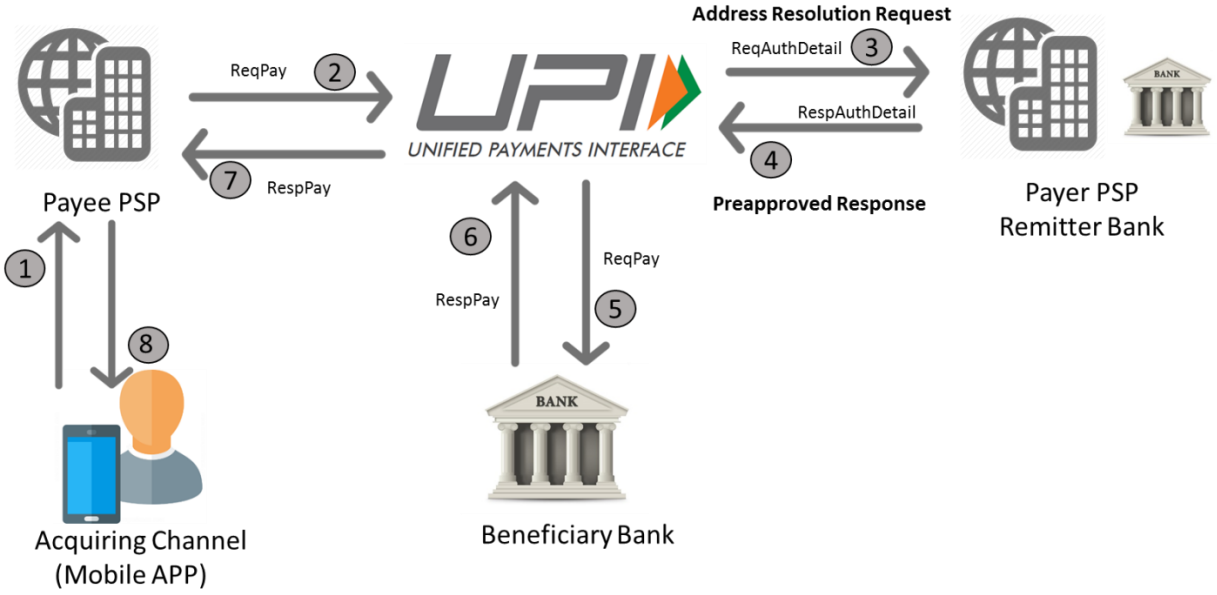
6. Remitter bank debits the Payer's account and sends the confirmation to UPI.
7. UPI sends the credit request to the Beneficiary Bank
8. Beneficiary Bank credits the customer's account and confirms the same to UPI
9. UPI sends the successful confirmation to the Payee PSP
10. Payee PSP sends the confirmation to the customer



Three Party Model

(Pull : Remitter Bank & Payer PSP are one entity, Payee Bank & Beneficiary Bank are separate entities)

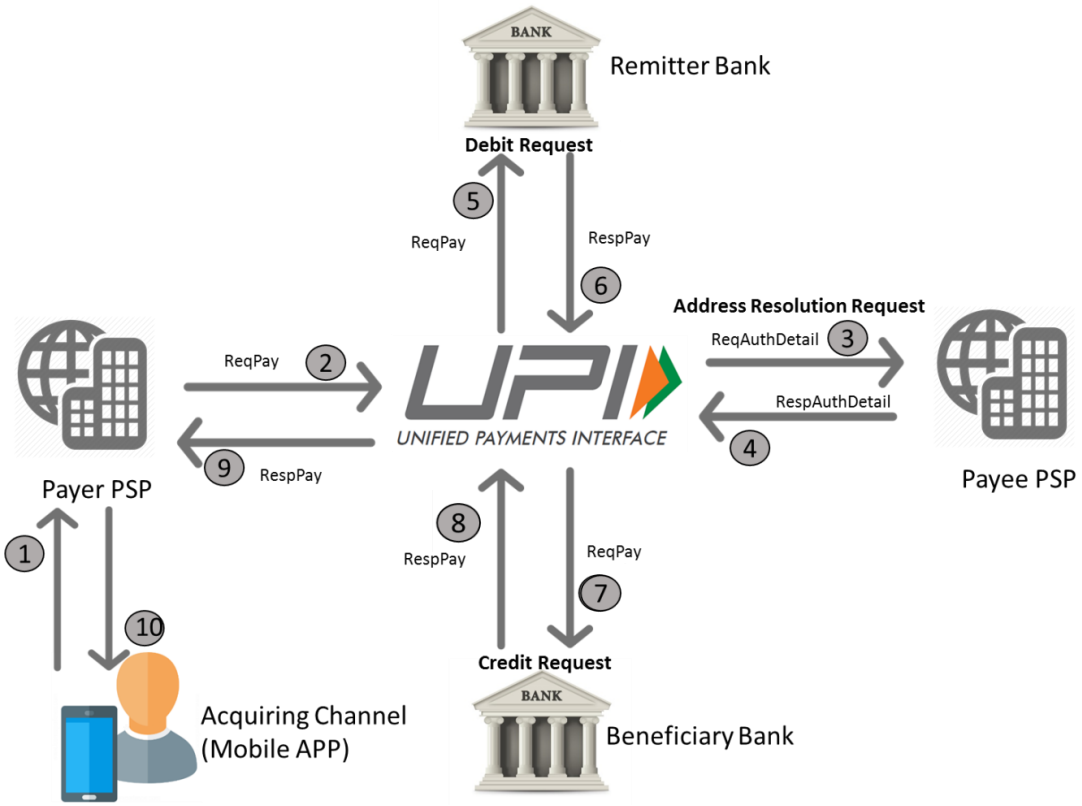
1. Customer sends a Collect Request by entering the UPI ID of the Payer.
2. Payee PSP sends the same to UPI
3. UPI sends it to the respective Payer PSP for address resolution and authorization
4. Payer PSP sends a notification to the Payer customer for authorization. Customer enters the PIN & confirms the payment. Remitter Bank debits customer account and sends response to UPI.
5. UPI sends the credit request to the Beneficiary Bank
6. Beneficiary Bank credits the customer's account and confirms the same to UPI
7. UPI sends the successful confirmation to the Payee PSP
8. Payee PSP sends the confirmation to the customer



Four Party Model

(Push : Remitter Bank & Payer PSP are separate entities, Payee Bank & Beneficiary Bank are separate entities)

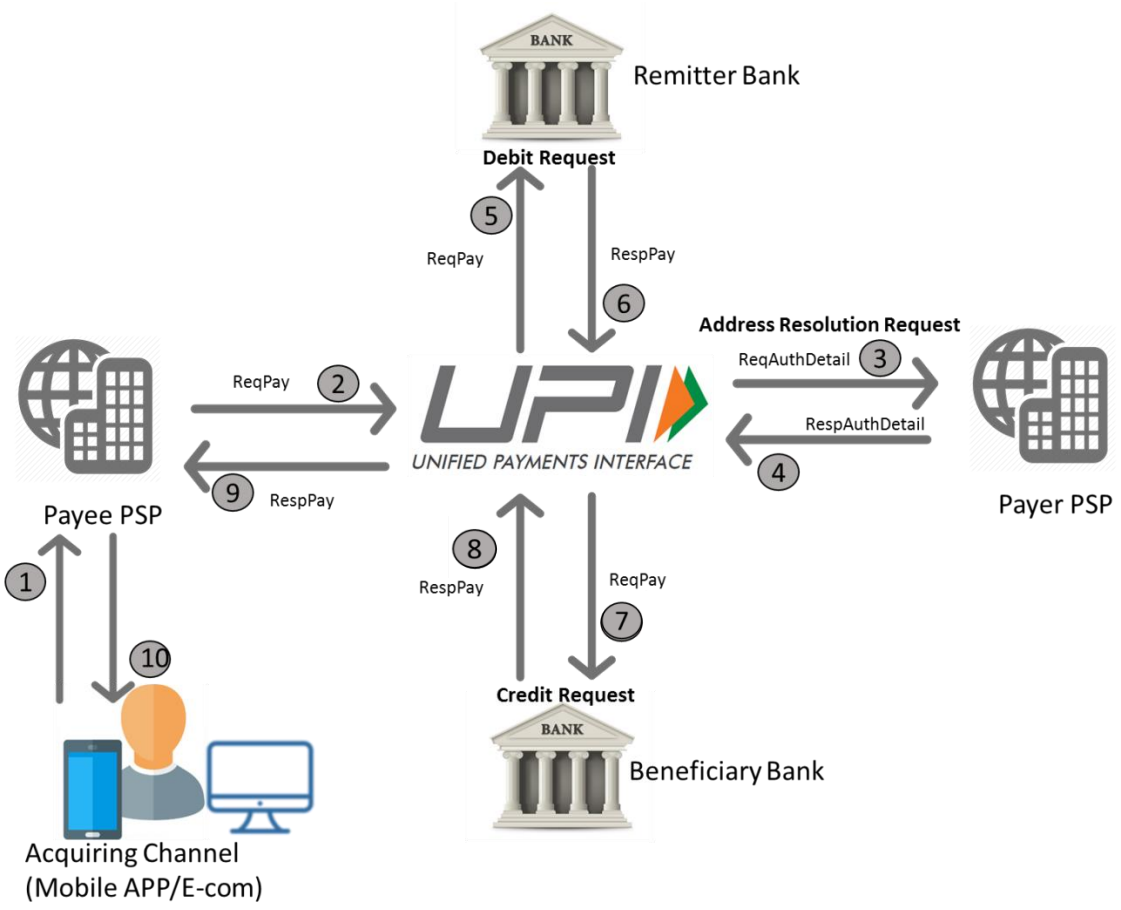
1. Customer sends a push Request by entering the UPI ID of the Payee
2. Payer PSP sends the same to UPI
3. UPI sends it to the respective Payee PSP for address resolution and authorization
4. Payee PSP sends relevant account details of the Payee to UPI
5. UPI sends the debit request to remitter bank.
6. Remitter bank debits the Payer's account and sends the confirmation to UPI.
7. UPI sends the credit request to the Beneficiary Bank
8. Beneficiary Bank credits the customer's account and confirms the same to UPI
9. UPI sends the successful confirmation to the Payer PSP.
10. Payer PSP sends the confirmation to the customer



Four Party Model

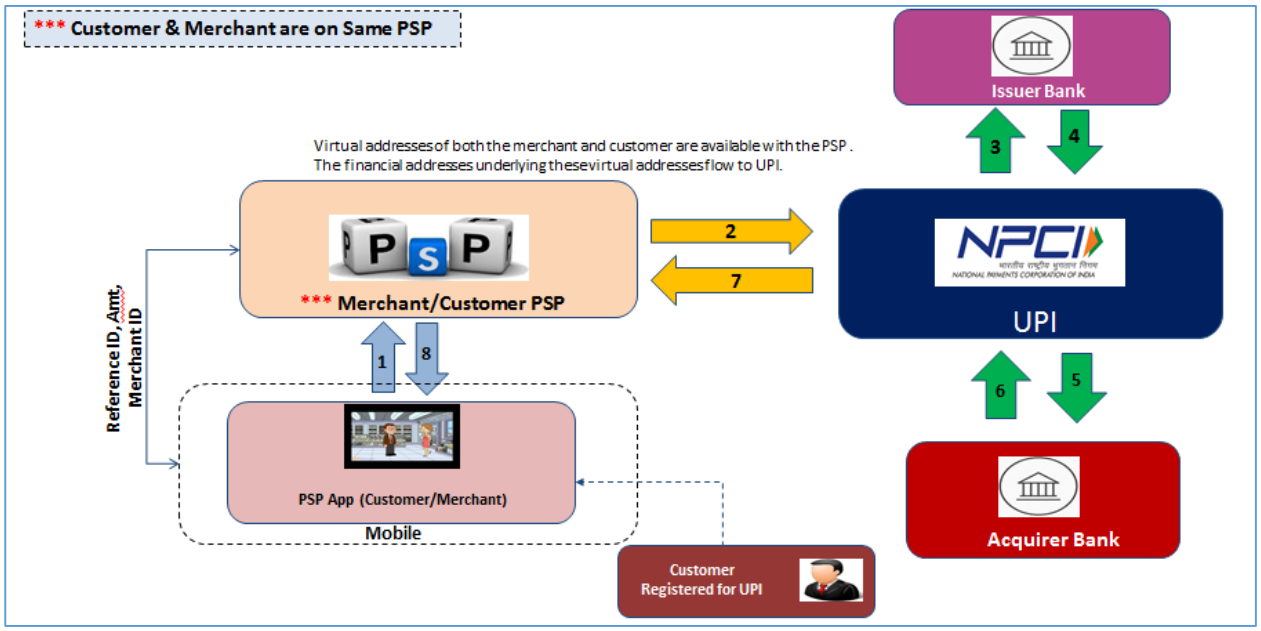
(Pull : Remitter Bank & Payer PSP are separate entities, Payee Bank & Beneficiary Bank are separate entities. It is applicable only for Person to Person transactions)

1. Customer sends a Collect Request by entering the UPI ID of the Payer.
2. Payee PSP sends the same to UPI
3. UPI sends it to the respective Payer PSP for address resolution and authorization
4. Payer PSP sends a notification to the Payer customer for authorization. Customer enters the PIN & confirms the payment. Payer PSP sends the same to UPI
5. UPI sends the debit request to Remitter bank.
6. Remitter bank debits the Payer's account and sends the confirmation to UPI.
7. UPI sends the credit request to the Beneficiary Bank
8. Beneficiary Bank credits the customer's account and confirms the same to UPI
9. UPI sends the successful confirmation to the Payee PSP. Payee PSP sends the confirmation to the customer

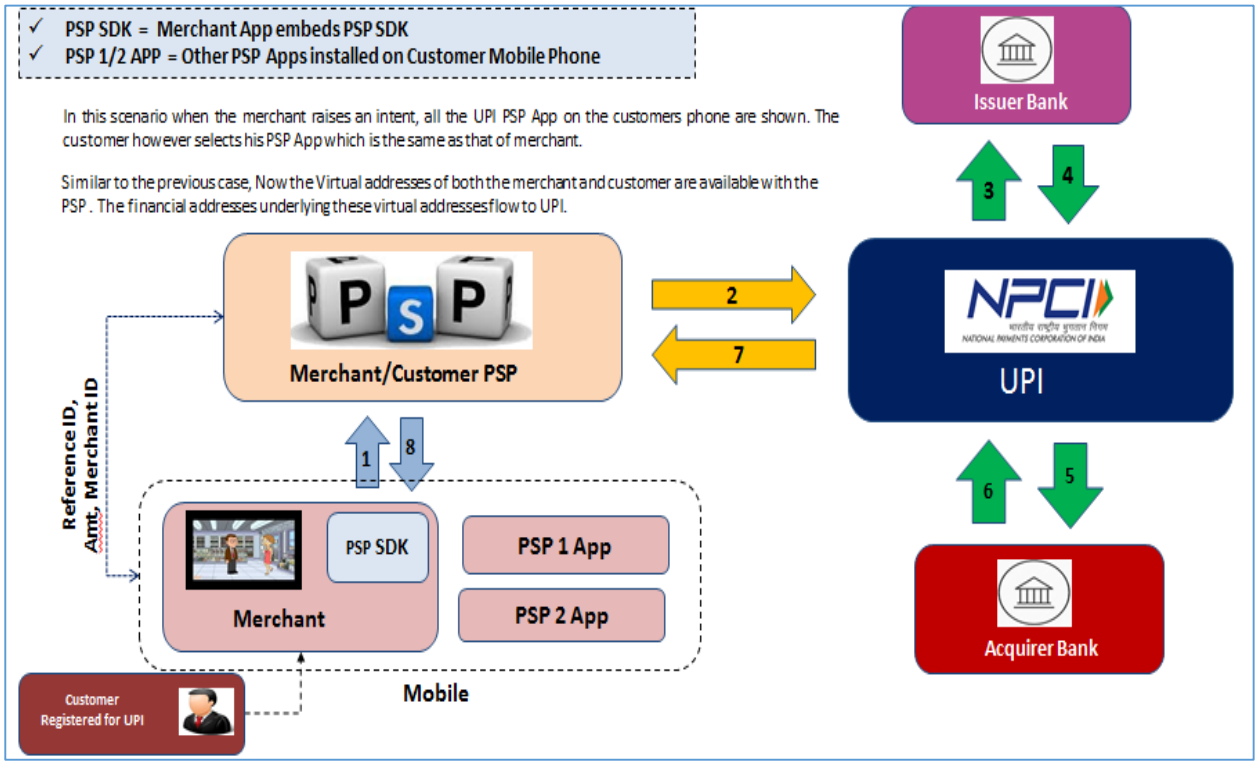


Merchant Transaction Flows:

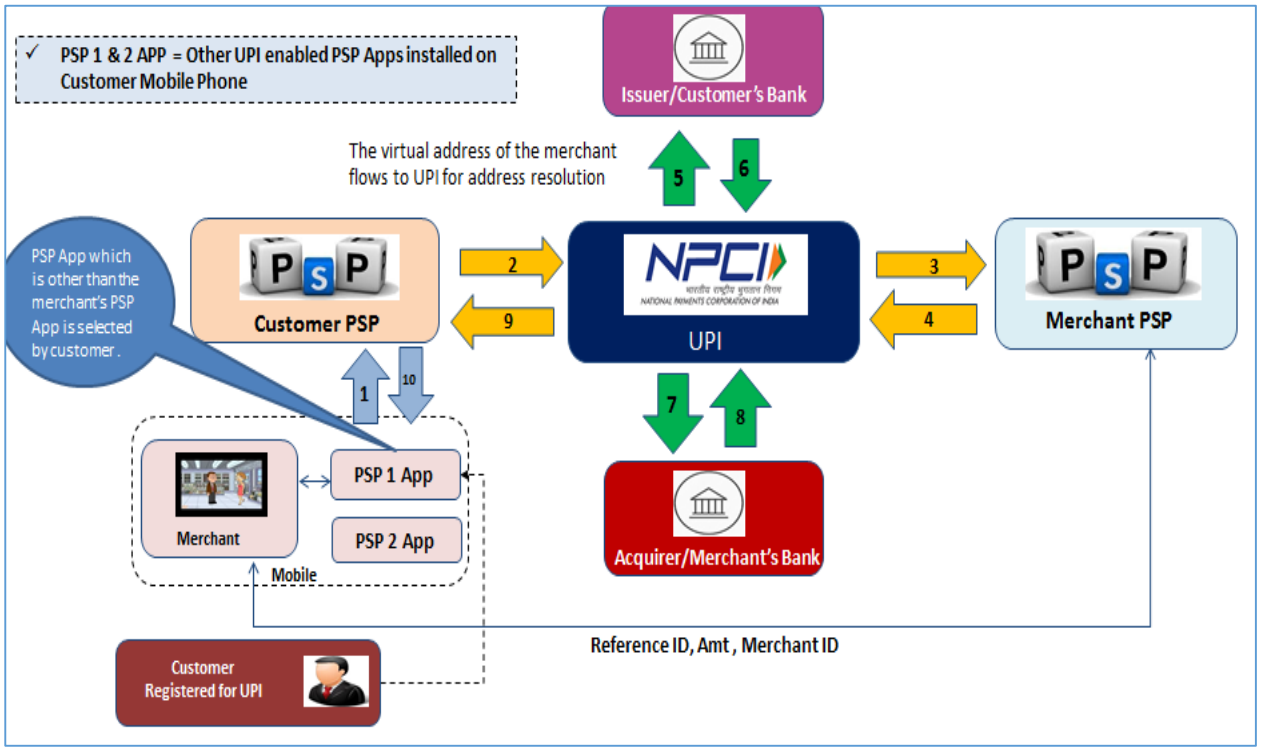
Case 1 : 3 Party Merchant Transaction - Customer & Merchant with Same PSP



