भारतीय राष्ट्रीय भुगतान निगम
NATIONAL PAYMENTS CORPORATION OF INDIA

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 1.5

July, 2016

CONTENTS

Introduction

The Unified Payments Interface (UPI) offers architecture 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 besides creating interoperability and superior customer experience.

The key aspects of the Unified Payments Interface are:

a) The Unified Payments Interface permits payments via mobile app, web etc.
b) The payments can be both sender (payer) and receiver (payee) initiated.
c) The payments are carried out in a secure manner aligned with the extant RBI guidelines.
d) The payments can be done using Aadhaar Number, Virtual Address, Account Number& Indian Financial System code (IFSC), Mobile Number & MMID (Mobile Money Identifier).
e) The payment uses 1-click 2-factor authentication, Biometric Authentication and use of payer's smartphone for secure credential capture etc. are other unique features.

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).

b) Simplifying Issuance Infrastructure – The virtual addresses/payment 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 easy, low cost and universal.

d) Enabling 1-click 2-Factor Authentication – UPI allows all transactions to be at least 2-FA using mobile and second factor (PIN or Biometrics) makes all transactions compliant with the existing regulatory guidelines.

e) End-User Friendly - Customers can make or receive payments with ease and security to/from friends, relatives, merchants, pay bills, etc. all using their mobile phones without sharing banking credentials. Alerts and Reminders, consolidation of multiple banking relationship via single mobile app, use of special purpose virtual addresses, etc. simplifies end-users experience.

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

g) 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.

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

Sl.	Challenge	UPI Offerings
1	Pull Based Mobile transactions	UPI permits real time Push & Pull transactions.
2	Options to customers	Customers can pay using multiple identifiers (Aadhaar Number, Virtual Address, Account no & IFS code, Mobile No & MMID). Payment can be requested on one interface and authorised on a different interface.
3	Single Identifier Fund Transfer	Funds can be transferred using Aadhaar Number stored in the NPCI Mapper. Local resolution by the Payment Service Provider using Virtual Address mapped to the Account at the time of registration by customer.
4	1 Click 2 FA	Single click two factor authentication enabled using Device Fingerprint as the first factor & PIN/Biometrics as second factor of authentication
5	Current Market Trend	Designed to embrace the smartphone boom in India & the inclination of customers to move to digital mobile based solutions

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 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.

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 and efficiency and risk guidelines issued by NPCI from time to time.

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 to provide an audit report for the Data Center & PSP App by CISA equivalent auditor. The Qualified Security Assessor (QSAs) empaneled 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.

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

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 steps have been initiated for winding up the business of the member.
    e. Suspension or cancellation of RTGS membership.
    f. 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.
- 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.
- UPI 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 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 SGM or a consolidated SGM subject to all requisite approvals being in place.
- UPI 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.

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.

Furthermore, the PSP may limit the UPI offerings to its own bank customers provided the bank allows its customers to register/get on-boarded with other PSP Apps. The PSP shall support the below transactions:

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

b) Non-Financial transactions including Mobile Banking Registration, Set & Change PIN, OTP Request and Mini Statement

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.

Addresses Allowed:

Transactions can be done using Mobile Number& MMID, Aadhaar Number, Account Number & IFS Code and Virtual 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	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 or Aadhaar No 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

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 3PSP handles. Any changes in this regard shall be governed by the Steering Committee direction/decision.

For transactions based on Aadhaar Number as the sole identifiers, the address resolution will be done by NPCI. These identifiers will be mapped to IINs (Bank Identifiers similar to NBIN in IMPS) in NPCI Centralized Mapper. However, actual account identification will be done at the beneficiary bank's end. Bank will have to do the integration at their end to credit the transaction based on Aadhaar Number and IIN. The customer may also enter the Account Number & IFSC and Mobile Number & MMID as the beneficiary inputs for sending money

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, Aadhaar Number, Virtual Address etc.
   b. *Collect Request*: A Collect Request is a transaction where the customer is pulling funds from the remitter by using 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 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 PIN.**

- For biometric based authentication, IRIS/Fingerprint is the second factor which will be validated by UIDAI (Trusted Third Party) on behalf of Issuer Bank. The Bio-metrics which are locally stored shall not be supported under this mechanism.

Below table represents the summary of the two factor 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	PIN/Biometrics*	Issuer	PIN /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.

Transacting Parties:

There are maximum upto four parties 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.

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

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 PKI Encryption.

NPCI will be using Public Key Infrastructure (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.