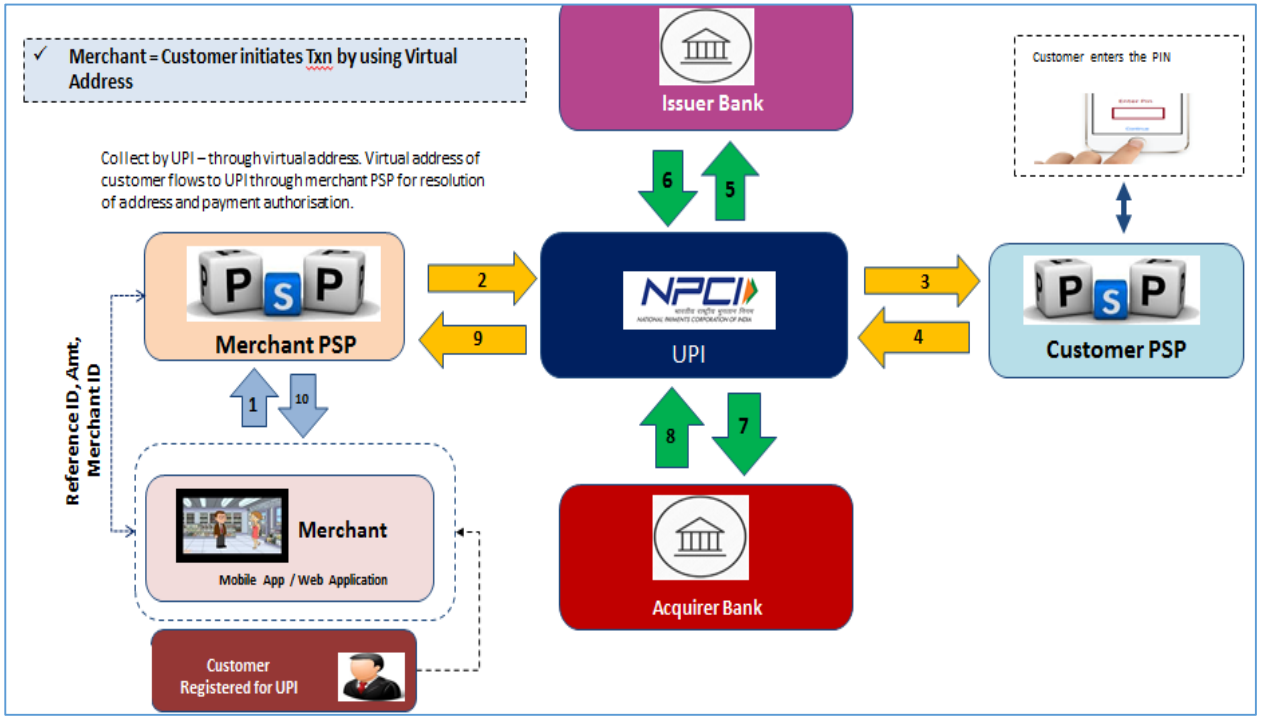
Case 2 : 3 Party Merchant Transaction - Customer & Merchant with Same PSP and PSP SDK embedded into Merchant App



Case 3: 4 Party Merchant Transaction - Customer & Merchant with different PSP



Case 4: 4 Party Merchant Transaction – Collect call based on UPI ID



Annexure -VII (Roles & Responsibilities of PSPs)

Roles and Responsibilities of the PSPs

a) The PSP shall ensure that its systems/ infrastructure remain operational at all times to carry out the said transactions. The PSP shall upgrade systems and message formats in a prompt manner, based on regulatory requirements or changes mandated by NPCI. The PSP shall adopt the data message standards as per standards of XML specified by NPCI from time to time

b) PSPs/Banks should benchmark their infrastructure (hardware & software) at their end for UPI to ensure to meet the UPI Benchmark criteria of processing 5millionper day & 500 TPS and 99.9% of uptime of services. Banks would be required to confirm in writing about this processing capacity before being declared Go Live.

c) The Bank/PSP should have the Disaster Recovery / Business Continuity management plan within 6 months of operationalization of the service.

d) The PSP shall integrate NPCI libraries in its PSP Application where the app in no way shall be able to capture sensitive customer data like Card Details, UPI PIN, Expiry Date, OTP etc. All these details shall be captured only by NPCI Libraries and the PSP app shall only facilitate it.

e) The PSP shall not share the data / information with any other third party, unless mandated by applicable law or required to be produced before a regulatory / statutory authority. In such exceptional cases wherein data / information is required to be shared under applicable law or required to be produced before a regulatory / statutory authority and to the extent permitted under such law / by such regulatory / statutory authority, the PSP shall provide a prior written intimation to NPCI & Bank of such disclosure.

f) The PSP shall undertake Device Hard Binding along with Mobile number verification.

g) As a pre-requisite, the PSP shall submit the third party audited report for the PSP App and PSP system to NPCI before go live and once in a year after go-live.

h) The PSP shall solely bear the cost/expenses relating to the establishment of connectivity between their switch and the UPI.

i) The PSP hereby agrees to abide by the dispute management rules and regulations specified by NPCI in document UPI Settlement Procedure.

j) The PSP shall not disclose, reveal, publish and/or advertise any material information relating to operations, membership, software, hardware, intellectual property etc. of NPCI without its prior written consent except and to the extent as may be required in the normal course of its business.

k) The PSP further agrees that NPCI reserves the right to terminate the membership of the PSP at any time in the event of non-compliance of any of the terms herein and/ or at its sole discretion for any other reason whatsoever.

l) The PSP shall provide access to NPCI to any records maintained by the PSP including but not limited to records of Transactions or dispute / problem resolution, within 2 days of a request being placed in this regard by NPCI.

m) The PSP shall ensure that adequate funds are available in its RTGS Settlement Account, after making necessary provisions for applicable holidays, to ensure seamless settlement.

n) The PSP shall ensure that the communication between the PSP switch and the UPI shall be encrypted using suitable mechanism and that UPI PIN shall not be disclosed or retained by it or its employees, service providers under any circumstances.

o) The PSP shall ensure that all the personnel employed/engaged by the PSP in this regard are adequately qualified and receive suitable training to ensure compliance with standards that are laid down by NPCI and the regulatory authorities in this regard.

p) PSP shall be solely responsible for UPI issuance and management of services to its customers and shall also handle Account holder's queries and complaints pertaining to other member on the UPI platform.

q) PSPs should maintain round-the-clock connectivity of their network for the UPI services with an uptime of 99.9%

r) Security of transactions between the mobile handset and the bank's server should be the responsibility of the remitting and beneficiary member.

s) The PSP will be liable for all compliance by its outsourced Technology Service Providers/sub-members for all the guidelines issued by NPCI, RBI, Government of India, and all other relevant regulatory authorities. The PSP should inform NPCI in case of cessation of the membership arrangement between the PSP and its outsourced Technology Service Providers/sub-members with a prior notice of at least three months through necessary communication channels that are deemed appropriate as per the compliance mandate

t) PSP will ensure that before adding a new outsourced Technology Service Providers/sub-member under the sponsorship product, due diligence is completed with respect to the outsourced Technology Service Providers/sub-members' system infrastructure and the due diligence report is submitted to NPCI at the time of obtaining permission from NPCI for including such outsourced Technology Service Providers/sub-members into the UPI Network. PSP may conduct this due diligence annually or as per directions from their board

u) If PSP fails to fulfil its settlement commitment towards UPI transactions, resulting in member banks or NPCI incurring any loss in the form of settlement, the transaction fees or switching fee respectively in such cases has to be borne completely by the respective Bank/PSP. In such a case, funds available in the bank's settlement account will be used to settle the claims of UPI member banks

v) PSP would be held accountable for making good the liability accruing to NPCI or any Issuing Member bank on account of any event that causes an operational risk with a financial impact (including negligence, fraud, omissions among others) by its outsourced Technology Service Provider/sub-member. PSP should also report to NPCI, any incidents causing operational risks encountered by its outsourced Technology Service Provider/sub-member with respect to UPI transactions. The Fraud Reporting needs to be done in the NPCI provided template.

w) PSP would be responsible for ensuring submission of the NPCI compliance form and for monitoring the implementation of best practices prescribed by NPCI, and/or any other document that shall be laid down in the UPI Procedural Guidelines and as amended from time to time."

x) PSP would be responsible for its outsourced Technology Service Provider/sub-member settlement and dispute management. PSP will provide the reports to its sub-member for reconciliation. PSP would raise the dispute on behalf of its sub-members in the stipulated time as per the UPI Procedural Guidelines and as amended from time to time.

y) Outsourced Technology Service Providers/sub-members needs to follow the RBI mobile banking guidelines and NPCI's UPI procedural guidelines mandatorily and any such other regulatory guidelines as may be applicable from time to time.

z) PSP should check the frequency of transaction initiated by one customer from one mobile No and take required actions basis their internal risk profiling. Further, the risk profiling from the PSP and the Issuers should also check and assess the following parameters, in addition to all the other parameters as per the internal risk processes of the issuer & PSPs:

   i. Velocity / Frequency of the transactions per customer. The check on the transactions should preferably be real-time.

ii. The Profiling of the customer should also be checked by the PSP & the Issuers.

aa) PSP should place a moratorium of at least Two (2) Years in case a UPI ID (VPA) is deactivated/deregistered by customer.

The Bank/PSP should bring any of the below to the immediate notice of NPCI:

a) Any of its outsourced Technology Service Providers/sub-members violating laws pertaining to Anti-Money Laundering (AML) as defined and articulated under the Prevention of Money laundering Act (PMLA) 2002

b) Any violation of regulation as issued by the Financial Intelligence Unit, Government of India, and the Reserve Bank of India in connection to KYC/AML/CFT

c) Any involvement of its outsourced Technology Service Providers/sub-members in any suspicious transactions and frauds. Fraud reporting has to be in the NPCI provided template

d) Any of its outsourced Technology Service Providers/sub-members resorting to any unfair practices relating to their participation in any NPCI products

e) Any of its outsourced Technology Service Providers/sub-members not adhering to the rules, regulations, operational requirements, and instructions of any NPCI products

f) Any suit filed in any court of law or arbitration where a sub-member and NPCI have been made parties

g) Any fine and/or penalty imposed by a regulator on the PSP/outsourced Technology Service Providers

Due Diligence of Technology Service Providers:

PSP should conduct due diligence on the potential technology service provider before selecting and entering into any form of outsourcing relationships. A bank/PSP should not rely solely on experience with or prior knowledge of the third party as a proxy for an objective, in-depth assessment of the third party's ability to perform the said activities in compliance with all applicable laws and regulations and in a safe and sound manner. The PSP should consider the following during due diligence:

a) Legal and Regulatory Compliance
b) Financial Condition
c) Business Experience and Reputation
d) Qualifications, Backgrounds, and Reputations of Company Principals
e) Risk Management
f) Information Security
g) Incident-Reporting and Management Programs
h) Business Continuity Program

The above are indicative activities only and the Principal PSP/Bank may do all the possible due diligence as per their internal risk assessment and policies.

Annexure –VIII (Roles & Responsibilities of Sub-Members)

Roles and Responsibilities of the Sub-Members

a) All sub-member banks participating in the UPI network must sign a non-disclosure agreement with NPCI.

b) All sub-member banks must sign a tri-partite agreement with NPCI and main member to abide by and comply with UPI rules and regulations.

c) Each member should treat UPI related documents as strictly confidential and should not disclose them to outsiders without prior written permission from NPCI, strictly on need basis and to the extent permitted by NPCI.

d) Sub-member bank has to submit NPCI Compliance form on a periodic basis to NPCI. A copy of this form should be submitted to the sponsor bank during the phase of joining the UPI network and subsequently, as per periodicity defined by NPCI.

e) All sub-member banks participating in the UPI network to comply with data integrity and data storage / data security laws as applicable in India.

f) NPCI would be entitled to conduct an audit of the sub-member bank's UPI platform and IT facility either on its own or by an independent agency periodically.

g) Sub-member should submit periodic reports, statements, certificates, and other such documents as may be required by the NPCI and should comply with such audit requirement as may be framed for the purposes of their audit.

h) Sub-member should indemnify NPCI and keep it indemnified against any loss/damages suffered by it, whether legal or otherwise, arising due to its non-compliance with the UPI Procedural Guidelines.

i) Disclosure of any sensitive information by sub-member banks pertaining to UPI network to parties not involved in the UPI network will be treated as breach of trust and could invite legal action. This will also mean termination from further participation in the UPI network. However, a sub-member bank may disclose such confidential information to its employees, officers, consultants, or agents on a need-to-know basis to the extent that such disclosures are required to exercise its rights and perform its obligations.

j) All sub-member banks should comply with statutory and RBI regulations. NPCI reserves the right to obtain assurance from sub-member banks through a certification process on such compliance.

k) Transaction between sponsor bank and sub-member will be considered as "Off–Us" and should be routed through NPCI UPI System

l) As UPI is a round-the-clock, real time fund transfer service, it is mandatory for a sub-member bank to credit the customer account in real time. Further, this service should be available for round-the-clock all through the year. Sub-member should reconcile and submit the adjustments action to sponsor bank within two hrs after settlement is performed by NPCI

Annexure –IX (Roles & Responsibilities of PSPs in SDK model)

a) The App provider shall provide the required documentation including data flow diagram, security details to PSP bank and NPCI.

b) The PSP bank must ensure that its board approves such PSP SDK arrangement, since all the liability arising in case of any data breach, wrong authentication etc. is borne by the PSP bank. The board resolution shall be submitted to NPCI as part of onboarding process.

c) The PSP bank shall continue the authentication, encrypted SMS OTP verification as detailed out in the current PSP SDK guidelines.

d) PSP bank must ensure that the system and app audit is performed to ensure data integrity, encryption and the app security. This audit shall be done on annual basis.

e) PSP Bank shall have the full right to conduct audit on the third party App provider infrastructure, systems and application, database and security practices including access/ user/ incident/ management at their end for components related to UPI.

f) PSP Bank shall ensure that it will facilitate RBI, NPCI or any other formally appointed agencies of RBI/ NPCI, to access the data and carry out audits of Bank and third party app provider, as and when required.

g) The PSP bank must provide all the documentation and audit reports as listed by NPCI (by Cert In empaneled auditors) before go live of any such third party app on single SDK model.

h) The PSP bank must have agreement with third party App provider for any liability arising out of data breach/fraud/compromise at the app or third party app provider's system. Further the agreement/ arrangement between bank and third party app provider must include compliance to Data Privacy, Informational Privacy (as aspect of Right to Privacy), IT act, Payment and Settlement System Act, UPI Procedural guidelines or any such future law and guidelines issued by government of India, RBI, any other regulator in India and NPCI.

i) The PSP bank must provision for customer to raise disputes on the app and should ensure complaint management processes as per UPI Operating and settlement guideline and Operating Circulars. The third party app provider and PSP bank must ensure the customer service in case of disputes as prescribed by UPI procedural guidelines and RBI customer service guidelines issued time to time.

j) The call center number (toll free number in India) must be prominently displayed on the app for customer service.

k) PSP Bank should ensure that all UPI customers could participate to use this app & choose any bank account from the list of Banks available on UPI platform.

l) PSP Bank shall ensure that third party app provider shall require an exclusive permission from NPCI & PSP bank for sharing individual UPI transaction data and UPI related customer details with any other third party including its own Parent, subsidiaries and subsidiaries of parents other than entities such as - Indian Government/Indian intelligence/Indian law enforcement agencies/Indian regulatory bodies.

m) PSP Bank shall ensure that the third party app provider shall take explicit customer consent for using transaction data for themselves and/or PSP bank for the purposes such as - Cross-Sell/ Promotions/ Offers/ Value Added Services/Increasing Transactions/Better User Experience/such other purposes as shall be approved by NPCI in writing.

n) PSP Bank shall ensure that the third party app provider will ensure that no application version with significant UPI related changes shall go live without a formal assessment and approval, excluding minor changes and bug fixes. Any major change can be qualified as major functionality change in UPI offering OR security related change that shall require audit and be governed basis the arrangement between PSP Bank &third party app provider.

o) PSP Bank shall ensure that the details of beneficiary customer such as account number and CBS name shall not be used by third party app provider other than for transaction processing.

p) For instances wherein the third party app provider's data resides outside the country, either the SOC 2 compliance audit report or a reputed third party auditor's report as per scope defined by NPCI needs to be submitted to NPCI and PSP bank.

q) PSP Bank will give reasonable assurance or undertaking directly by the PSP Bank or from third party app provider that the app is adequately secured.

Annexure -X (Roles & Responsibilities of PSPs in Multi bank model/API approach)

a) The App provider shall provide the required documentation including data flow diagram, security details to PSP bank and NPCI.
b) The PSP bank must ensure that its board approves such multi-bank arrangement, since all the liability arising in case of any data breach, wrong authentication etc. is borne by PSP banks. The board resolution shall be submitted to NPCI as part of onboarding process.
c) All data exchange between the app, the app providers system and PSP bank shall be through a secure channel.

d) The PSP bank shall continue the authentication, encrypted SMS OTP verification as detailed out in the current PSP SDK guidelines.

e) It is assumed that the data for device binding shall come from the app and the third party app provider. The bank must ensure that the system and app audit performed to ensure data storage/integrity, encryption and the app security. This audit shall be done on annual basis.

f) PSP Banks shall have the full right to conduct audit on the third party App provider infrastructure, systems, application and database for components related to UPI.

g) PSP Bank shall ensure that it will facilitate RBI, NPCI or any other formally appointed agencies of RBI/ NPCI, to access the data and carry out audits of Bank and third party app provider, as and when required.

h) The PSP bank must have agreement with third party App provider for any liability arising out of data breach/fraud/compromise at the app or third party app provider's system. Further the agreement/ arrangement between bank and third party app provider must include compliance to Informational Privacy (as aspect of Right to Privacy), IT act, Payment and Settlement System Act, UPI Procedural guidelines or any such future law and guidelines issued by government of India, RBI, any other regulator in India and NPCI.

i) The PSP bank must provision for customer to raise disputes on the app and should ensure complaint management processes as per UPI Operating and settlement guideline and Operating Circulars. The third party app provider and PSP bank must ensure the customer service in case of disputes as prescribed by UPI procedural guidelines and RBI customer service guidelines issued time to time.

j) The call center number (toll free number in India) must be prominently displayed on the app for customer service.

k) PSP Bank should ensure that all UPI Customers could participate to use this app & choose any bank account from the list of Banks available on UPI platform.

l) PSP Bank shall ensure that that third party app provider shall require an exclusive permission from NPCI & PSP bank for sharing individual UPI transaction data with any other third party including its own Parent, subsidiaries and subsidiaries of parents other than entities such as - Indian Government/Indian intelligence/Indian law enforcement agencies/Indian regulatory bodies.

m) PSP Bank shall ensure that Customer can get the handle of the bank where he/she has their account, by default; and for or all other bank customers (i.e. other than the participating banks) this allocation happens at the back-end on a fair distribution method as agreed between PSP Bank and the third party app provider. Any changes in the handle allocation rule shall require explicit approval of NPCI. In case the handle of the default bank cannot be made available for technical reasons, the handle may be allocated through the fair allocation method.

n) PSP Bank shall ensure that the customer has the choice of changing the handle later through appropriate enablement in the app.

o) PSP Bank shall ensure that the third party app provider shall take explicit customer consent for using transaction data for themselves and/or PSP bank for the purposes such as - Cross-Sell/ Promotions/ Offers/ Value Added Services/Increasing Transactions/Better User Experience/such other purposes as shall be approved by NPCI in writing.

p) PSP Bank shall ensure that the third party app provider will ensure that no application version with significant UPI related changes shall go live without a formal assessment and approval, excluding minor changes and bug fixes. Any major change can be qualified as major functionality change in UPI offering OR security related change that shall require audit and be governed basis the arrangement between PSP Bank &third party app provider.

q) PSP Bank and/or third party app provide shall not route any interbank transactions within themselves.

r) PSP Bank shall ensure that the details of beneficiary customer such as account number and CBS name shall not be used by third party app provider other than for transaction processing.

s) For instances wherein the third party app provider's data resides outside the country, either the SOC 2 compliance audit report or a reputed third party auditor's report (CERT IN) as per scope defined by NPCI and banks needs to be submitted to NPCI and PSP banks.

t) PSP Bank will give reasonable assurance or undertaking directly by the PSP Bank or from third party app provider that the app is adequately secured.

Annexure –XI (Roles & Responsibilities of TSPs)

This may please be read in conjunction with **Annexure XII (PSP Role)**

Roles and Responsibilities of the TSPs

a) TSP should ensure that all transactions routed to UPI should comply with the message specifications, as specified by UPI, based on XML message formats

b) Each TSP will be provided with a report on the state of operations, including a description of the systems of internal control and any deficiencies.

c) Each TSP should also proactively conduct annual internal audits of itself and its processing agents, if any, on a regular basis to comply with the UPI Procedural Guidelines

d) Each TSP participating in the UPI Network through its Sponsor PSP is expected to maintain round-the-clock connectivity of their switch for the UPI services with an uptime of 99.9%

e) All TSPs participating in the UPI network through their Sponsor PSPs must comply with data security / data integrity laws as applicable in India. They must be compliant with the applicable security regulations as defined for UPI and/or guidelines as issued by RBI & NPCI from time to time. In addition to it, any other regulations for data storage of payment details will also be adhered to.

f) Each PSP should submit periodic reports, statements, certificates, and other such documents as may be required by the NPCI from time to time. Furthermore, the PSP should comply with such audit requirements as may be framed by NPCI for the purposes of their audit.

Annexure XII (UPI PSP ROLE)

PSP, as per the extant approval from the RBI are Banks only, regulated by RBI under Banking Regulations Act 1949 and should be authorized by RBI for providing mobile banking service. The PSP role along with various guidelines including merchant acquiring guidelines, handle guidelines etc. for UPI are defined under the following heads along with a brief explanation:

1. Ownership of data:

Under UPI, Security & integrity of the data will be the responsibility of the PSP/Bank even in cases where the Bank/PSP & the outsourced technology service providers are different entities. Therefore, it is recommended that the PSP/bank does full due diligence of the outsourced technology service provider as they are dealing with sensitive customer data.

Only the PSPs can provide the UPI App for customer On-boarding. An outsourced entity having an experience in the customer front end may create an App for the Bank, which may be used by the PSP Bank for on-boarding the customers. The App is however in the Bank's name and all data of the customer stays with the Bank only.

2. Acquiring Merchant /Customer:

Under UPI, there are broadly 2 types of transactions viz. Peer to Peer (P2P) and Merchant Payments (P2M). In both the cases, PSP bank should ensure that while the bank's technology platform can be outsourced, its functions 'as a PSP' cannot be outsourced. It is also recommended that PSP's Central Application must reside in Bank's own Data Centre and in under no condition, the PSP customer data to be shared with Merchant App.

In case wherein the Bank / PSP embeds the Common Library in the Merchant App through an SDK provided by PSP Bank, PSP has to ensure that all sensitive customer data must reside at PSP and not with merchant.

The acquiring function of customer should remain with PSP Bank and not with merchant. It has been amply clarified that the outsourcing is permissible only in cases where the bank does not have an interface for UPI and can take support of the outsourced Technology providers who can provide for the interface basis the 'Outsourcing model'.

The PSP bank shall ensure that all the financial and Non-financial transactions are provided through the front end PSP App to the end customer as mandated from time to time.

3. PSP Liability

a) Authentication

The onus of validation of the first factor of authentication of customer credentials including Mobile device fingerprinting or any other material information which identifies the customer lies with the PSP. It has been mandated that the PSP send an outward encrypted SMS from the customer's mobile number to the PSP interface for device fingerprinting. This SMS has to be completely automated with no intervention from the customer. Only after proper validation of the customer identification and customer authorization credentials, the PSP will offer UPI services and allow the account to be operated under UPI. The Banks/PSPs shall also own the full liability should the Common library be compromised in case of common library integrated with PSP App or Merchant App through PSP. It has to be noted that for all subsequent financial transactions done by the customer, the onus of authenticating the first factor (hard bound Mobile device with mobile number) is on the PSP alone. Accordingly, the PSP has to ensure proper device binding with the mobile number.

The PSP should also ensure that the most recent of the Common Library versions is available in the App and there are adequate provisions to update the latest version of UPI Common Library released by NPCI. The PSP also has to ensure that the guidelines with regard to invoking of the NPCI Common library for capture of PIN is available as mandated.

b) Data security

Under UPI, the PSP shall be liable whether for any loss or corruption (whether direct or indirect) of data or information. The PSP will be liable for loss on account of breach of data (whether loss is direct or indirect) even if such loss was in the contemplation of the system participants or was wholly foreseeable. The PSP shall be fully liable for any loss of data or any loss arising out of breach of data whether due to willful misconduct of PSP's representatives or arising out of gross negligence or misconduct, etc.

4. Technology Partners Role in UPI

Under UPI, it is possible that banks can have tie up with Technology Partners and provide the PSP app to customers. However PSP bank should ensure the data ownership and due diligence of App for any 3rd party including that of the Technology Service Provider.

5. Settlement through banks with merchants

Under UPI, if merchant is holding bank account relationship with PSP Bank, PSP has to ensure the settlement with merchant into his bank account.

It is the ownership of Acquiring Bank to populate the correct MCC code, under which merchant is set-up. The UPI system will calculate and settle the Interchange between Acquiring Bank and Issuer bank basis MCC code populated. Merchant Category Code should flow in all the transactions from Acquiring Bank. The acquiring bank may have compliances built in for deviations, if any, basis various parameters such as velocity checks. In case of merchant pushes the P2P then compliance rule of MDR/Interchange will be applicable. The PSP has to do routine data checks to assess any inconsistencies for the transactions coming in from the merchant.

6. Ownership and branding of PSP App.

The ownership and branding of PSP App lies with PSP Bank. The responsibility of the functionality mentioned for the PSP app in the guidelines shall remain with bank. The PSP bank must have the mechanism to certify the PSP app with aligned merchant app and with proper invocation by any other app on the phone for payments. The UPI payment app must contain the PSP logo and look and feel for the customer irrespective of the UPI app distribution mode (embedded or independent), UPI app should offer exactly same screen and payment experience to consumer.

7. Ownership and branding of Handles

Under UPI, handles will be allotted to only PSP Banks. Bank has to ensure that under no circumstances, PSP handle allotted by NPCI to be transferred to any other entity/bank. PSP bank has to accept full responsibility for any and all activities related to handle provided by NPCI for offering UPI services. The Bank has to also ensure that PSP is the owner of the entire right, title

and interest in the registered trademark and/or copyrights of the handle name or PSP Handle owned by PSP and shall maintain title and ownership of all intellectual property rights in the handle name or PSP Handle.

Note: The handles available in the Phase I of UPI shall be only in the names of UPI member banks and no third party names shall be accommodated in the PSP Handles, unless otherwise approved by the Steering Committee.

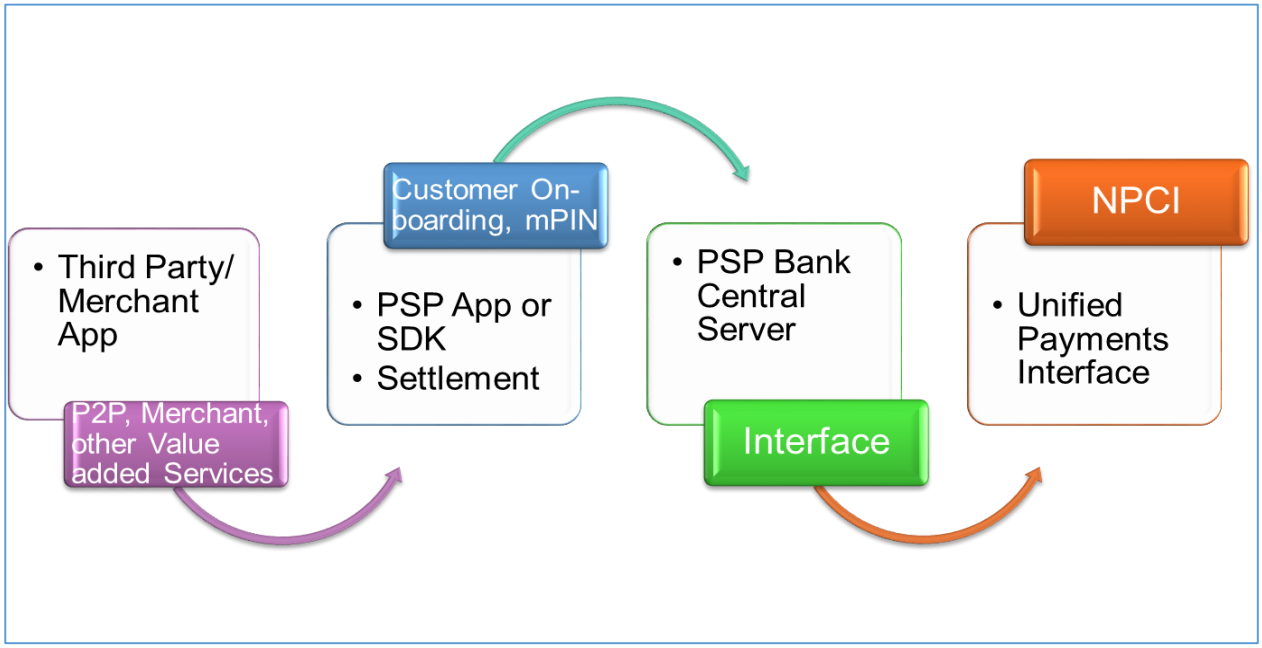
8. Portability of handles

Under UPI, the handle will be allotted at time of on-boarding of bank as PSP after written request from bank. The additional handles will be allotted only after written request from bank and after review of requirement by NPCI. Under no circumstances, the portability of handle will be allowed i.e. handle once allotted to one bank, cannot be transferred to any other bank.

9. Embedding of NPCI Library into Banks mobile banking App and Merchant through SDK through banks

Under UPI, it is possible to embed the NPCI Library into Bank's App and/or Merchant App through binary/SDK. In this case, the Banks/PSPs shall own the full liability should the Common library be compromised from Bank's App and/or Merchant's App. There is also possibility of NPCI providing separate APK (application) for Common Library (CL), however it has been decided that the same will not be provided by NPCI.

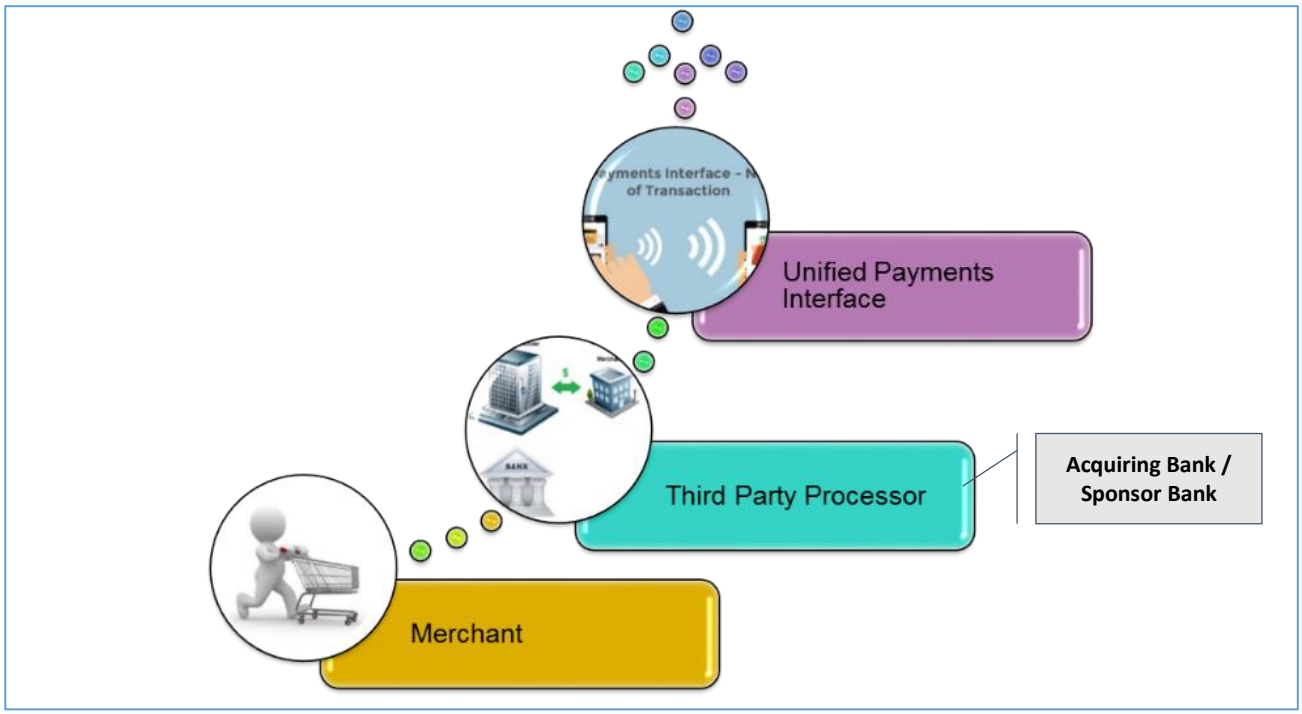
The broad approved architecture of UPI shall be as under:



10. UPI transactions through Third Party Processor for Merchant Payment

For merchant on-boarding in UPI, it is possible for the merchants to be enabled on UPI through the Third Party Processors. However, this activity should not include on-boarding of customers.

This approach can be enabled for Offline / Online merchant payments (without PSP SDK) and can be enabled on UPI. The following architecture may be followed in this regard (Applicable for Merchant on-boarding with a Third Party).



Annexure XIII (BROAD SECURITY CONSIDERATIONS)

1. **Saving the Collect requests (Marked Safe) received towards future authentications:**

   a) UPI Pull functionality provides for a Collect request of money originating from the end beneficiary.
   b) An individual's smart phone gets a Push notification from its PSP that a request for seeking /collecting money has been initiated by the end beneficiary.
   c) The message along with the virtual address of the beneficiary for e.g. rachitsoral@abcbank would also have the name being displayed on the App i.e. "Rachit Soral". Mr. Rachit Soral being an acquaintance of the sender, the sender knows that it is safe to send money for the request that has been originated and can treat the person as a white-listed entity/person for future requests. This can be made possible through population of the values in the element 'Verified Name' in the Payer / Payee tags. The name is as per the details stored in the CBS of the bank and is picked up without any customer intervention.
   d) The Recipient should be able to save such Collect Requests as references for future and mark these incoming requests as "Safe" for all future Collect requests coming in from this particular sender.

This shall ensure that scrupulous and Spam collect calls can be prevented where the beneficiaries are already known and registered through the "Save" option by the recipient.

2. **Display of the Name on the PSP Mobile App while adding the Account (Pulled from CBS) / Name display on the remittance transaction either Collect OR Pull requests**

   a) While the customer is adding the Account to the Profile / UPI ID (Virtual address), he/she selects the Bank name for which the Bank account has to be added. The request for account fetching goes from the PSP App to UPI to the Issuing Bank.
   b) The PSP App should also display the Account Name of the customer as it is stored in the Core banking system of the Bank. This will provide the actual name to be stored in the App since it is completely automated with NIL customer intervention.
   c) Like-wise the name of the customer should be displayed on the App – both in the case of sending monies (who is the sender) and for Collecting money (who is the initiator of the Collect request).

These steps would help ensure that any fraud pertaining to the wrong representation by the perpetrator can be prevented.

3. **Merchant white listing in UPI**

Under UPI, it is possible to initiate Merchant transactions under the following 3 modes/methods:

   a) Collect request originated over the Web App or Internet App by the merchant: This payment is initiated when the customer has selected the payment option as "Pay by UPI". This would send a Push notification to the customer's smartphone through his PSP App and the customer can enter his UPI PIN and initiate a Debit on the account.

b) The Push transaction – Where-in the customer knows the UPI ID (Virtual address) and/or IFSC and Account number of the Merchant & he can Debit his account to pay the Merchant.

c) In – App Payment method : Where-in the Merchant's Mobile App 'calls/invokes' all the UPI certified PSP Apps on the customer's phone & the customer selects his/her preferred App for making the payment by entering his MPIN on the PSP App.

It is recommended by NPCI that the large merchants be white listed by the PSP Bank. The merchant can be "whitelisted" by the PSP Bank using APIs **(CreateWLentry / UpdateWLentry/GetWLentry)**, checking with the centrally stored merchant details. This will help ensure that the customer has confidence in terms of the Merchant relationship with the PSP bank along with credibility and he/she can initiate the payment seamlessly.

NPCI shall incrementally provide the list of large merchants enabled on UPI to the PSPs on a monthly basis. These details can also be marked at the PSP server level basis the information provided by NPCI.

4. Name Check for UPI ID (Virtual addresses) created by customer

a) This implies holding a list of such names at the PSP Server which cannot be added.
b) The list of top 100/200 names can be stored in the database by the PSP, against which the names being entered by the customers shall be checked. If the name being entered in the list falls in the negative list, it will not be allowed. (NPCI shall endeavor to provide such list of names to the member banks)
c) Further, the display of names as in CBS under the 'Verified Name" element in the Payer/Payee tags ensures, that – even though the requesting Virtual Address may read as ***presidentofindia@abcbank*****,** the name of individual actually originating the request, shall be shown as 'Mr. Rachit Soral' and not 'Shri Pranab Mukherjee'.
d) Further, once the Virtual Address has been opted by a customer and later the profile is closed, then the PSP should not allow this UPI ID to be used by any other person/entity at least till 2 years post the deactivation by the initial customer.

The display of name in the collect request of the initiating customer is therefore a must for the PSP Banks. The name can be picked up from the UPI online message as stated above.

5. Mask Collect Request - check at NPCI to decline the request

a) It also needs to be ensured that the Collect requests received by the Beneficiary are not in a masked format. If this were to be permissible, then the requirement of displaying the name of the initiator of collect request is defeated.
b) The name should appear in clear on the PSP App for the customer to see. NPCI shall put in a process of terminating a request that is received in the message where the name and/or any other required details are in a masked format.

This would be required from the perspective of preventing any fraudulent and spam requests being received by the payer.

6. Velocity check of multiple credits to single account at beneficiary Bank end

a) The Collect requests can be initiated by an individual registered for the PSP App of any bank on any other individual who has registered and has created a Virtual address at the time of registration of the User profile with the UPI App.
b) Basis the Virtual Address, It is possible for an initiator to send multiple Collect requests to a single Virtual address such as Mr. Vikrant Sharma (vikrant@xyzbank) sending multiple collect requests on the virtual address rachitsoral@abcbank.
c) This is an avoidable nuisance for the recipient if he/she is flooded with such requests on a continual basis and are akin to Spam requests.

Recommendation would be have a velocity check on the following parameters:

1) Not more than **10 transactions** in a day on the same UPI ID (VPA)
2) Not more than **25 transactions** in a week on the same UPI ID (VPA).

In such cases the following are recommended:

a) For Individuals: As a Beneficiary PSP, the PSP Bank should build in checks to ascertain the number of such requests coming in from a particular virtual address (viz - vikrant@xyzbank) and if such requests exceed the prescribed threshold set by the PSP for an individual V.A sending collect request, then action could be taken at the PSP level to block any more requests coming in for its customer OR may take any such other action as is deemed appropriate.

b) For Merchants: This step mentioned above can also be utilized by the Acquiring PSP Bank for a merchant transaction. It is possible within the UPI framework for a Merchant to initiate a Collect request from the end customer as an individual (P2P) payment, whereas it is actually a merchant transaction. A merchant may resort to such means in order to escape the MDR/Interchange applicable in the Merchant transaction cycle.

a) It is therefore critical that the Beneficiary PSP Bank/Acquiring Bank in this case have a check on the velocity of such transactions coming in to the same Virtual Address.
b) It is an indication for the PSP Bank that excessive collect requests for a particular Virtual address may actually be a merchant transaction where the entity is collecting money on a P2P basis. PSP Bank could then initiate an inquiry / assessment, basis which the individual should then be set up as a merchant in the UPI framework along with the respective MCC and the corresponding MDR/Interchange. NPCI has also prescribed Merchant Compliance guidelines in this regard.

Note: NPCI shall provide report on velocity of the transactions of merchants towards aiding appropriate decision making by the PSP.