Biometrics/IRIS will also be captured in a secured way as per UIDAI framework guidelines. Only UIDAI supported biometrics authentication will be supported in UPI. Closed loop biometric authentication will not be supported as they do not extend the validation to UIDAI (Trusted Third Party).

Originating Channels Allowed:

Banks may decide their own way of authorization of transactions and channel when the transaction is a pre-approved transaction for UPI. Pre-approved transactions are those transactions where the Payer PSP & Remitter Bank are one entity and the transaction is received to NPCI only after debiting the Remitter's account. However, for all Collect Requests, authorisation has to be done on the Mobile App (Mobile Channel). Use of NPCI libraries in such cases will depend on the PSPs.

For Pay Requests where the transaction is not a pre-approved transaction, the initiation channel will be Mobile App (Mobile Channel) and the authorisation parameters shall be secured credentials (PIN) or Biometrics (IRIS, Fingerprint). The Mobile App needs to use NPCI libraries for capturing these secured credentials.

Collect Requests carrying details like Virtual Address can be initiated from a non-mobile channel depending on the requirements of the bank, but authorisation of such transactions by the Payer customer has to be on PSP App (Mobile channel), where the customer gets notification of the Collect Request.

Transaction Limit: UPI transaction limit will be pegged with IMPS transaction limit which will change from time to time following the approval from the IMPS/UPI Steering Committee. As per extant approval from the steering committee, the upper cap per UPI transaction will be Rs. 1 Lac. Accordingly it is mandatory for the banks to set a default limit of Rs. 1 lac per transaction for UPI to begin with. Banks cannot set a different upper limit for their customers and have to mandatorily have the default limit to be set to Rs. 1 lac.

Settlement of UPI transactions and Reports availability:

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

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*.

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.

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.

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.

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.

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.

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 with the same could invite legal proceedings
- 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.

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.

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.

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.

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 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 authorisation of the transaction needs to occur at Mobile channel only. Mobile banking registration is mandatory for the Payer.

Customer Registration Process:

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.

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*.

UPI Transaction Flows:

The UPI transactions flows are outlined in Annexure VI.

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 - IX*

UPI PSP role:

The UPI PSP roles are outlined in Annexure –XII

Broad Security Considerations:

The broad security considerations are outlined in Annexure – XIII

App Checklist:

The App checklist are outlined in Annexure - XIV

Annexure – I (Settlement & Reports)

UPI Settlement & Reports Availability:

The settlement of UPI transactions will be facilitated through IMPS. All the rules and regulations of IMPS Settlement will be applicable in UPI for transactions where the credit leg is processed through IMPS. No separate raw files, STL & VERAF will be available for such transactions. They will be part of existing IMPS raw files.

For transactions where both the debit and the credit leg of the transactions is processed through UPI, then separate raw files, DSR and other reports will be provided in the existing IMPS RGCS interface.

Following table provides the details

Sr.	Details	Debit & Credit (Customers)	Settlement
1	Sending Bank live in UPI & Recipient Bank live in IMPS only	Debit in UPI Credit in IMPS	Settlement in IMPS
2	Both the Sending & receiving Bank live in IMPS	Credit in IMPS	Settlement in IMPS
3	Both Banks live in UPI	Debit in UPI Credit in UPI	Settlement in IMPS

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 through the DMS/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 reference to the data available at their end.

- 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 stringent action as deemed fit by NPCI.

- Letter of authority: For existing banks which are live on IMPS, existing mandate to RBI for credit/debit of settlement account will suffice.

- 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.

Any changes due to settlement of UPI transactions in IMPS Settlement shall be made at later stage if required.

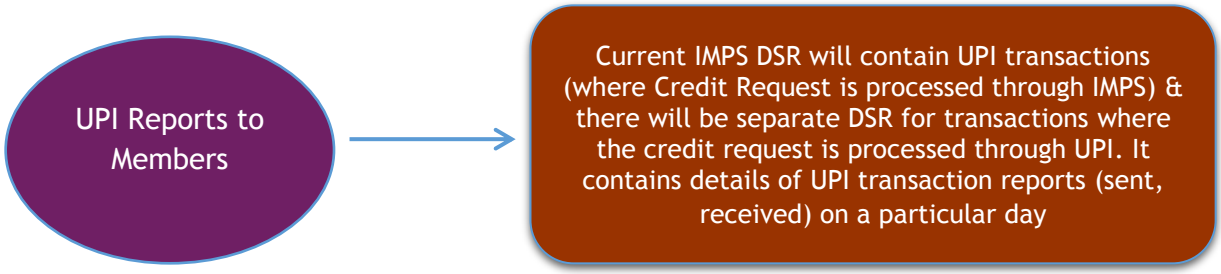
Reports Availability:

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

- Raw data file
- Net settlement report (NTSL)/Daily Settlement Report (DSR)*
- Settlement file (STL) – on NPCI settlement day
- Any other reports as may be relevant

* Available only during RTGS working days for settlement

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.