7. Prudent steps to be followed where the Mobile number / Mobile device has been changed.

7. a) Change in the Mobile Device:

a) In case of the change in the handset, it is mandatory basis the UPI framework to download the App again.
b) In this case, the mobile number shall again send the encrypted SMS to the PSP Interface. The PSP interface identifies that the same mobile number had been previously registered with it.

c) The PSP App should allow the customer to continue with the existing Virtual address, while it creates the new Device Hard-biding basis the encrypted SMS sent to the PSP interface.

7. b) Change in the mobile number:

a) A change in the mobile number would require the customer to give the new number / Update the number with his/her Issuing Bank.
b) The customer would be required to download the UPI App again using the same mobile number.
c) The PSP app sends the encrypted SMS to the PSP interface for creating the Device Hard binding.
d) The customer would be required to create a new Virtual Address to continue & this will be treated as a new registration by the PSP. This is to prevent any fraud related to usage of UPI ID (VPA).

Note: If the PSP can assess the veracity of the customer basis some secret Question / Answers, details of which were captured at the time of initial registration – the PSP may permit the customer to use the same UPI ID (VPA) in-spite of he/she using a new mobile number.

8. Outbound encrypted SMS

a) The most critical security requirement is to bind the mobile number with the device at the time of customer downloading the PSP App and creating a profile.
b) It has been mandated that the PSP App shall send an outward encrypted message to the PSP interface from the mobile number being used by the customer for registering the PSP profile. It is also recommended that this SMS is sent for every critical change (for e.g. upgrade of the OS version on the handset) to maintain security level checks).
c) In doing so, the PSP interface creates a Device fingerprinting of the mobile number, closely bound with Device Id, App Id, IMEI number or any other.
d) The outward SMS being sent is initiated automatically from the PSP App invoking the mobile number. There is no intervention of the customer to send this message out.
e) However, an alert may be generated by the PSP App indicating to the customer that an outward message is being initiated which would cost a nominal 'SMS charge" to the customer.
f) It is this device "hard binding" that shall be used by the PSP for authenticating the first factor of the subsequent financial transaction.
g) Secondly, the Mobile number being bound to the App, the hard bound mobile number (authenticated by the PSP) also becomes the carrier of the information in an interoperable transaction bringing in the trust between the PSP & the Issuer.
h) **Rooted Devices (Android) / Jailbreaking (iOS**) – for the rooted devices where the customer has control, the PSP may decide whether it wants to let the customer continue towards creating of the profile (for security reasons). The PSPs may have internal policies in this regard.

Annexure XIV (APP CHECKLIST)

Purpose of Document

The purpose of the below Checklist is to ensure that the UPI based Applications (Android / iOS and any other OS) have the same look and feel across applications of different entities. The

specific sections also include Apps developed under the "multiple bank model to "have functionalities offered as per the standard UPI guidelines and the APP adherence to overall UPI guidelines. The Field Marked with * have to be filled by PSP officials only after ensuring complete APP testing.

Note: -

a) It is mandatory for the banks to provide UPI app Checklist and application to NPCI before going live in public domain. All applications can only be made available in public domain post getting necessary NPCI approval.

b) The application checklist should be read in conjunction with the NPCI Operating circulars issued from time to time. The Application checklist is subject to change basis inputs & approvals – either internally from NPCI/RBI basis risk parameters and/or critical inputs from the ecosystem. Please get in touch with your Relationship manager for the latest version of the App checklist

M- Mandatory; **O**- Optional; **C** - Conditional

Level 1:- How to download any UPI enabled Application.

Sr.	Location	Bank/PSP Name in the App name	Mandatory*/Optional	Yes / No
a	Play Store (Android)		**M**	
B	App Store (IOS)		**M**	
C	Windows Store		**O**	
D	Any Other		**O**	

Level 2:- Home screen checklist

Sr.	Transaction Type		Mandatory/ Optional	Yes / No	Remarks (If Any)
A	language interface on App	1. English 2. Hindi 3. others	M O O		
B	Send Money (Push)	1. UPI ID* 2. Account / IFSC 3. Mobile No/MMID 4. Any Other (including mobile no only)	M O O O		

C	Collect Money (Pull)	1. UPI ID 2. Any Others (including mobile no only)	M O		
D	Add or Link a Bank A/C		M		
E	Transaction history		M		
F	Mobile Banking registration	1. Last 6 digits of Debit Card No. & Expiry date is manual entry. 2. Picture/Scan - Debit Card number	M O		
G	Virtual Keypad option on CL page & removal of original keypad	—	M		NPCI Common Library. (NPCI to check integration)
H	Change UPI PIN	Old UPI PIN & New UPI PIN is manual entry	M		
I	Forget UPI Pin option on CL page	—	M		(NPCI to check integration)
J	Resend OTP option on CL page	—	M		(NPCI to check integration)
K	OTP on CL Page	1. Auto Read on Android 2. Auto Read on IOS	M C^^		
L	Log a complaint	—	M		
M	UPI ID should only contain a-z, A-Z, 0-9, .(dot), -(hyphen)	—	M		
N	Instructions to create UPI ID	—	O		
O	Instructions/Steps to create UPI PIN	—	O		
P	Application password for login	—	O		

Q	Forgot password option	The password can again be set through email verification or by asking security question to user or OTP.	C		If App password is available, Forget password option is mandatory
R	Change Application Password		O		If App password is available, Forget password option is mandatory

**UPI ID known as Virtual Payment Address -VPA)*

Level 3:- How to register and deregister on PSP application.

Sr.	**Action**		**Mandatory/ Optional**	**Yes / No**	**Remarks (If Any)**
A	Mobile no should be fetched at the time of mobile-banking registration.	**1.** Device binding by sending encrypted outward message automatically **(on Android)** 2. Device binding by customer initiating the SMS string manually **(on IOS)**	M M		
B	SIM Selection option while customer on boarding	**1.** Choice of SIM Selection should be there in case of Dual SIM phones. **(on Android)** 2. Choice of Sim selection **(on IOS)**	M C^		
C	Type of SMS Encryption (**PKI**)		M		
D	Profile Creation		M		
E	UPI ID Creation		M		
F	Application password management		O		
G	Login Page to restart application		O		
H	Deregistration from App		M		

I	Deletion of Account linked to UPI ID		M		
J	Deletion of UPI ID		M		
K	User should be able to SET UPI PIN using any debit card assigned to him	Debit card (RuPay, Visa etc.)	M		
L	Notification to user	For e.g. - Pay / Collect etc.	M		
M	Mobile Number Registration Confirmation : -	1. In case if Mobile no. not registered 2. Mobile no. registration for SMS alerts 3. Mobile no. registration for mobile banking	M M M		
N	1 Lakh limit to be available at each PSP and issuer bank per transaction & per day		M		To be changed as per NPCI guidelines from time to time
O	Banks to integrate updated common library – PSP App & SDK	Name of latest Version ___	M		
P	Default collect timeout to be 30 min (if customer does not specify time). Option to be given to customer to select the timer of expiry of collect request		M		
Q	On the fly transaction should be available in PSP application – Direct entry of the beneficiary id		M		
R	Log a complaint to be available under each transaction in History		M		
S	Limit of Log a complaint		M		
T	RGCS response for Customer complaint to be displayed on front end PSP App and SMS/notification to be sent		M		
U	Collect Notification to be present in PSP	The notification should contain expiry date and expiry time	M		
V	Alert for first time collect Request		M		
W	Blocking or SPAM collect Request		M		

X	Intent Call functionality and response handling		M		
Y	Transaction history to be available Date-wise		M		

^ *If the OS provides for the possibility*

Level 4:- Add a bank Account / UPI ID & Account handling

Sr.	Actions	Mandatory/Optional	Yes / No	Remarks (If Any)
A	List of banks to be displayed as an Issuer in drop down menu	M		
B	List of bank to be displayed as an Issuer in drop down menu and to be searched by start letter of the bank (e.g. – I – icici bank, IndusInd bank, Indian overseas bank) etc.	M		
C	If customer is "not registered for Mobile Banking (i.e. No UPI PIN set) - then display Set UPI Pin transaction to customer and allow set-pin based on last 6 digits of Debit card & expiry date followed by OTP from Issuer **OR** If customer has UPI PIN (i.e. Issuer responds stating that UPI PIN exists for this user -, the app should provide an option – "Continue with Existing UPI PIN".	M		
D	If customer is not registered for MB (UPI PIN not set) - customer should be routed to Mobile Banking Registration transaction with the same details required for Set UPI PIN	M		
E	One UPI ID to multiple Account	O		

	(Default UPI ID selection)			
F	Multiple UPI ID to Single Account	O		
G	One PSP APP to register Multiple bank accounts with multiple UPI IDs	M		
H	Generate OTP (Set UPI PIN) • Auto read OTP **(Applicable on Android)** • Manually type OTP (**Applicable on IOS)**	M C		

^ - Depending on OS providing the possibility

Level 5:- Send Money (Pay Transaction)

Sr.	Action		Mandatory/ Optional	Yes / No	Remarks (If Any)
A	Send Money (Pay)	1. UPI ID 2. a/c & IFSC 3. mob & MMID 4. Any Other (including Mobile no Only)	M O O C O		
B	UPI PIN to be used by customer	1. Preapproved transaction 2. Non pre-approved	O M		
C	Online Confirmation of transaction		M		
D	Dlength of UPI PIN to be passed by the PSP App to NPCI i common library page for PSP App	Length of UPI PIN___	M		
E	Methodology of invoking Common Library Page 1. UPI Pin preapproved /onus transaction invocation of common library		O M		

	2. UPI Pin Non-preapproved /offus transaction invocation of common library 3. PSP App should provide to common library complete details on transaction such as Bill No. , amount , Transaction ID , and other details		M		

Level 6:- Collect Money (Collect transaction)

Sr.	Actions		Mandatory/Optional	Yes/ No	Remarks (If Any)
A	Collect Money	1. UPI ID 2. Any Other (including Mobile No only)	M O		
B	UPI PIN	1. Preapproved 2. Non pre-approved	O M		
D	Transaction Status Confirmation		M		
E	Display of UPI ID and Name for incoming collect request		M		
F	Display of Expiry time in case of incoming collect request		M		
G	Default validity of 30 minutes in case customer is not specifying the expiry time. Customer must be given an option to select the expiry of the collect request being initiated		M		
H	Minimum validity of 1 Minutes in case customer is selecting expiry time of collect request explicitly		M		

I	Methodology of invoking Common Library Page 1. UPI Pin preapproved /onus transaction invocation of common library 2. UPI Pin Non-preapproved /offus transaction invocation of common library 3. Ref URL in common library should take customer to relevant page with complete detail i.e. Bill No. , amount , Transaction ID , and other details		O M M		
J	Collect Request handling (Collect coming from other PSP/3rd party App)		M		

Level 7:- Balance Enquiry *

Sr.	Action	Mandatory/Optional	Yes/ No	Remarks (If Any)
A	Select Account	O		
B	UPI Pin Preapproved	O		
C	UPI Pin Non Preapproved	O		

**- Storage & usage of customer account balance by any PSP App or 3rd party UPI enabled App (including Apps in the Multi bank model) is not permissible. The customer account balance cannot be stored even in encrypted form.*

Level 8:- Check Transaction Status / Raise Query/ log a complaint

Sr.	Action	Mandatory/Optional	Yes /No	Remarks(if Any)
A	Transaction History • Ref no. wise • Date wise	 O M		**Banks to decide on the parameters**
B	Raise a query / Dispute • Basis On ref no. • date wise	 O M		**Banks to decide on the parameters**

C	While raising the query/dispute, the App should display • Transaction ID • Beneficiary and Remitter • UPI ID/other address • Date & Time • Amount	M		
D	Check Transaction Status • Option Raising a query/ Log a complaint against each transaction should be there.	M		
E	Last 5 Transactions	M		

Level 9:- Hot listing/Deletion of UPI ID

Sr.	Action	Mandatory/Optional	Yes/ No	Remarks (If Any)
A	Once hot listed or deleted, is Bank allowing to re-allocate the same UPI ID?	M (Minimum 2 years Moratorium)		

Level 10:- Payments by UPI

Sr.	Action	Mandatory/Optional	Yes/ No	Remarks (If Any)
A	Pay by UPI	M		Nomenclature is to be decided by the bank
B	Collect by UPI	M		
C	Reject/Accept Collect request	M		

Level 11:- QR Code based enablement

Sr.	Action		Mandatory/Optional	Yes/ No	Remarks (If Any)
A	**Generate the QR Code** (Customer Should be able to generate the QR Code - both Static and	1. UPI QR Code	M		

	dynamic with inhis App -)				
B	**Scan the QR Code** (Customer should be able to scan the QR Code of a Merchant / Another PSP app for making payments)	1. UPI QR Code 2. Bharat QR Code	M M		
C	It is mandatory to display to the customer at least UPI ID, amount and the name in QR Based Payments		M		

Level 12:- Raising and listening Intent Call

Sr.	Action		Mandatory/Optional	Yes/ No	Remarks (If Any)
A	The App to support Intent Call request from the Merchant Apps (Applicable for all type of UPI APP)	1. Android 2. IOS 3. Windows 4. Any Other	M C^ O O		
B	The App to support raise the intent call from the App (Also Applicable for Third party UPI enabled APPs – including Apps under Multi bank model)	1. Android 2. IOS 3. Windows 4. Others	M C^ O O		

^ - *Bank to enable basis their development*

Level 13:- Total User entry

Sr.	Action	Mandatory/Optional	Yes / No	Remarks (If Any)
A	UPI ID	M		
B	Debit Card • Entry • Scan	 M O		
C	SET UPI PIN	M		
D	Saved beneficiary while approving Collect Request	O		

	)			
E	If Merchant is whitelisted display verified Merchant on the PSP with incoming collect request	C		White listed merchants
F	Saving Beneficiary by nick Name (For UPI ID, Acc+IFSC, Aadhaar No etc.)	O		
G	Amongst saved beneficiary – option of marking Bene as a Favourite	O		
H	Restoring of UPI ID by PSP in case of deletion of UPI ID by user	M (minimum2 years Moratorium)		
I	When a payee initiates a collect request the name of the payer should be verified name (CBS name) and should be displayed to the payee.	M		
J	In Pay/Collect transaction the entry of 'Remarks' should be optional for user • If a user does not wish to enter any remark, bank should populate a default remark as 'UPI' in the back end • If a user wishes to enter any remark, bank should populate the same in the back end	M		

Level 14:- UPI ID/ VPA Allocation

Sr.	Action	Bank Name in the handle name	Mandatory/Optional	Yes / No	Remarks (If Any)
a	Handle Name		M		
B	Default Handle name		M		Multi bank model only if account listed by customer is also of the same sponsor PSP NPCI Circular 15/15A apply for single SDK
C	Changing the handle Name		M		Multi Bank API Model
D	Fair Distribution of handle		M		Multi bank API model only

Level 15:-UPI Interoperability principals for SDK integration & web enablement

(Applicable for P2M only)

Sr.	Action		Mandatory/ Optional	Yes / No	Remarks (If Any)
A	"Pay by UPI"	This option is equally placed along with other payment options on merchant / P2p provider on App/Web	M		
B	Choice of UPI ID	Merchant/P2P provider must give equal choice to the customer to pay by UPI ID of his choice i.e. registered UPI ID in SDK or any other UPI ID customer has. (Merchant/P2P provider to use intent or collect call on App and collect call on web to facilitate customer to use UPI ID of his choice)	M		
C	Enabling condition for other UPI ID's to be accepted	PSP SDK app should not mandate the customer to register for UPI or create UPI ID to avail product or services provided	M		
D	de-register & delete UPI ID	PSP SDK must provide an option to customer to de-register & delete UPI ID (life cycle management)	M		
E	Intent and collect calls	PSP SDK must respond (once customer has registered successfully) to intent calls and collect calls.	M		
F	Default option for payments	PSP SDK to provide an option to customer to	M		

		register the handle as 'default' for payment on this specific app during on-boarding process.			
F.1	The 'Default' option provided should be pre-checked on 'No'		M		
F.2	If customer has chosen 'Yes', then the PSP SDK is absolved from mandated intent / collect call only for that "merchant or P2P provider services".		M		
F.3	Provision to allow customer to alter the 'Default' option during the life cycle (Change the option chosen earlier)		M		
G	Branding for PSP bank	PSP SDK on-boarding and payment pages should only have branding of the PSP bank	M		
H	Not sharing of customer data	PSP bank is not sharing any customer data with the merchant/P2P provider, unless specified by industry regulator. E.g. SEBI, IRDA etc. (permitted only for specific regulated merchants). No authentication data shared outside PSP bank.	M		
H.1	Beneficiary account number , CBS name and transaction related data stored by 3rd party server in Encrypted manner		M		
I	PSP banks should ensure that Merchant / P2P provider Apps are called as "UPI Compliant Apps" and not "UPI PSP Apps"		M		
J	Call centre details	PSP must ensure that PSP or 3rd	M		

		party call centre number is prominently mentioned in the application for handling customer queries.			
Applicability of Conditions (3rd Party App / 3rd party Server)- As per Terms of Multiple Bank arrangement in UPI (API approach)**					
K	Restriction on adding of Account	PSP Bank / 3rd party does not place restriction on customer to add any of his/her accounts	M		Any account of participating UPI Member bank
K1	Customer choice on selecting handle	Post initial allocation of Handle (default where account listed by customer = Sponsor PSP), customer has the option of creating UPI ID with another handle of participating member bank in multiple bank model	M		As per Multi Bank approach
K2	Account Number storage in the 3rd party App and Server	Stored in encrypted manner only	M		
K3	Beneficiary Account No; Beneficiary CBS name in 3rd party App and Server	Stored in encrypted manner only	M		
K4	Beneficiary details entered by customer - not used	For Cross-Sell, Up-Sell, Value Added Services etc.	M		
K5	Customer Account Display on 3rd party App	Only in Masked Manner	M		
K6	Transaction logs & Transaction data	Stored in 3rd party App & 3rd party Server – only in encrypted manner	M		For customer to log a compliant
K7	Customer Consent for data usage	Explicit Customer consent for usage of data	M		Limited internal functions only (Cross-Sell/ Promotions/ Offers/ Value Added

					Services/ Increasing Transactions /Better User Experience
K8	Monitoring of Rogue Apps	PSP & 3Rd party have processes for monitoring of rogue apps (similar to their Apps)	M		
K9	Vulnerability Management program	PSP Bank follows updated guidelines / checklist as part of Vulnerability Management program for 3rd party	M		
K10	Customer payment sensitive data: • Last six digit of Debit Card • Expiry Date of Debit card • Account Number • Bank Account Balance • Issuer OTP • Issuer PIN	Never stored in the 3rd party App or 3rd party Server	M		Payment Sensitive data

*** - Conditions (other than what is explicitly stated for multi bank API model) under point K above are also applicable for 3rd party UPI enabled Apps under the SDK model*

All above features, must be verified by "Bank's Compliance Team" and given their sign off in writing to bank's UPI business/technology team to on-board this merchant/P2P provider with PSP SDK.

Additional Comments (if any):-

Sign off

National Payment Corporation of India

Annexure XV (Merchant SDK Guidelines)

Background & Objective

UPI Framework provides for embedding PSP SDKs in the Merchant Apps to facilitate customer on-boarding and payments. The extant Policy document deals with the guidelines for PSP SDK integration in the 3rd party merchant or user services app.

a) The policy framework shall govern the SDK integration and is based on the inferences & conclusions drawn from the UPI Steering Committee Meeting/s with member banks and may undergo changes from time to time.

b) The objective of this policy is to lay out the ground rules for SDK integration and drive uniformity in the approach across all member banks participating in the UPI framework.

c) The SDK integration in 3rd party Apps providing for merchant payments, payment of Utility Services or value added services, P2P services etc.

d) The pricing to the end consumer shall be governed by the circulars issued by NPCI or RBI from time to time.

e) It would be mandatory for the banks to adhere to guidelines and changes issued in this regard, thereafter.