Dispute Management:

There will be broadly two types of variants in UPI Disputes Management & Settlement:

a) U2U

- Denotes transactions where both the debit and credit request are processed through UPI and will be available in separate raw data, reports, settlement files & DSR.
- In case of timed-out transactions (cases where NPCI was not able to receive the response in a specified time frame from Remitter/Beneficiary Bank), settlement of such cases will not be performed as this will be considered as declined transactions. The debit and the credit reversals will be processed.
- Accordingly, all the transactions will be categorised as either a successful or a failed transactions and there will not be any transactions with pending status.

Timeouts:

Timeouts in UPI will treated as declined transaction, wherein Reversal will be generated by Beneficiary bank and/or NPCI as applicable:

- **Wrong Credits / Closed / Frozen Accounts:**
  Credit adjustment option has been given to beneficiary banks. Beneficiary banks will raise credit adjustment once they recover funds successfully from their customer.
- **Complaint Window to PSPs:**
  PSPs (who are not remitter bank or not a beneficiary bank for particular transactions) are also allowed to raise complaint on either remitting bank or beneficiary bank for UPI transactions. E.g.: If online reversal fails and customer a/c is still in debit.
- **Search Transactions & Adjustment Status:**
  All parties of the UPI will be provided to search Transaction & Adjustment status through RGCS system.
- **UPI Merchant Payment Transactions:**
  For merchant Payments transactions, existing chargeback cycle will be applicable.

b) U2I:

- Denotes transactions the debit request is processed through UPI and the credit request is processed through IMPS and will be available in existing IMPS raw data and other related files.
- In case the credit leg is processed through IMPS, then the existing rules of IMPS Settlement will be applicable for such transactions.

Both U2U & U2I transactions will be posted as a single entry as IMPS Settlement entry, but banks will be able to differentiate between the same as separate reports will be provided.

NPCI will issue circular from time to time in case of any changes in the Dispute Mechanism.

For Detailed dispute management processes, please refer to the UPI Operating and settlement guidelines.

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 Day0)

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, all UPI enabled Apps installed / embedded on the mobile application should be mandatorily shown to user, so that the customer can select the UPI App of his choice to pay the merchant.
c) 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.
d) The central PSP system must have mechanism to authenticate the merchant before proceeding for the payment transaction.
e) 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.

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

h) Bank must ensure to conduct the independent IS audit for the built PSP app and the backend system.
i) 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.
j) 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.).
k) 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 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 will publish the standard deep-linking URL spec (for intent) 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 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 App requests the customer to assign the transaction limit. The default value should be provided as Rs. 1 lac.
6. 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.
7. If the user has not setup PIN, they can request PIN to be setup during the account adding process. The user requests PIN to be setup for the account.

Step –III Generate PIN:

1. The customer logs into the PSP application and selects the option to "Generate 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 PIN is also provided.
4. The issuing bank will only allow the 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 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 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 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 PIN Transaction:

Set PIN transaction allows the customer to set or change his 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 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 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 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 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 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.

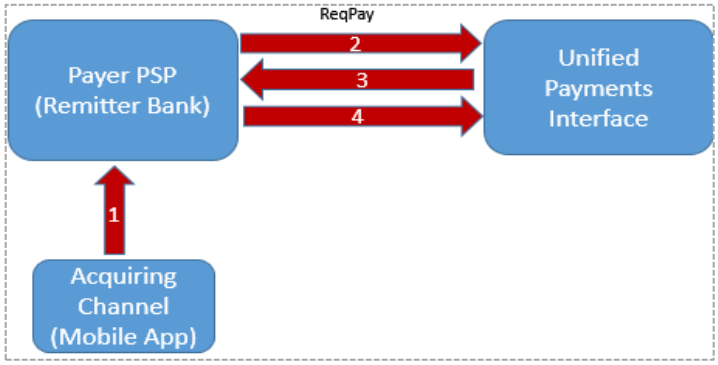
Annexure -VI (Flows of Financial Transactions)