Guidelines:

1) **Guideline Framework 1:** ***Only Bank led Apps be called UPI Apps:***

   a) The merchant or user services (p2p/bill pay/Aggregator) apps, can be referred to as UPI compliant apps and cannot be referred as "UPI PSP Apps".

   b) Banks must get into proper agreements with the merchant incorporating its PSP SDK's having key terms and conditions and must verify the same before going live.

   c) Under no circumstances, such 3rd party shall either project or portray itself as a UPI PSP App in the industry.

2) **Guideline Framework 2:** ***All 3rd party – "UPI compliant apps" to have the intent call enabled on all transactions when customer selects payment:***

   a) All 3rd party Apps, must mandatorily have the intent call enabled after user has enabled the UPI ID in that SDK.

   b) However, the PSP SDK, may ask the customer to select this PSP SDK as default payment option while purchase on this merchant/user services app while user on boarding. After specific consent from the user that he has checked in the "default" SDK for this merchant, in that case the intent is not necessary.

c) When intent or collect call is involved, the relevant PSP SDK's should open up instead of the merchant or user services app. For e.g. the bank's screens in that integrated PSP SDK should open up for the user instead of the main merchant app on any other bank calling the intent for payment.

3) **Guideline Framework 3:** ***A Bank should use the same codebase for all its PSP and SDK integrations (security and user experience)***

a) Bank must use the same code base for its own PSP app and PSP SDK's. However bank may do minor customizations (not changing the core and security architecture) if needed for SDK's.

b) If a user registers a Virtual Payment Address (UPI ID) with any of the PSP SDK's of a bank, then this UPI ID must also be visible to all the merchant apps that use the same PSP SDK using the same phone. Customer need not be asked to register in all SDK's.

c) The SDK's should be certified by third party security auditor and clean report must be submitted to NPCI. (any major change in the SDK shall go through the security audit process)

d) The bank must give similar user experience for the customer to on-board/transact using SDK or its own PSP app from the standardization view.

e) The App embedding an SDK shall allow the user to manage all UPI IDs, and Accounts on boarded into UPI through an SDK even in cases where he is on another merchant App with the same SDK.

f) There should not be any co-branding on the PSP SDK pages. It should only display bank brand.

4) **Guideline Framework 4:** ***Banks are allowed to configure merchant SDK to their acquired merchant (with the approved policy)***

a) Only merchant with an App distribution to customers for e.g. in excess of 500,000 or higher number to be provided an SDK embedding by the member banks. Rest of the merchants can use only the collect feature.

b) Banks should get the policy of SDK sharing to be approved from their 'Risk Management Committee' as they need to take complete liability for any breach of merchant app where bank's PSP SDK's are integrated.

c) NPCI strongly recommends that bank should also take similar security certification for the merchant app after the integration of their PSP SDK as a whole before go live.

5) **Guideline Framework 5:** ***UPI PSP Apps that come up/Respond to the intent call of the Merchant shall only be those Apps where the customer has created a UPI ID and added an account.***

a) A merchant app (SDK mode) shall register to handle the UPI intent, only after a customer has a UPI ID / account linked to it. This will help prevent clutter on the display and bring up only the relevant UPI PSP Apps.

6) **Guideline Framework 6:** ***Banks shall handle a Collect call to a UPI ID created by the merchant app (SDK route) in a consistent manner.***

a) The incoming collect call, should not open up multiple apps by the PSP app or PSP SDK's, rather it should know which one app to be opened for consistency.

7) **Guideline Framework 7: The security of the data residing in PSP SDK**

a) Bank shall ensure full responsibility towards ensuring that the merchant app (SDK) data is not visible to merchant app other than required.

Important Notes:

b) NPCI Verification of the SDK: After security certification by third party, the bank must submit the SDK to NPCI for verification.

c) The services that can be provided through PSP Bank SDK may include:

d) Creation of UPI ID (VPA)

- Linking of bank accounts
- Create, set and change UPI PIN
- View balance of issuing bank account
- Payment

PSP Banks shall provide NPCI common library only through PSP bank SDK for integration with merchant/user services provider

Annexure XVI (Merchant SDK Checklist)

INTRODUCTION:

"Banks have envisaged the embedding of their PSP application, through an SDK in other applications as a means of distributing their applications. This is provided for in the UPI framework to facilitate customer on boarding and payments. The bank continues to remain the PSP and is responsible and accountable for all UPI requirements, including security, handling of customer complaints, fraudulent transactions, etc. to the same extent as their own applications."

A) Guidelines for merchant/ P2P provider payment
   a. Initiated through webpage
   b. Initiated through mobile (without SDK)
   c. Initiated through mobile (with SDK)

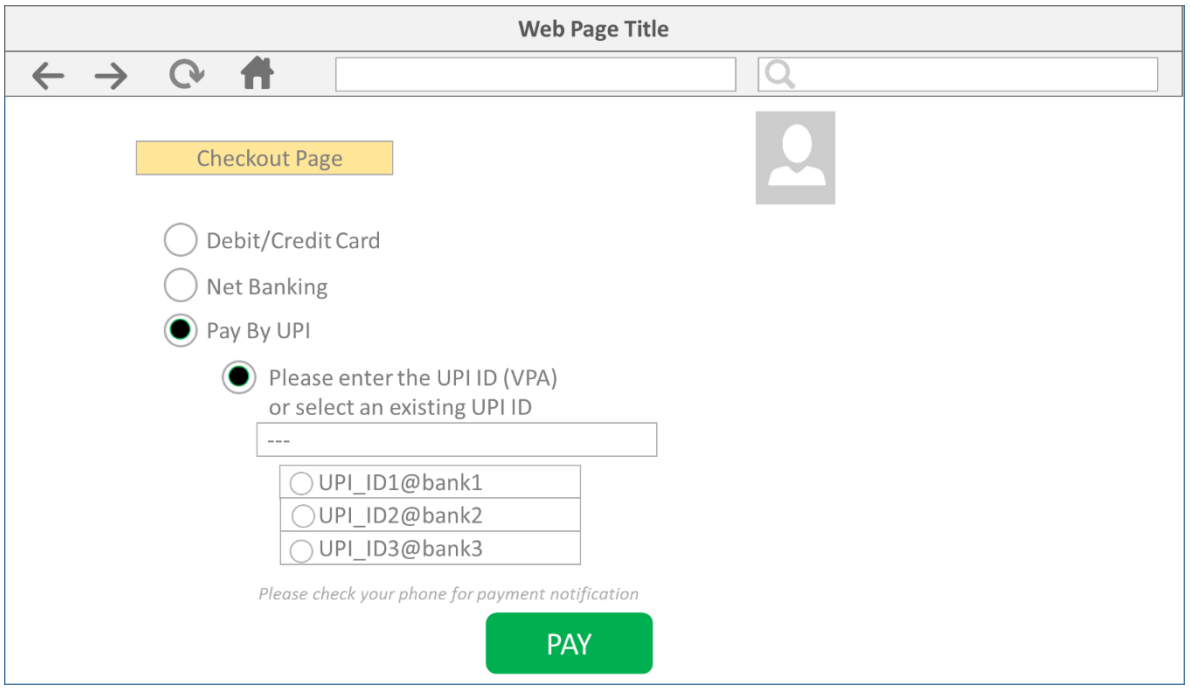
B) Checklist for SDK Integration

- **Checklist part 1: Collect Payment Request**
- **Checklist part 2: Payment Request**
- **Checklist part 3: PSP SDK functions**

C) Annexure - Flows

APPROACH TO BE FOLLOWED:

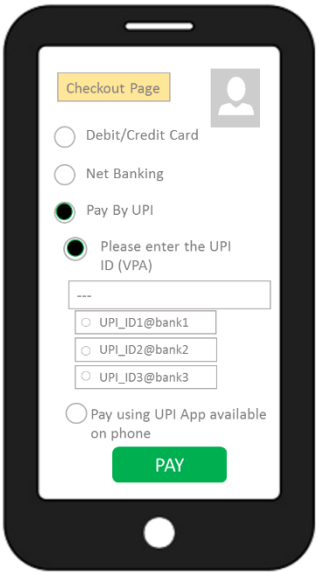
(A) **Payment using UPI on the Merchant/ P2P provider Webpage:**



The user has selected the article to buy on the merchant/ initiating transaction on P2P provider webpage and wants to check-out. He sees the payments options including “Pay by UPI”:

a) If customer had used the UPI Payment option for this merchant/ P2P provider, he shall see the previously used UPI IDs listed in the drop down (e.g. UPI_ID1@bank1, UPI_ID2@bank2) .
b) If he had not used UPI payment option earlier for this merchant/ P2P provider, he can enter his preferred UPI ID (VPA) in the writable dropdown space provided - (*name@abcbank*).
c) Merchant/ P2P provider prompts him to check for a payment notification on the phone for this payment.
d) Customer gets a payment notification on the ‘abcbank’ App. Customer enters UPI PIN and completes the transaction.

(Detailed flow: Please refer flowchart 1 from the annexure-flow)



B) Payment on the Phone (Without the SDK integration):

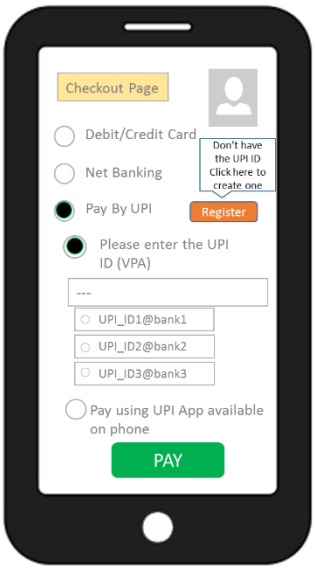
The user has selected the article to buy on the merchant/ initiate transaction on P2P provider App and wants to check-out. He sees the payment options including "Pay by UPI".

Customer had used UPI for payment earlier onany PSP / merchant/ P2P provider:

1) ***Customer can enter the UPI ID or use an existing UPI ID option***
   a) If customer had used UPI as payment option earlier, he shall see the previously used UPI IDs listed in the drop down.
   b) Merchant/ P2P provider prompts him to check for payment notification on his phone for this payment.
   c) Customer gets a notification. He enters his PIN and completes the transaction.

2) ***Customer wishes to pay using a PSP App already available on customers phone:***
   a) Merchant/ P2P provider detects that there are other eligible UPI Apps on the phone.
   b) Merchant/ P2P provider calls the other eligible UPI Apps listening to the payment request and the eligible Apps open for customer to initiate payment. Amongst these Apps, customer uses his preferred App to complete the transaction.
   c) Customer checks the payment details and enters the PIN for completing his transaction.

(Detailed flow: Please refer flowchart 2 from the annexure



(C) Payment on the phone (through SDK embedded App):

The user has selected the article to buy on the merchant/ initiate transaction on P2P provider App and wants to check-out. He sees the payment options including "Pay by UPI". There are following 3 possibilities:

1) ***Customer had used UPI for payment earlier on this merchant/ P2P provider:***
   a) If customer had used UPI as payment option earlier, he shall see the previously used UPI IDs listed in the drop down.
   b) Merchant/ P2P provider prompts him to check for payment notification on his phone for this payment.
   c) Customer gets a notification. He enters his PIN and completes the transaction.

2) **Customer has not used a UPI payment option on this merchant/ P2P provider:**
   a) Customer gets the option to Register/Create his UPI ID with this App. This App has an SDK integration from "abcbank"
   b) Customer completes his registration on this app and creates a UPI ID, e.g. name@abcbank.
   c) After the UPI ID is created, the customer can be given an option to set this App as default App for his future payments. Here, the default option selected always is "NO". If the customer knowingly wants to make this App as his default App, then he selects the "YES" option.

3) ***Customer has not used UPI payment option on this merchant/ P2P provider:***
   a) Merchant/ P2P provider detects that there are other eligible UPI Apps on the phone.
   b) Merchant/ P2P provider calls the other eligible UPI Apps listening to the payment request and the eligible Apps open for customer to initiate payment. Amongst these Apps, customer uses his preferred App to complete the transaction.
   c) Customer checks the payment details and enters the PIN for completing his transaction.

(Detailed flow: Please refer flowchart 3 from the annexure)

Checklist part 1: Collect Payment Request

Collect request has to be made available as an option for all the transactions:

1. Collect – Merchant Webpage
2. Collect - Mobile without SDK integration
3. Collect - Mobile with SDK integration

(Please refer the guideline section for merchant payments and corresponding flowcharts in annexures)

When a customer receives a collect payment request on a UPI ID (e.g. customername@abcbank), below mentioned scenarios are possible:

(Suppose: M1 as Merchant/ P2P provider 1 App, M2 as Merchant/ P2P provider 2 App and P1 as bank's PSP App with same virtual address as above registered on each of them)

Case 1: Customer has only one PSP SDK integrated application in his handset (In this case customer is registered on M1)

Case 2: Customer has Same PSP SDK integrated in two or more merchant/ P2P provider applications present in his handset. (In this case customer is registered on both M1 and M2)

Case 3: Customer has sponsor bank's PSP app along with sponsor bank's PSP SDK integrated in two or more applications (In this case customer is registered on M1, M2 and also P1)

Case No	**Description**	**M/O**	**Y/N**
Case 1	PSP SDK application open up directly for the collect request without showing parent merchant/ P2P provider app's interface - Collect will come on M1	M	
Case 2	PSP Bank should either configure one app for receiving the request or segregate subsequent requests among the merchant/ P2P provider apps. **In any case collect request should come only on one app for customer convenience.** - Collect can come on either M1 or M2	M	
Case 3	PSP Bank should either configure one app for receiving the request or segregate subsequent request among the merchant/ P2P provider apps. PSP app may priorities itself to respond to collect call. **In any case collect request should come only on one app.** - Collect can come on either M1 or M2 or P1	M	

Checklist part 2: Payment Request

When the customer selects "Pay by UPI" on the merchant/ P2P provider app payment page, following 3 options should be made available in addition to Collect:

A) Create new UPI ID using PSP bank's SDK handle
   i) For Single SDK
   ii) For Multiple SDK
B) Show already existing UPI IDs.
C) Pay with any other UPI App on phone (intent call)

A (i). Single SDK scenario:
If the first time customer (never registered for UPI before) selects UPI as Payment option – Customer Creates new UPI ID (one Single SDK integrated in a single App)

Sr No	Description	M/O	Y/N
1.	After selecting "create UPI ID option", the app will prompt for customer's consent to send an encrypted SMS (PKI encrypted) as per process	M	
2.	On the merchant/ P2P provider App customer will receive the option to Create the UPI ID through PSP SDK. e.g. user-name@abcbank belongs to 'abc bank' SDK	**M**	
3.	After UPI ID availability and confirmation, customer will proceed to add account and set UPI PIN (refer UPI App checklist). All the application pages for on-boarding should have the bank's branding only.	M	
4.	- Merchant/ P2P provider App may have PSP bank's branding in a prominent manner to indicate that there is a PSP SDK embedded. - Bank's PSP SDK screens will not have Merchant/ P2P provider branding.	M	
5.	**The PSP SDK may provide the option to set the Application as default.** In this regard the process flow under point 2.c of the guidelines section - **(C) Payment on the phone (through SDK embedded App)** may be referred/used.	O	
6.	PSP SDK will route customer directly to payment confirmation page (Before invoking Common Library page of that bank) Note: This may help customers to review his complete payment details, which are not captured in CL e.g.: Product name etc.	O	

B. If customer is already registered on UPI – He can use his existing UPI ID

Sr No.	Description	M/O	Y/N
1.	On the app the customer see the option to select Available/existing UPI IDs in the PSP SDK integrated application, following are the possibility: • Customer will be shown the UPI ID which he has created on this App (this can be shown as a separate option or as primary payment option separately for the subsequent transactions) • The customer gets to see his UPI ID which he created on another merchant/ P2P provider App but the SDK was same. • The customer gets to see his UPI ID created on sponsor PSP bank's App **Note:** In all the three options, the assumption is that the SDK is same and therefore it can show all the UPI ID's created by this customer. (Common database) Irrespective of the above three options, customer should also be shown the UPI ID's (if any) which he had used previously to raise collect to initiate a collect transaction	M	
2.	"Create New UPI ID" option to be provided by the PSP SDK	M	
3.	After the UPI ID selection on the PSP SDK, customer shall directly reach to payment confirmation page (prior to leading into Common Library page of that bank)	O	
4.	First time payment using existing UPI ID, app should prompt for customer's consent to send an encrypted SMS (PKI encrypted)	M	

C. Already registered on UPI – payment via other UPI app (by intent call)

Sr No	Description	M/O	Y/N
1	The App should automatically detect the presence of any UPI App and in case there is an existing App, then only this option should be made available.	M*	
2.	On the merchant/ P2P provider app when the customer selects "Pay with other PSP application", other eligible UPI Apps (as per UPI App checklist) should be shown	M*	
3.	Merchant / Initiating App should get the final status / response of the transaction.	M*	

** The section is not applicable in case the default option was selected by customer as "Yes" during UPI ID creation.*

Checklist part 3: PSP SDK functions

The integrated PSP SDK shall provide the following functions:

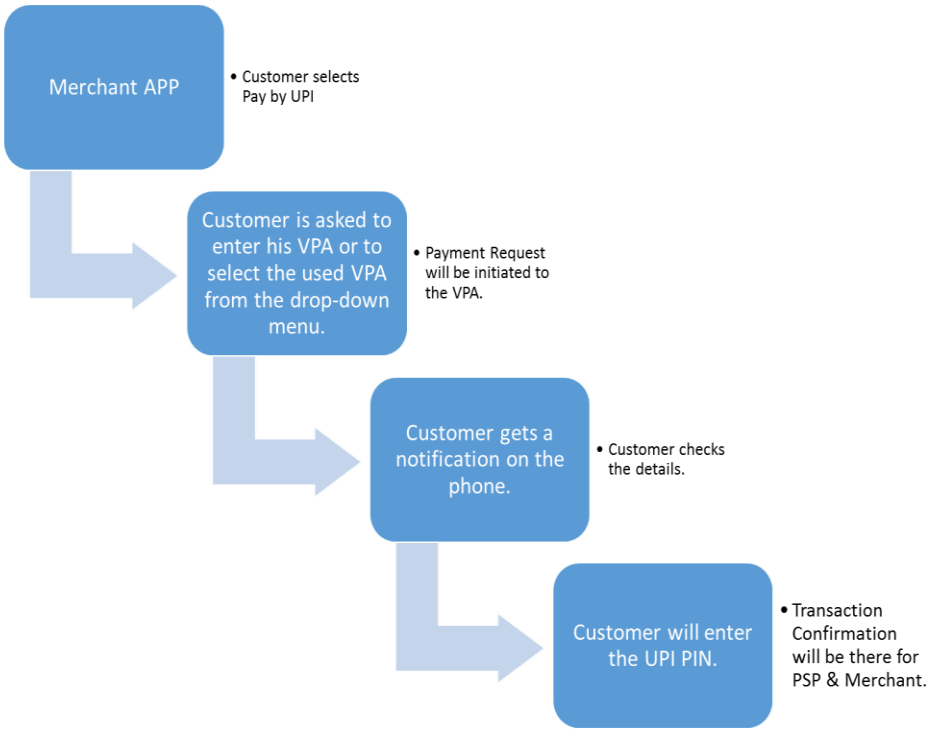
Sr No	**PSP SDK functions**	**M/O**	**Y/N**
1.	PSP SDK integrated app shall allow the user to manage UPI IDs and accounts across other apps with same PSP SDK and sponsor bank's PSP app e.g. Three accounts added in M1 should be reflected in M2	M	
2.	Common library (secure component) should be separate for each PSP SDK integration.	M	
3.	Common library should remain with PSP SDK wrapper and cannot be exposed directly for security reason.	M	
4.	PSP SDK integrated app should only respond to intent call post addition of account and UPI ID to it in order to avoid clutter.	M	
5.	When an intent call is received by PSP SDK integrated app, PSP SDK application should open up directly without showing parent merchant/ P2P provider app's interface for customer convenience.	M	
6.	Customer should be given an option to change the 'default' option of the payment App at any point of customer choice	M	

NOTE:

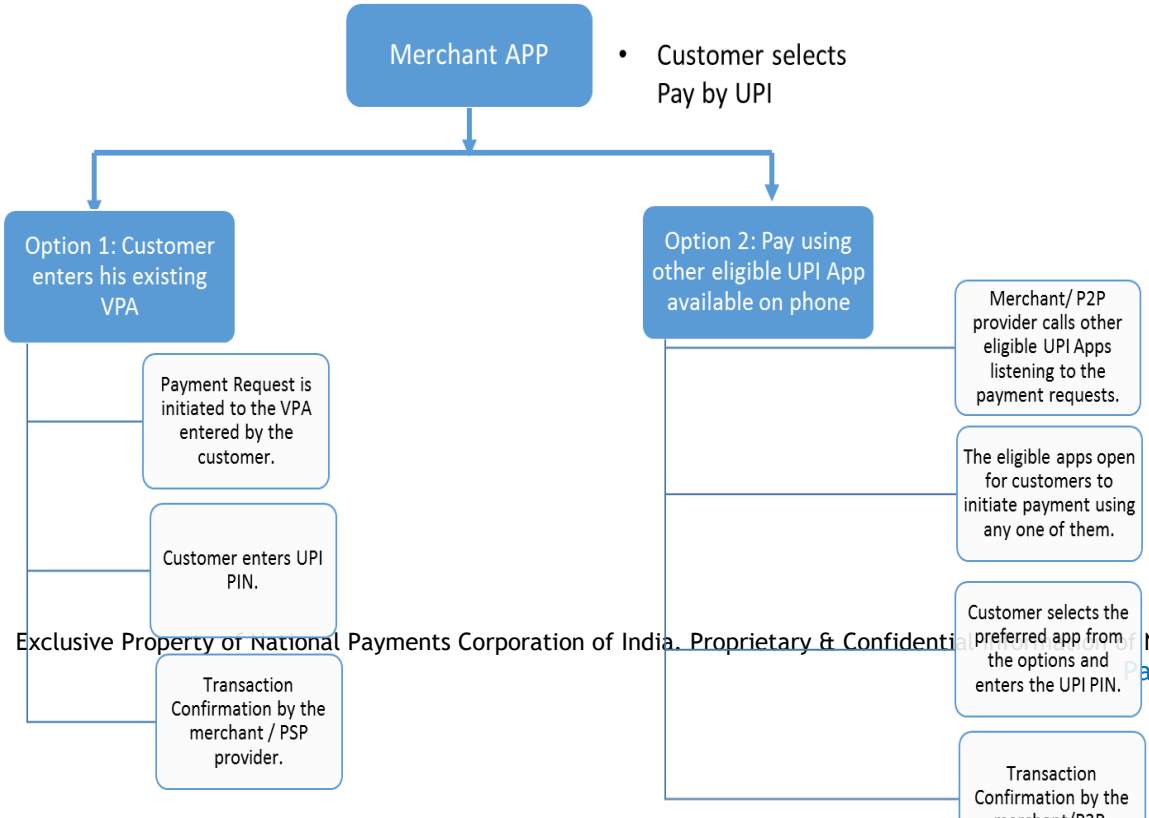
1) PSP SDK with common library in wrapper should be shared with the merchant/ P2P providers as per bank's policy & their board approval.
2) The PSP SDK should have the same codebase across all merchants.
3) Bank need to ensure that whenever a merchant/ P2P provider with its PSP SDK is involved in a payment transaction, no customer data is shared with any other party other than those involved in the transaction, including the other merchant/ P2P provider (with exception being scenarios where merchant/ P2P providers such as Brokers and Mutual Funds are required to do third party validation as per regulatory or other mandatory requirements).
4) Only two merchant PSP SDK per handle is permissible.
5) PSP SDK integrated apps cannot be called UPI apps and shall be referred to as UPI compliant apps. This should be clearly mentioned in all the customer communication.
6) Banks which are live as PSP themselves can only create SDK solution.
7) Banks need to carry out a third party audit of SDK and merchant/ P2P provider App which will be submitted to NPCI and NPCI will perform a third party audit (CertInEmpanelled)on each SDK provided by banks before going LIVE. (For SDK and merchant Apps already in production environment, bank should submit their third party audit (CertIn Empanelled) Annually to NPCI). NPCI shall empanel the security agencies to audit the merchant apps having bank PSP SDK's. NPCI will publish the list of empanelled agencies separately.
8) Bank to communicate to NPCI the details of each SDK and App release before GO LIVE.
9) This document should be read in conjunction with PSP SDK guidelines, APP Checklist and PG, including the transaction sets as may be applicable

Annexure - Flows

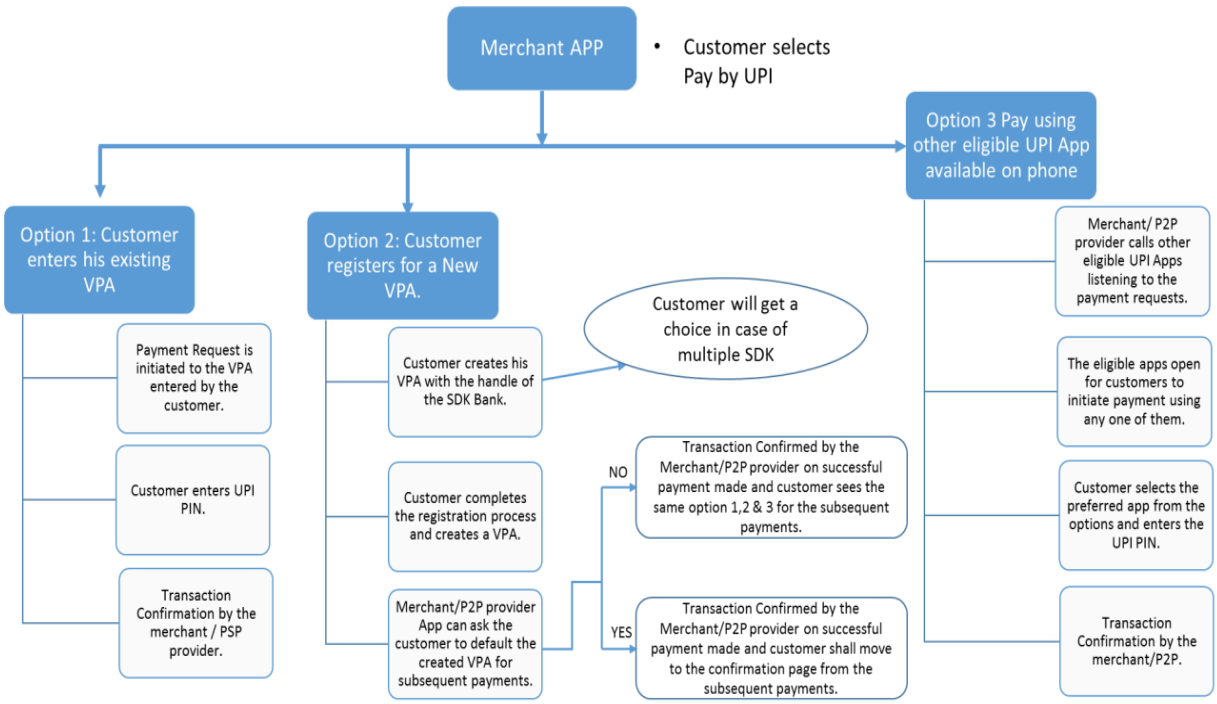
Flow chart 1: Payment using UPI on the Merchant/ P2P provider Webpage



Flowchart 2: Merchant/ P2P provider Checkout on Phone – Without SDK



Flowchart 3: Merchant/ P2P provider Checkout on Phone – With single* SDK



Annexure XVII (Off boarding Process)

Steps to be followed for off-boarding of member:

1.1 Off-boarding of member on direction by regulator/Competent authority/Court

TAT: within 3 working days

Regulator/Competent Authority/Court may issue a directive, stopping a bank/institution from participating in clearing/payment systems.

Risk team shall receive intimation of such directives from RBI and/or other authorities. If intimation of such directive is received by any other team in NPCI, they should immediately (on the same day) inform Risk team and share the copy of the directive over email. Risk team shall maintain a tracker of all such directives received from Regulator/Competent Authority and update the action taken at NPCI.

On receipt of such intimation Risk team will send a mail with copy of directive to the operations team (online and offline both) to check the status of the bank/institution in our system.
[TAT: within 1 working day from the day such information is received]

Operations teams will check the status of the bank/institution in each of the online and offline products and update it to Risk team by responding to the email.

[TAT: within 1 working day from the day such information is received]

a.Bank/institution not live for any one or more product/s

If the bank/institution is not live for any one or more product/s, no action shall be taken in such cases.

Risk team shall send email communication of such directive to all other stakeholders i.e. Business / Product and Technology teams for their reference. The tracker maintained by Risk team for such directives will be updated accordingly.
[TAT: within 1 working day from the day such information is received]

Risk team shall refer this tracker before giving approval for on-boarding of banks/institutions in any product so as to ensure that no bank/institution is on-boarded where such directive is subsisting.

a. Bank/institution live on any one or more product/s

If the bank/institution is live on any product then the following process will be followed:

i. If operations team confirms that the bank/institution is live on any product, Risk team shall instruct all stakeholders i.e. Business, Technology and Operations teams to off-board the bank/institution through email along with copy of such directive.
[TAT: within 1 working day from the day such information is received]

ii. The Bank/institution should be deactivated by technology team for online products and operations team for offline products (as the case may be) in NPCI's production system for further transactions.
[TAT: within 1 working day from the day such information is received]

However, the Bank/Institution shall continue to be part of the settlement process for transaction life cycle period as defined for each product for settlement of funds for disputes/adjustments raised and/or received by them. (If Bank/institution OR its sponsor bank is still a member of RTGS).

iii. Business team to send an email and formal letter to such member and to the sponsor bank, in case the member is a sub member, informing them on the action taken by NPCI based on the direction of the regulator/competent authority.
[TAT: within 2 working day from the day bank/institution is off boarded]

iv. Operations team to communicate to all other members by issuing an operating circular (OC) informing them on the action taken by NPCI.
[TAT: within 2 working day from the day bank/institution is off boarded]

v. Operations team shall also prepare a checklist as given in **Annexure – A**. Operations team shall update the action taken section and share the scanned copy of the checklist with Risk team (over email) for their records.
[TAT: within 2 working day from the day bank/institution is off boarded]

vi. Product team shall arrange to remove the name of the bank/institution from the live banks list published on the website/landing page.
[TAT: within 3 working days from the day bank/institution is off boarded]

b. On-boarding of bank/institution again once the issued directive ceases

If the bank/institution is to be on-boarded again once the issued directive ceases, following process to be followed:

i. The Bank/Institution concerned should write a formal letter to NPCI requesting NPCI to on-board them again.

ii. Business team should share such request and the directive with Risk team.

iii. Risk team to assess/verify such request and directives from regulator/competent authority, and shall allow to on-board the bank again in that particular product at NPCI, if found appropriate.

iv. **Existing process and TAT** for on-boarding the bank/Institution for each of the product shall be followed by each department of NPCI.

v. Operations team to send a communication to all members in form of an OC once the bank/institution is on-boarded again.

1.2 Off-boarding of member on a voluntary decision of bank/institution

Depending on the business performance, a bank/institution might want to wind up the operations in a city/country or may want to terminate their membership in any one or more products of NPCI.

a. Off-boarding a bank on offline products

TAT: 3 months

Following process shall be followed for off-boarding of bank on offline product:

i. Bank needs to submit a formal request on its letter head duly sealed and signed by appropriate authority of the participant to RBI and NPCI's Business/Operations team. The request should explicitly contain the reason for seeking voluntary termination.

ii. If the bank is a sub member, then such request should be sent through their Sponsor Bank On Sponsor Bank's letter head.

iii. Operations team will intimate Risk team (send email) on the request received from the Bank.
[TAT: within 3 working days from the day such request is received]

iv. Operations team to call for the steering committee meeting (SCM) to decide on the grace period within 14 days from the date of request from the bank. Grace period should not be less than two months from the date of such request. If SCM cannot be called, the decision can be taken via circulation of matter with SC members.

v. Operations team will issue an OC to communicate the voluntary termination of the member and the grace period decided in the SCM to all other member banks in the system.
[TAT: within 2 working days from the day of SCM]

vi. Operations team will prepare the checklist for off-boarding the bank as per

vii. Necessary update in system for AePS/NACH /CTS/NFS/IMPS/UPI/RuPay/BHIM/Bharat QR/BBPS and all NPCI products, as required, will be carried out by Operations team to remove the bank at the end of the grace period.

viii. Operations team will send a communication in form of OC to all other member banks to stop initiating transactions on the blocked bank.
[TAT: within 1 working day from the day bank/institution is off boarded]

ix. Operations team will arrange to remove the name of terminated bank from the live banks list published on the website/landing page.
[TAT: within 3 working day from the day bank/institution is off boarded]

b. Off-boarding a bank/institution on online products

TAT: 3 weeks

Following process shall be followed for off-boarding of bank on online product:

i. Bank/Institution needs to submit a formal request on its letter head duly sealed and signed by appropriate authority of the participant to RBI and NPCI's Business team. The request should explicitly contain the reason for seeking voluntary termination.

ii. Business team to intimate Risk Team (send email) on the request received from the bank.
[TAT: within 3 working days from the day such request is received]

iii. Risk team verify/assess the request and accord approval for off-boarding the bank. Risk team to send email to all stake holders (i.e. Operations, Business, Product and Technology teams) instructing them to off-board the bank/institution.
[TAT: within 7 days from the day such request is received]

iv. For termination of membership, Bank/Institution and NPCI shall be guided by the procedural guidelines issued by NPCI for each of the products.

v. The Bank/institution shall be deactivated by technology team for online products and operations team for offline products (as the case may be) in NPCI's production system for further transactions.
[TAT: within 3 working days from the day such request is received]

However, the Bank/Institution shall continue to be part of settlement process for transaction life cycle period as defined for each product for settlement of funds for disputes/adjustments raised and/or received by them. (If Bank/institution OR its sponsor bank is still a member of RTGS).

vi. Business team to send an email and formal letter to such member and to the sponsor bank, in case the member is a sub member, informing them on off-boarding of bank/institution.
[TAT: within 2 working days from the day bank/institution is off boarded]

vii. Operations team to communicate to all other members by issuing an operating circular (OC) informing them on off-boarding the bank.
[TAT: within 2 working days from the day bank/institution is off boarded]

viii. Operations team shall also prepare a checklist as given in **Annexure – A**. Operations team shall update the action taken section and share the scanned copy of the checklist with Risk team (over email) for their records.
[TAT: within 2 working days from the day bank/institution is off boarded]

ix. Product team shall arrange to remove the name of the bank/institution from the live banks list published on the website/landing page.
[TAT: within 3 working days from the day bank/institution is off boarded]

c. On-boarding of bank/institution again on request from Bank/institution

If the bank/institution is to be on-boarded again, following process to be followed:

i. The Bank/Institution concerned should write a formal letter to NPCI requesting NPCI to on-boarding them again.

ii. Business team should share such request with Risk team.

iii. Risk team to assess/verify such request and instruct internal teams Technology, Business, Product and Operations to on-board the bank again in that particular product at NPCI, if found appropriate.

iv. **Existing process and TAT** of on-boarding the bank/Institution for each of the product shall be followed by each department of NPCI.

v. Operations team to send a communication to all members in form of an OC once the bank/institution is on-boarded again.

1.3 Termination of membership of any bank/institution by NPCI

In case of any breach or severe non-compliance by a member, NPCI may have to terminate the membership of a Bank/Institution in any one or more of the products.

NPCI may also have to terminate the membership of a Bank/Institution, due to suspension or cancellation of RTGS membership of any bank or its sponsor bank, termination of their AUA/KUA license by UIDAI if the Bank/Institution is amalgamated or merged, steps have been initiated by member for winding up the business, etc.

a. Off-boarding a bank/institution by NPCI

TAT: within 2 weeks (can extend if SCM is called)

Following process shall be followed for off-boarding of bank:

i. Originating team (Operations, Business or Product – as the case may be) will send a mail request to Risk teams for seeking approval to terminate the membership of a Bank/Institution in any one or more of the products along with their submission (reason for termination).

ii. Risk team to assess/verify such request and accord its approval for off-boarding the bank/institution if found appropriate. Risk Team to send email to all stake holders (i.e.

Operations, Business, Product and Technology teams) instructing them to off-board the bank/institution.
[TAT: within 7 working days from the day of initiation of termination]

iii. For termination of membership, Bank/Institution and NPCI shall be guided by the procedural guidelines issued by NPCI for each of the products.

iv. The Bank/institution shall be deactivated by technology from online system/ operations team from off line system (as the case may be) in NPCI's production system for further transactions.
[TAT: within 3 working days from the day such initiation received]

However, the Bank/Institution shall continue to be part of settlement process, if the RTGS membership is not suspended/cancelled OR the settlement account with RBI is not frozen.

It RTGS membership of Bank/Institution OR its sponsor bank is not suspended/terminated, then Bank/Institution shall continue to be part of settlement process for transaction life cycle period as defined for each product for settlement of funds for disputes/adjustments raised and/or received by the Bank/Institution.

v. Business team to send an email and formal letter to such member and to the sponsor bank, in case the member is a sub member, informing them on the action taken by NPCI.
[TAT: within 2 working days from the day bank/institution is off boarded]

vi. Operations team to communicate to all other members by issuing an operating circular (OC) informing them on the action taken by NPCI.
[TAT: within 2 working days from the day bank/institution is off boarded]

vii. Operations team shall also prepare a checklist as given in **Annexure - A**. Operations team shall update the action taken section and share the scanned copy of the checklist with Risk team (over email) for their records.
[TAT: Within 2 working days from the day bank/institution is off boarded]

viii. Product team shall arrange to remove the name of the bank/institution from the live banks list published on the website/landing page.
[TAT: within 3 working days from the day bank/institution is off boarded]

Note: For any reason, if the decision is to be taken in SCM, then SCM shall be called or decision shall be taken by circulation of matter with SC members. In such cases the TAT increase to such extant.

b. On-boarding of bank/institution again once the bank confirms on compliance / RTGS membership is activated.

If the bank/institution is to be on-boarded again once the bank/institution confirms on compliance or RTGS membership or UIDAI membership is activated (as the case may be), following process to be followed:

i. The Bank/Institution concerned shall write a formal letter to NPCI requesting NPCI to on-boarding them again.

ii. Business team should share such request with Risk team.

iii. Risk team to assess/verify such request, and instruct internal teams – Technology, Business and Operations to on-board the Bank/Institution again in that particular product at NPCI, if found appropriate.

iv. **Existing process and TAT** of on-boarding the bank/Institution for each of the product shall be followed by each department of NPCI.

v. Operations team to send a communication to all members in form of an OC once the bank/institution is on-boarded again.

1.4 Process of recovery of dues, if any from Bank/Institution is off boarded

i. For online products, Business team to check with finance, operations and product team, whether any amount is due from the bank/institution. If any amount is due, Business team to initiate the process of recovery of the dues.
[TAT: within 7 working days, from the day bank/institution is off boarded]

ii. For offline products, Operations team to check with finance, whether any amount is due from the bank/institution. If any amount is due, Operations team to initiate the process of recovery of the dues.
[TAT: within 7 working days, from the day bank/institution is off boarded]

Annexure –XVIII (Glossary)

List of Important Terms:

Sl. No.	Terms	Description
1	Payer	Person/Entity who pays the money. Account of payer is debited as part of the payment transaction.
2	Payee	Person/Entity who receives the money. Account of payee is credited as part of the payment transaction.
3	Customer	An individual person or an entity who has an account and wishes to pay or receive money.
4	Payment Account (or just Account)	Any bank account or any other payment accounts offered by a regulated entity where money can be held, money can be debited from, and can be credited to.
5	Payment Service Provider	RBI regulated entity that is allowed to offer UPI based payments. Unless otherwise specified, the term PSP shall mean “banks only”.
6	IMPS	Immediate Payment Service
7	2-FA	Two factor authentication.
8	UPI PIN	Personal Identification Number which is used as authorization credentials by the Issuer Bank for debiting customer's account. It will be 4-6 digits numeric PIN only.

9	OTP	One Time Password
10	Payer PSP	The entity on whose interface PIN/Biometric authorization credentials will be captured.
11	Remitter Bank	The entity that will process the debit request
12	Payee PSP	The entity who will provide the Account details against a virtual address credit request.
13	Beneficiary Bank	The entity that will process the credit request
14	SDK	Software Development Kit
15	APK	Application Package provided to PSPs
16	CL	NPCI Common Library, where customer's secured credentials being captured
17	DSR	Daily Settlement Report provided to member banks
18	MCC	Merchant Category Code populated by Acquiring Bank
19	TAT	Turn Around Time

Annexure XIX (P.G Sign-off)

(Bank Acknowledgement and Sign off on UPI Procedural Guidelines)

On Sponsor Bank's Letter Head

To,

The Head Products,
Unified Payment Interface,
National Payments Corporation of India,
Mumbai.

Dear Sir,

Subject: UPI Procedural Guidelines sign off

We, the _____ (Name of the Bank) having its registered office at _____have read and understood the UPI procedural Guidelines.

We do hereby undertake and declare that:

We shall abide by the UPI Procedural guidelines as applicable from time to time including any/all regulatory guidelines applicable to payment transactions in general and mobile banking in specific. The guidelines as stated in the UPI PG shall be binding on us.

The above declaration may please be taken on record by NPCI as our sign off to UPI procedural Guidelines.

Date: Sd…

Place: (Authorized Signatory.)

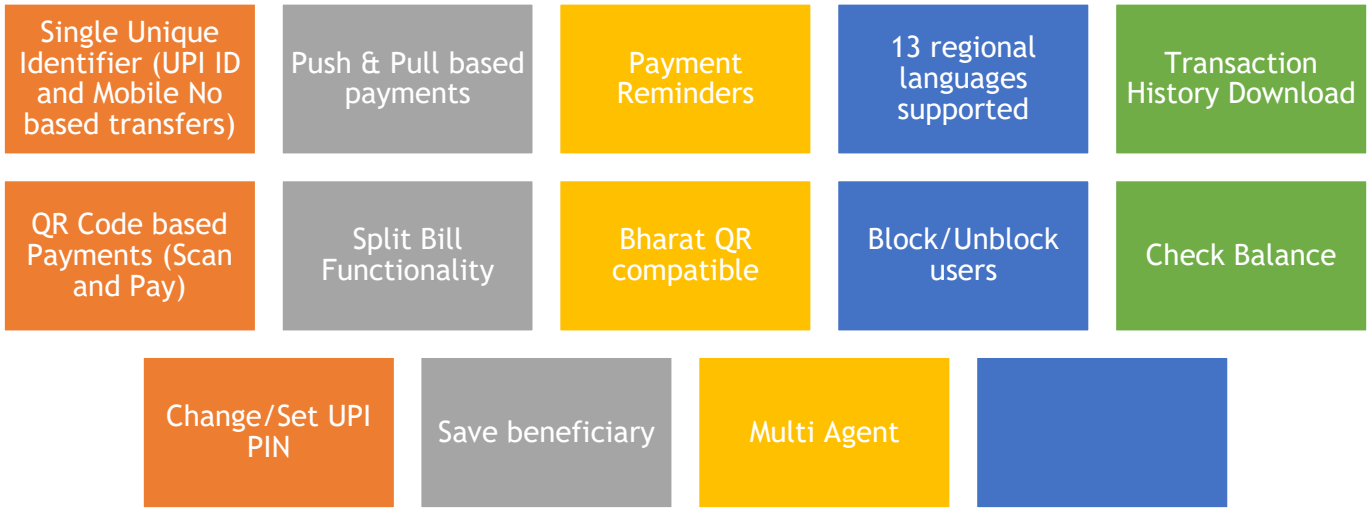
Annexure XX (BHIM,*99# & Role and obligation for BHIM Bill Pay)

BHIM – Bharat Interface for Money/ COMMON APP

About BHIM

Bharat Interface for Money is an app that lets you make easy and quick payment transactions using UPI. It is a starter application where the interface has been kept very simple for first time customers. BHIM reduces the tedious job of filling bank account details again and again for every transaction. BHIM facilitates direct Account to bank payments and instantly collect money using just Mobile number or UPI ID (Payment address).

Features on BHIM



Transaction Sets

a) Account Balance
b) Transaction History
c) Send Money – Mobile Number (In case customer have the mobile number registered on BHIM)
d) Send Money - UPI ID (Virtual Payment Address)
e) Send Money – Account+IFSC
f) Collect Money - UPI ID (Virtual Payment Address)
g) QR – Generate / Pay

Transaction Limit

For sending money using BHIM, the transaction limit has been set to Rs 20,000 per transaction and Rs 40,000 per day per bank account. Any changes in these limits shall be governed by regulatory directives Steering Committee/RBI as applicable.

While NPCI has put in place the validation for restricting transactions up to the approved ceiling on BHIM, banks can also put necessary checks & validations at their end.

Languages

Currently BHIM can be accessed using 13 languages, following are the languages available

a) English
b) Hindi
c) Gujarati
d) Tamil
e) Kannada
f) Telugu
g) Bengali
h) Malayalam
i) Odia
j) Assamese
k) Punjabi
l) Marathi
m) Urdu

Membership and Registration

BHIM membership is open to all the banks which are LIVE in UPI eco system as an Issuer.

The on-boarding process for a member on BHIM platform will commence on successful completion of document verification.

***All the process unless specified such as customer registration process, settlement and dispute management is as per UPI guidelines**

Version 1.0

- Launch version
- Languages supported – English / Hindi
- UPI enabled financial as well as non-financial transactions – viz send/collect money using UPI ID Acct & IFSC & mobile number , account balance , transaction history
- Scan & Pay feature – Read UPI QR
- Generate Dynamic QR Code
- Add / Change Bank Accounts
- Interoperability with *99#

Version 1.2

- BHIM for iOS users
- Languages addition – Malayalam/Kannada/Telugu /Tamil/Odiya/Bengali/Gujarati
- Pay using Aadhaar number of beneficiary
- Functionality of 'Return Transaction' – Send money back to Payer directly
- QR Code – Read & Share
- Save for future (for Acct/IFSC)
- Enable/Disable feature for mobile No. UPI ID created by 'default'
- Deregistering service
- Marking unwarranted collect requests as SPAM
- Introduction of Forgot Passcode, password block after 3 unsuccessful attempts
- Sync PIN set at a different PSP App
- Notification for all requests & activities in the App

Version 1.3

- Languages addition – Marathi, Punjabi & Assamese
- Send Money using Phone Contacts(To BHIM/*99# users
- Blocking/Unblocking feature to protect users from unknown collect requests
- Easy access to saved beneficiaries (on home screen)
- Scan QR saved in phone gallery to send money
- Download of transaction history
- SBI Maestro card acceptance on BHIM
- One time option to edit non-mobile VPA (name@upi)
- Disabling *99# via BHIM
- Introduction of customer referral & merchant cashback scheme

Version 1.4

- New language – Urdu(total languages 13)
- Scan & pay using Bharat QR (with UPI elements) also Scan & Pay without APP login for quick payments
- Push Message and Notification (Geo Location)
- Customizable payment reminder (including UPI ID, Amount, etc.)
- Split bill functionality
- Improvised refund option for wrong credit (customer sends money to unintended person
- Accessibility support for visually challenged
- Filter for transaction history details
- Blocking/Unblocking Misleading UPI ID
- Simplifying customer complaints and Resolution

Version 1.4.1

- Multi Agent Model
- Share with friends
- Security Enhancements
- UPI ID

Version 2.O (Current version)

- Linking Overdraft account in UPI
- UPI Mandate with one time execution
- Invoice in the inbox (view and pay)
- Signed Intent and QR

BHIM BBPS integration:

In order to offer Bill payment functionality to BHIM users, BHIM uses the interoperable platform of Bharat Bill Pay (BBPS). This is done through the technical integration between the two systems and with this, BHIM user will be able to make payment for availing any services from billers on-boarded on Bharat Bill Pay.

Bill Pay approach

BHIM-Bharat Bill Pay integration covers following aspects:

- BHIM system connects to BBPS clearing house, on behalf of BBPS COU (using the IDs of these COUs).
- BHIM to fetch customer bill details from Biller Operating Unit (BOU) of BBPS.
- Customer will initiate Bill Payment through BHIM which will be routed through UPI and the service delivery confirmation will be availed from BHARAT BILLPAY.

Settlement Process for BHIM Bill Pay:

Separate raw file will be provided for BHIM BBPS transactions in the UPI RGCS. It will be an additional raw file to the existing raw files. File format will be shared in the operating circular.
Existing BBPS raw file shall contain the transactions happened in BBPS through BHIM switch (i.e. transaction legs between customer Operating Unit (OU)& biller Operating Unit (OU)) as well as through the customer OU's other channels. However, BHIM initiated BBPS transactions will have a channel specific identifier. For uniquely identifying BHIM Bill Pay transaction in UPI the transaction id will start with "BBP". The same transaction ID of BHIM Bill Pay transactions generated in the UPI leg will be populated in the 'Reference ID' tag of Bharat Bill Pay Confirmation leg.

Disputes Process for BHIM Bill Pay:

Disputes pertaining to the BBPS transactions routed via BHIM switch should be managed in BBPS – CANVAS application same as per the existing process. Existing dispute guidelines of BBPS – RGCS will be applicable for BHIM BBPS transactions/disputes.

On boarding of Banks on BHIM Bill Pay Requirement from member banks:

1. Bank needs to provide UPI ID or A/C+IFSC for the money to be parked at the end of the UPI Transaction.
2. SLA from the bank's side.

Role and obligation for BHIM Bill Pay is explained in **Annexure XX.**

NOTE: Any UPI PSP Application can opt for the BBPS service post satisfaction of all the pre requisites of both the systems. The bank have to be mandatorily **LIVE** in BBPS along with UPI to provide this service.

Unified USSD Platform of NPCI (*99#)

About *99#

*99# (National Unified USSD Platform), the financial inclusion project and part of Prime Minister **'Jan Dhan Yojana'** based on the USSD platform is of national importance and was dedicated to Nation on 28thAugust, 2014. It is an interoperable infrastructure, comprising banks & telecom operators, using USSD technology to provide banking services through a common platform.To transfer funds through *99# customer does not need internet. Customer only needs his mobile number to be registered for mobile banking transactions.

UPI (Unified Payment Interface) is more simplifying way of sending and receiving money launched on 13thAugust, 2016. The need was felt to provide the UPI based services on feature phones by dialling *99# and using USSD technology. Therefore with upgraded version of USSD 2.0 the, user can avail the services of UPI by dialling *99#. This service works across all GSM mobile handsets and on either feature phones or smart phones.

User will be prompt for registration on their dial of *99# for the first time. Once user confirms the Bank Account to link and generates UPI PIN, they are ready for receiving and sending money using UPI over USSD channel.

Objectives of UPI on *99#

- To leverage on high penetration of Mobile phones for offering non-internet based mobile banking service.
- To provide safe, secure, cost effective, 24X7X365, real-time, access to banking services.
- Unifying USSD system with UPI platform for interoperability
- To be a catalyst in facilitating financial inclusion process and to provide banking services to even last mile customer.
- One Step on-boarding process allowing users to send /receive money

Features

- Standardized Menu for Banks and Customers
- Facilitates interoperable mobile banking transactions
- Works across all handsets(Basic & Smartphones) & GSM service providers
- Works without internet and service available while roaming as well
- Multilingual options (Available in 13 languages including English & Hindi)

Transaction Set

- Send Money using Mobile Number / Payment Address / Saved Beneficiary / IFSC & A/C No
- Request Money using Mobile Number / Payment Address
- Check Balance
- My Profile- Change Bank Account, Change Language, My Details, Payment Address, Manage Beneficiary
- Pending Requests(collect requests pending)
- Transactions(last 5 *99# or BHIM transactions linked with same account)
- UPI PIN- Set/Forgot UPI PIN, Change UPI PIN

Service variants

- *99# - Financial and Non-financial Transactions

Transaction Limit

For sending money using *99#, the transaction limit as prescribed by RBI for unencrypted channel shall be applicable. Currently this limit is Rs 5000/- for transactions initiated using unencrypted channel.

Languages

Currently *99# can be accessed using 13 languages, following are the languages available

a) English
b) Hindi
c) Gujarati
d) Tamil
e) Kannada
f) Telugu
g) Bengali
h) Malayalam
i) Odia
j) Assamese
k) Punjabi
l) Marathi

m) Urdu

Membership and Registration

*99# (USSD) membership is open to all the banks which are LIVE in BHIM eco system as an Issuer.

The on-boarding process for a member on USSD platform will commence on successful completion of document verification as applicable.

***All the process unless specified such as customer registration process, settlement and dispute management is as per UPI guidelines**

ROLES AND OBLIGATIONS OF BHIM BILLPAY:

a. NPCI shall maintain the network infrastructure necessary to the operation of UPI systems & UPI BHIM/COMMON APP, ensuring working of the Interface / switch on 24 hours a day, 7 days a week with a monthly uptime of99.5%.
b. NPCI may use the services of third parties for maintenance of the UPI Common APP and the UPI systems or any of its infrastructure or for any other support required for the delivery of the service under this agreement subject to adequate security procedures as envisaged under this agreement.
c. Information of the customer registering on the NPCI Common app shall be kept confidential and shall be used solely for the purpose of enablement on the UPI Common App.
d. As part of the authentication framework, NPCI shall be responsible for hard-binding the device of the customer on which the UPI COMMON APP has been downloaded. NPCI shall also be responsible for holding the device hard-binding details in a secure and encrypted manner and authenticating such device hard-binding as the factor of authentication from subsequent transaction. The first transaction or set UPI PIN shall be duly authenticated by the customer's bank with customer entering 2FA as per RBI guidelines and as per UPI guidelines.
e. UPI Common APP shall assign a common default handle as "@upi" for the registrations done by the customers, towards identification and resolution of the customer details held on NPCI PSP interface.
f. NPCIshallmaintainallrequisiterecords,registers,accountsbooksetc.,asapplicabletoit, whichare obligatory under any law to the use of UPI Interface & the UPI COMMON APP and shall provide any information as may be required under any statutory obligation.
g. NPCI in its role of the UPI network shall be responsible for switching the transactions including the transactions originated from the UPI COMMON APP and hence it shall charge the UPI switching and settlement fee as currently applies to the entity as applicable.
h. As a part of its services relevant to the UPI Framework, NPCI shall provide the front end COMMON APP including the option of raising complaints for the customers. The customers can raise a complaint in the UPI COMMON APP, where-in NPCI shall ensure to provide for the upload and resolution of complaints as per the dispute life cycle as applicable for UPI Operating and Settlement guidelines.
i. All costs – including Project, Infrastructure and any other Hardware & Software and the related systems shall be borne exclusively by NPCI for provision of UPI COMMON APP.
j. As a part of value added services, NPCI shall integrate Bharat Bill Payment System

("**BBPS**") with UPI COMMON APP, and shall be entitled to charge the switching and settlement fee, to Bank/PSP, under the aegis of the procedural guidelines and circulars related to Unified Payments Interface (**"UPI"**) and BBPS issued by NPCI from time to time.

k. NPCI shall, on best efforts basis, ensure to extend its support to Bank/PSP to handle/resolve any bill payment issues & queries, if any, raised by / referred by any customer of Bank/PSP. However, it is clarified that ultimate and prime responsibility to resolve any such grievances shall at all times reside on Bank/PSP.

2. ROLES AND OBLIGATIONS OF THE PSP / BANK:

a. PSP/BANK shall continue to comply with all requirements existing and future with regard to and in connection with the appointment and continuance as Bank under the RBI License terms in its own capacity.
b. PSP/BANKS shall not have the right to have an audit either directly or through any 3rd party on the systems, Processes, Architecture, Network and any other hardware/Software services procured and deployed by NPCI for provision of the COMMON UPI APP. RBI may however audit the systems and processes of NPCI as per the extant regulatory procedures & guidelines.
c. PSP /BANKS shall not disclose, reveal or publish any material information relating to operations, software, hardware, etc. of the NPCI PSP Interface and/or UPI COMMON APP without prior written consent of NPCI authorities.
d. PSP/BANKS shall take full responsibility as defined in the UPI procedural guidelines duly approved by RBI for playing the PSP role.
e. PSP/BANKS - shall be responsible and ensure to reverse the amount of the transaction *(as would be entered by customer towards payment of any biller)*, to the customer's account *(through which the transaction has taken place)* following the settlement process defined in the OPG, once it is ascertained by PSP/BANKS that though account of the customer has been debited, the transaction has not been successfully processed.
f. PSP/BANKS shall be responsible to handle/resolve any bill payment issues & queries, if any, raised by / referred by any customer of PSP/BANKS
g. PSP/BANKS shall be responsible to maintain a separate pool account for all bill payment transactions and share the same with NPCI, enabling NPCI to process, settle & reconcile the same.
h. In order to extend the facility of BBPS to its customers through UPI COMMON APP Banks- hereby confirms that it has entered and executed necessary documents/Agreements with NPCI and shall ensure to keep them valid and subsisting during the entire term of this Agreement.
i. Bank/PSP shall ensure to adhere to all the procedural guidelines, circulars and standards related to UPI and BBPS issued by NPCI from time to time.

Annexure XXI – UPI 2.0

1.1 Linking overdraft account on UPI

User can now link his/her overdraft account in any UPI App like saving bank and other accounts. This shall help in digitisation of OD account usage. There shall be no difference in the user experience while doing transaction in OD account, from the existing UPI user experience.

1.2 UPI Mandate with One Time Execution Block Funds

Mandate functionality in the retail payments systems refers to the functionality wherein a customer authorize future debit of his/her bank account by authorizing before. With 2.0 UPI also will have the mandate functionality, however each mandate created in UPI shall be for one time execution only and for the purpose for which the mandate was created and customer account shall be blocked for the equivalent amount immediately with the mandate creation . UPI mandate currently does not have the functionality of recurring payments through one time authentication.

UPI mandate allows user's account to be debited as per the agreed terms and condition when the payee initiates the collect request for funds. In this case the user does not need to authenticate the transaction since a mandate for this debit has already been given by him. This functionality shall have its own mechanism of generating/accepting mandates; independent of any similar services available in the ecosystem.

The mandate with recurring execution and without block is currently not offered as part of the UPI mandate. UPI mandate service will allow both payer and payee to create mandates and is available for all types of transactions such as P2P & P2M. While UPI Mandate creation can be done as push (Payer initiated) or pull (Payee initiated) and using QR/Intent, however mandate execution shall also be payee initiated and shall be similar to an existing collect transaction. Clear distinction between the UPI Mandate and regular transactions shall be made, also the record of mandate created & executed shall be provided by the PSPs.
Note: Mandate cannot be created for the sole purpose of blocking only, it has to be followed by financial transaction unless revoked or in ASBA/ IPO like scenario where shared are not allotted.

Use cases: All possible scenarios where funds are to be blocked towards future payment (one time), UPI Mandate is expected to be used in below.

- Gifting (individual ,Corporate and Employee incentives)
- Rent payments
- E-com transactions
- Hotels booking
- Cab booking etc. are few of the likely scenarios.

1.3 Invoice in the inbox

UPI has a provision where the merchants can share Invoices/invoices with the customers before the transaction is authorised. This will help customers to verify the invoice details such merchant name, amount, due date etc. before making the payment. This functionality shall be available only for the verified merchants.

The invoice can be embedded as URL and that be accessed through clicking link in a collect request or scanning QR or intent.

The Invoices/invoices can either be downloaded as PDF or can be viewed on a browser. This provision requires the PSP applications to display an option called 'view invoice'. This option will be present for collect transactions and intent/QR initiated pay transactions. Entities/merchants can raise collect request for all outstanding payments. This collect request may also contain the Invoice / invoice details for the user to check before making a payment.

When the user scans a QR or triggers an intent carrying URL tag then he will get an option on the app to click that URL. This URL can redirect him to the invoice which can be either viewed or downloaded (As per the PSP). If URL is not passed then 'view invoice' shall be disabled. Similarly for collect requests received on handset, by clicking the 'view invoice/Invoice' option the URL can be browsed. The URL embedded in the request should be secure, come from a secure source and should only display the details relevant to that user.

1.4 Signed Intent

Objective of intent/QR based payments is to incorporate simplicity, security and seamlessness in UPI transactions. Intent/QR method also makes payment integration easier for merchants providing scope for new use cases.

Existing intent/QR payment method allows the UPI User to complete the transaction, invoking the PSP application by means of Android/iOS intent, QR, NFC, BLE and UHF. The invoked application prompts the UPI User to enter UPI PIN to complete the transaction. The current implementation of intent is invoked by merchant application shooting intent or merchant terminal pushing channel specific intent. The existing intent/QR reception on PSP application faces the below challenges:

a) Any application/terminal can act as a source of an intent/QR and can imitate as an authorized source or may spoof the UPI User by altering terminal, populating incorrect payment details.
b) The intent is received by PSP application, the UPI User has to enter application passcode followed by his UPI PIN to complete the transaction which acts as an additional step creating

friction in paymentIn order to overcome the challenges in the existing intent/QR mechanism in UPI signed intent/QR is being introduced. Signed Intent/QR is expected to provide an additional layer of security, simplify transactions and bring sanity across ecosystem for intent/QR based payments. With the signed QR, issues related to tampering QR as well as having non-verified entities shall be reduced.

1.5Foreign Inward Remittance (FIR)

UPI has received necessary RBI approval to process the domestic leg of foreign inward remittance to member's account. UPI shall only act as an additional channel available for processing such transactions and it shall be incumbent upon members, at both end, to abide by the necessary regulatory guidelines as issued under/by FEMA,RBI or any other competent authorities from time to time, such transfers can take place only to KYC compliant accounts. Further. (Refer **UPI circular 48 dated May 9, 2018**)

- Transaction would be in Indian Rupees between the Intermediary bank, NPCI and beneficiary bank.
- NPCI shall define the limit for such transactions, however in absence of any such limit, it shall be same as that of prevalent UPI transaction limit.

Roles & Responsibilities

UPI Mandate, Overdraft Facility, Signed Intent & QR, Invoice in the Inbox

Project	Roles and Responsibilities		Payer PSP	Payee PSP	Rem	Bene	NPCI/ UPI	Remarks
Mandate		**Passing Attributes**						
	Create	Initiate a Create	✓	✓	✓	No Role		Both Payer and Payee can create a mandate; Issuer generates a signature block
		Generate UMN	✓	No Role	No Role	No Role		UMN is always generated at end of Payer PSP
		Block & Unblock Fund functionality	✓	✓	✓	No Role		Block/ Unblock Fund will be initiated by Payer or Payee PSP. But the complete responsibility of blocking and unblocking the account will lie with remitter. Remitter bank to keep the fund blocked between start date and end date or till the execution of mandate whichever happens first. Post expiry/ end date the block fund should be unblocked automatically.
		Check on the rule & recurrence pattern	✓	✓	✓	No Role		Rule must be checked by Payer PSP, Payee PSP and remitter. PayeePSP must initiate the mandate with correct credentials. Payer PSP acts as

								fist level of check but remitter bank has the ultimate responsibility before debiting.
		Check on expiry date	✓	✓	✓	No Role		Rule must be checked by Payer PSP, Payee PSP and remitter. PayeePSP must initiate the mandate with correct credentials. Payer PSP acts as fist level of check but remitter bank has the ultimate responsibility before debiting.
		Check on amount	✓	✓	✓	No Role		Rule must be checked by Payer PSP, Payee PSP and remitter. PayeePSP must initiate the mandate with correct credentials. Payer PSP acts as fist level of check but remitter bank has the ultimate responsibility before debiting.
		resolution of VPA	✓	✓	No Role	No Role		VPA must be resolved at Payer PSPS and Payee PSP end based on who created the mandate
		Passing the account details	✓	✓	No Role	No Role		Payer and Payee PSP must resolve the VPA and pass the account details

		Validation of UPI PIN	No Role	No Role	✓	No Role		UPI PIN will be passed by the Payer PSP but will be validated by issuer only
		Signing mandate	No Role	No Role	✓	No Role		Issuer Should sign mandate
		Storing DS	✓	No Role	✓	No Role		Payer PSP should store DS. Remitter is also suggested to store DS to cross check the DS of creation and execution.
		Share to Payee	✓	No Role	No Role	No Role		Payer PSP either turns flag on / off based on the payers decision to inform the Payee or not
	Modify	Initiate a Modify	✓	✓	✓	No Role		Payer or Payee can initiate a modify. In both the scenarios Modify must be authorized by the Payer by entering UPI PIN. remitter bank must make a note of the modify at his end.
		Ensure Modify has been executed successfully	✓	✓	✓	✓		All parties must ensure modify is executed successfully
	Revoke	Initiate a revoke	✓	✓	✓	✓		Payer and Payee invokes revoke. But in cases of mobile being stolen where customer cant invoke revoke through his PSP he can approach bank. Payer enters his pin for revoking a mandate. Payee initiated revoke

								does not require payer authorization.
		Ensure revoke has been executed successfully	✓	✓	✓	✓		All parties must ensure revoke is executed sucessfully
		Revoked mandate has not been executed	✓	✓	✓	✓		All parties must ensure revoke is not re executed
		SMS communication	✓	✓	✓	✓		All parties must ensure revoke notification reaches all the parties
	Execution of mandate	Presentment of Mandate	No Role	✓	No Role	No Role		Payee PSP only can present a mandate
		Passing DS	✓	No Role	No Role	No Role		Payer PSP must pass the DS while payee has invoked a mandate
		Debiting the amount/ Validation of DS	No Role	No Role	✓	No Role		remitter should validate DS before executing a mandate
	Failure of mandate	Mandate Failure	✓	✓	✓	✓		All the parties must ensure that mandate is failed and notified to all the parties
	Pause (Optional functionality)	Presentment of Pause	✓	No Role	✓	No Role		Payer PSP and remitter can invoke a pause
Customer Grievance	Customer Grievance/ Dispute Management	App issues/ other issues	✓	✓	✓	✓	Arbitrator of the last resort	Allthe parties must ensure that notification is sent to the

								remitter and Beneficiary. NPCI is arbitrator of last resort.
	Customer communication/ Intimation	Notifications/ SMS	✓	✓	✓	✓		Allthe parties must ensure that notification is sent to the remitter and Beneficiary
Limits	Limits	Limits	✓	✓	✓	No Role	✓	Payer, Payee, remitter must check limits. NPCI has central level checks for the main limits.
OD	Creation	List account	✓	No Role	✓	No Role		Remitter must fetch the list account when called by Payer PSP.
	Execution	OD to only P2M execution	✓	✓	No Role	No Role	✓	Payer, Payee must check OD listing. NPCI has central level checks for allowing OD txn.
Signed Intent/ Signed QR	Creation (P2P)	Upload and Store Keys	✓	✓		☐	✓	PSP to create signed intent/ signed QR.PSP to upload the keys of individual through UPI. UPI to keep a repository of all the keys.
	Execution (P2P)	Fetch Keys	✓			☐	✓	It's the role of the Payer PSP to call List Keys and fetch keys before execution of QR/ Intent call. UPI responds to List Keys API call.
			Issuer PSP	Acquiring PSP	Issuing Bank	Acquiring Bank		

	Creation (P2M)	Upload and Store Keys		✓		✓	✓	Acquiring bank to create signed intent/ signed QR.Acquiring bank to upload the keys of merchants QR/ Intent using Manage VAE. UPI to keep a repository of all the keys.
	Execution (P2M)	Fetch Keys	✓			☐	✓	It's the role of the Issuer PSP to call List VAEand fetch keys before execution of QR/ Intent call. UPI responds to List VAE call.
Invoice in the box	Execution	Uploading Link/ doc		☐		✓		Acquiring bank to upload the link free from virus and from a secure source and a verified domain
		Displaying the Link/ doc	✓					Issuer PSP to read the link and display the link to his customer to view the bills before paying.

UPI 2.0 App Checklist

The purpose of the below Checklist is to ensure that the UPI based Application **(Android ,iOS and others)** have the same look and feel across applications of different entities for all the functionalities of UPI 2.0.

Note:

- Application release in public domain cannot happen without this Checklist clearance & explicit approval from NPCI end.
- This checklist is in addition to the functionalities of UPI 1.0.

1. UPI Mandate- with one time execution and block functionality

Below are the scenarios where implementations on UPI mandate for PSP App (P2P)

UPI PSP Application Name	Payer initiated mandate (Mandatory/ Optional)	Payee initiated mandate (Mandatory/ Optional)
	M	NA

UPI-Mandate for PSP Apps: P2P App

Mandate features on UPI-Mandate home screen:
The PSP App must not alter the *Nomenclature "UPI-Mandate" it must be same across all PSP apps.*

UPI Mandate Options	Mandatory/Optional/ Conditional	Yes/No	Description/ Comments
UPI-Mandate to be prominently displayed: Below are the option to be made available			
Mandate Create *(Payer initiated mandate)*	M		
Mandate Request received *(Approve incoming Mandate request)*	M		
Mandate history *(All details of executed or failed mandates)*	M		
My Mandate (ongoing/active/ revoked/ modified mandates with subsequent Action)	M		
Scan Mandate QR *(To test and qualify UPI Mandate Linking Specifications Version 1.0)*	M		

Specifications of Functionalities of UPI-Mandate: (Actions applicable to the Payer)

Attribute Name	Initiator	Mandatory/Optional /Conditional	Yes / No	Description/ Comments
Create Mandate				
To be allowed on only UPI ID	Payer	M		
Beneficiary name* *(Nick name)*	Payer	O		

Validity date : • Start Date (>= the creation date) • End Date (Expiry date)	Payer	M M		Period between the creation date and end date shall not be more than 90 days (eg: creation date 1st August 2018 and end date can be up to 30th Oct 2018) creation date can be defaulted to start date
Amount	Payer	M		
Amount Rule (Fixed/Up to (Max.)	Payer	O		In P2P, amount rule = Fixed/ exact default and keep the same in backend. Max rule can be applied on P2M txns on the discretion of the merchant acquiring bank.
Recurrence pattern (one time only)	Payer	M		
Remarks	Payer	O***		
Inform Recipient Button*	Payer	M		
Prompt UPI PIN mandate creation	Payer	M		
QR Generation – Post mandate creation	Payer	M		
Create mandate for Payee/ Merchant initiated mandate:				
Mandate creation - By authorising Collect request	Payer	M		
Mandate creation – Through QR code	Payer	M		
Mandate creation – by Merchant intent request	Payer			
Mandate approval screen for Payee initiated mandate **MUST** be non-editable	Payer	M		
Modify Mandate (allowed only up to 24 Hrs before the end date)				
UPI ID	Payer	NA		
Beneficiary name* (nick name)	Payer	NA		

Validity date : • Start Date (>= the creation date) • End Date (Expiry date)	Payer	NA M		Modification of End Date should be limited to the Maximum date allowed for Amount blocking from the Creation date. As per 90 dats rule between creation date and end date (eg. creation date 1st Aug 2018 and end date 29th aug 2018 than end date can be modify up to 30th oct 2018)
Amount	Payer	M		
Amount Rule (Fixed/Up to (Max.))	Payer	NA		
Recurrence pattern (one time)	Payer	NA		
Remarks	Payer	O		
Inform Recipient Button*	Payer	NA		
UPI PIN while modification of mandate	Payer	M		
Generate new mandate QR Code after creation of the Mandate	Payer	M		
Revoke Mandate (allowed only up to 24 Hrs before the end date)				
Revoke	Payer	C***		
UPI PIN while revoke of mandate	Payer	M		

***Nomenclature is to be decided by the bank in their application.*

***optional for customer but tag needs to be pass in back end.*

**** For merchant initiated mandate with Revoke flagged as "N ", the option to revoke MUST not be made available.*

Specifications of Functionalities of Mandate: (Actions applicable to the Payee)

Attribute Name	Initiator	Mandatory/Optional /Conditional	Yes / No	Description/ Comments
Intimation to Payee on Mandate creation				
Mandate creation detail on Payee PSP if tag "Share to payee = Y"	Payee	M		

No Mandate creation detail on Payee PSP if tag “Share to payee = N”	Payee	M		
For Mandate Execution				
Mandate Execution by scanning the mandate QR (For both cases “Share to payee = N/Y”)	Payee	M		
Provision of Mandate execution button on the app for tag “Share to payee = Y”	Payee	M		
Mandate approval screen for Payee initiated mandate **MUST** be non-editable	Payee	C*		
For Revoke Mandate (allowed only up to 24 Hrs before the end date)				
Revoke	Payee	M		

***** *Only Amount field can be editable in case the amount rule is ‘max’*

Communication to Users post Mandate creation: Payer/Payee

Actions	Initiator	Mandatory/Optional /Conditional	Yes / No	Description/ Comments)
SMS/notification to user	Payer/payee	M		For mandate creation, modification, revoke, (success failure and pending etc.) as well as at the time of execution.
Confirmation page with details on creation/ modification/ revoke /Executing Mandate	Payer/payee	M		Before entering the UPI PIN

Other Hygiene Factors

Actions	Mandatory/Optional/ Conditional	Yes / No	Description/ Comments)
Actions to be performed by payer for Payee/merchant initiated mandate			

Alert for Mandate request (Incoming Collect)	M		
Provision to decline the collect request	M		
Blocking or SPAM for Mandate request(Incoming collect)	M		
Blocking or spamming – Not applicable for verified merchants	M		
Provision to accept the Mandate request	M		
UI to confirm Mandate before final creation	M		
Other Actions			
Mandate transaction history(both financial and nonfinancial) • Minimum 10 transactions Detail in transaction • Transaction ID • UMN Number • Beneficiary and Remitter UPI ID • Start date and End date • Date & Time • RRN • Amount • Remarks • Ref ID	M M M M M C* C* M C** M(For P2M)		The PSP may choose to display information over and above these to customer REF ID should be shown to the user when request is received
My mandate (All Mandate detail)	M		
Raise a query/ Dispute (Option against each transaction should be there - RGCS response)	M		Banks to decide on the parameters
While raising the query /dispute, the App should display all transaction details	M		Banks to decide on the parameters
SMS/ notification to user while • Creating the mandate • Sending Collect request for mandate • Revoking the mandate • Modifying the mandate	M M M		

• Execution of the Mandate	M M		
App should verify the UPI ID display CBS name/ Merchant	M		
Display of expiry time for incoming mandate collect request	M		
Default validity of 30 minutes in case Merchant/customer fails to specify expiry time for the collect request sent	M(for normal collect)		
2,00,000*** limit to be available at each PSP and issuer bank per Mandate transaction per day	M(for SEBI Transactions)		
Prohibit deregistration of mandate – In case of any active/ pending mandate execution against the UPI ID	M		
Compliance to UPI Mandate Linking Specifications Version 1.0	M		

**in case of financial transaction*
***if the remarks are being sent by the psp/merchant then app has to show the same to the user in front end*
**** Limit may be subject to change based on guideline issued by NPCI*

2. Overdraft facility on UPI

Models	Type of services	Payer availing Overdraft facility (Mandatory / Optional)
Bank PSP Apps/BHIM	**P2M***	**M**
	Both P2P & P2M**	**M**

** Only P2M transactions allowed on unsecured O/D.*
*** Both P2P & P2M transactions allowed on secured O/D.*

Overdraft for Bank PSPs

Home screen

Sr.	Functionality	Mandatory/Optional/ Conditional	Yes / No	Description/ Comments
i.	Add/Link an Overdraft bank Account	M		
ii.	Set UPI PIN/Change UPI PIN	C*		
iv.	Balance enquiry	M		
v.	Transaction	M		

**May be applicable subject to issuer banks policy for UPI PIN set*

Add /Link an Overdraft bank Account

Actions	Mandatory/Optional/Conditional	Yes/No	Description/ Comments
Bank to display "**Overdraft Account**" while fetching/ Adding of account	M		
Name "Overdraft account" should be shown in the Bank Account profile along with savings and current account to the user.	M		
Overdraft account should be shown instead of UOD/SOD	M		
UOD on-boarding message "Only P2M transactions allowed" to be displayed to customer upon account fetching	M		
Repayment to the OD Account should be allowed	M		

Balance Enquiry

Actions	Mandatory/Optional/ Conditional	Yes/No	Description/ Comments
UPI Pin Preapproved	O		

UPI Pin Non Preapproved	M		
Show below detail while balance enquiry : • Total limit • Available Limit	M		

Transaction: Pay using overdraft

Attribute Name	Mandatory/Optional /Conditional	Yes / No	Description/ Comments
Transaction to : 5. UPI ID 6. A/C & IFSC 7. Mobile number (app specific)	 M O* O		
All type of transaction for SOD	M		
Only Merchant transaction for UOD	M		

**However, A/c & IFSC based transaction mandatory for Bharat QR*

Other Essentials

Actions	Mandatory/Optional/ Conditional	Yes / No	Description/ Comments
Overdraft Transaction History • Minimum last 10 transactions Below detail in transaction : • Transaction ID • Beneficiary and Remitter UPI ID • Date & Time • Amount • RRN	 M M M M M M		
Raise a query / Dispute (Option Raising a query/ Log a complaint against each transaction should be there)	M		Banks to decide on the parameters
While raising the query/dispute, the App should display all transaction history details	M		Banks to decide on the parameters

3. Signed intent/QR

Below are the scenarios where implementations on Signed Intent third party application.

Models	Type of Transactions	Payer availing Signed Intent /QR facility (Mandatory / Optional)
Bank PSP Apps/BHIM	**P2M**	**M**
	P2P	**M**

For Signed Intent – As a Payer PSP

Pay Transaction:

Actions	Mandatory/Optional/ Conditional	Yes/ No	Description/ Comments
Response to Intent & to surface the App on the phone	M		
Notification for unsigned Intent – "Notification message"	M		
Notification for Signature Mismatch – "Error message"	M		
Skip passcode in case of signed intent	M		
Payment confirmation Page (Details: Bill No, Merchant Name, Amount, Transaction ID and complete details)	O		
Pay using UPI PIN	M		
Payment Confirmation Page	M		
App to pass the control to merchant app, along with mandatory response parameters – TID, Tr, Amount, Tnx status & RespCode	M		
Compliance to Deep Linking Specs 1.6	M		

For Signed QR– As a Payer PSP

Pay Transaction:

Actions	Mandatory/Optional/	Yes/ No	Description/ Comments

	Conditional		
Provision of “Scan & pay” in the app	M		
Notification for unsigned QR – “Warning Message”	M		
Notification for signature mismatched – “Error message”	M		
Payment confirmation Page (Details: Bill No, Merchant Name, Amount, Transaction ID and complete details)	M		
Pay using UPI Pin	M		
Payment Confirmation Page	M		
Compliance to Deep Linking Specs 1.6	M		

4. Invoice in the inbox (View &Pay)

Below are the scenarios where implementations on Signed Intent third party application.

Models	Type of Transactions	Payer invoice in the inbox facility (Mandatory / Optional)
Bank PSP Apps/BHIM	**P2M**	**M**
	P2P	**NA**

Behaviour on the PSP App

Actions	Mandatory/Optional/ Conditional	Yes/ No	Description/ Comments
Invoice in the inbox is applicable for verified merchant	M		
Display invoice on the following mode of transactions • QR • Intent • Collect request	 M M M		
Link to be prominently displayed eg. **“click here to view the attachment"** & the url should not be visible to the customer	M		
Invoice to be shown in transaction history(for success /failure/pending) page as well - "Click here to view the attachment"	M		
Skip passcode upon return post invoice view	M		

Compliance to Deep Linking Specs 1.6 – With mandatory parameters.	M		

5. Miscellaneous

Actions	Mandatory/Optional/ Conditional	Yes/ No	Description/ Comments
When a User put the UPI ID/ Account + IFSC of Payee/payer in the app. App should display the CBS verified name	M		
After Mandate Creation, If the default bank account is changed, Mandate should not fail.(check for Modify and revoke)	M		
For above scenario, multiple accounts from same bank are added and default account is switched	M		
multiple accounts from different banks are added and default account is switched	M		
After Mandate Creation, Should not be able to delete the Active Mandate bank account	M		