PROCESS FLOWS FOR FINANCIAL TRANSACTIONS:

A. Transaction Flow when NPCI Libraries are used:

For Pay requests & 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 (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

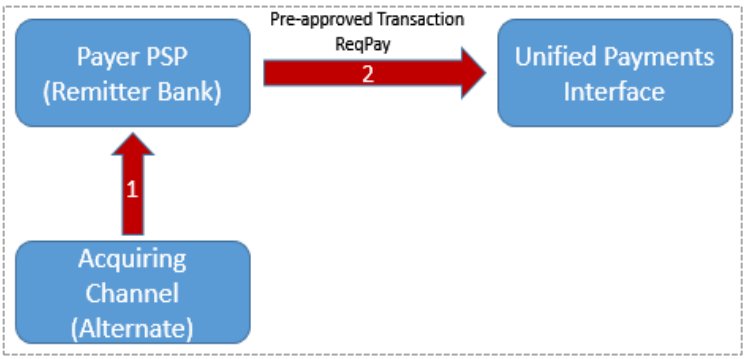


For illustration purposes, Step 3 & 4 is not provided in the process flows for non pre-approved transactions

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 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.

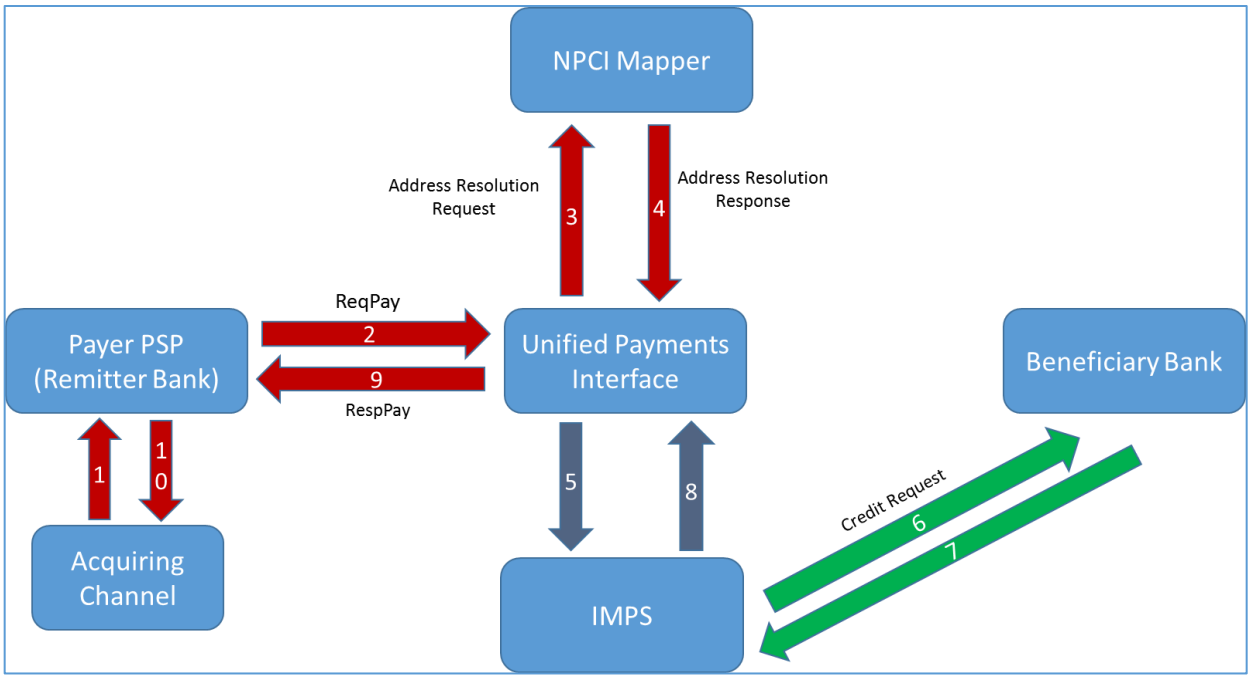


C. Push Transactions with Addresses like Aadhaar Number:

Global Addresses are Aadhaar Number. These global identifiers will be mapped to Banks in the NPCI Mapper. The data will be provided by the banks.

Case-1: Where Beneficiary Bank is not live on UPI, but live on IMPS:

In the above case, NPCI Centralized Mapper is used to resolve the bank linked with the global Address and the Beneficiary Bank is not live on UPI, but it is live on IMPS.



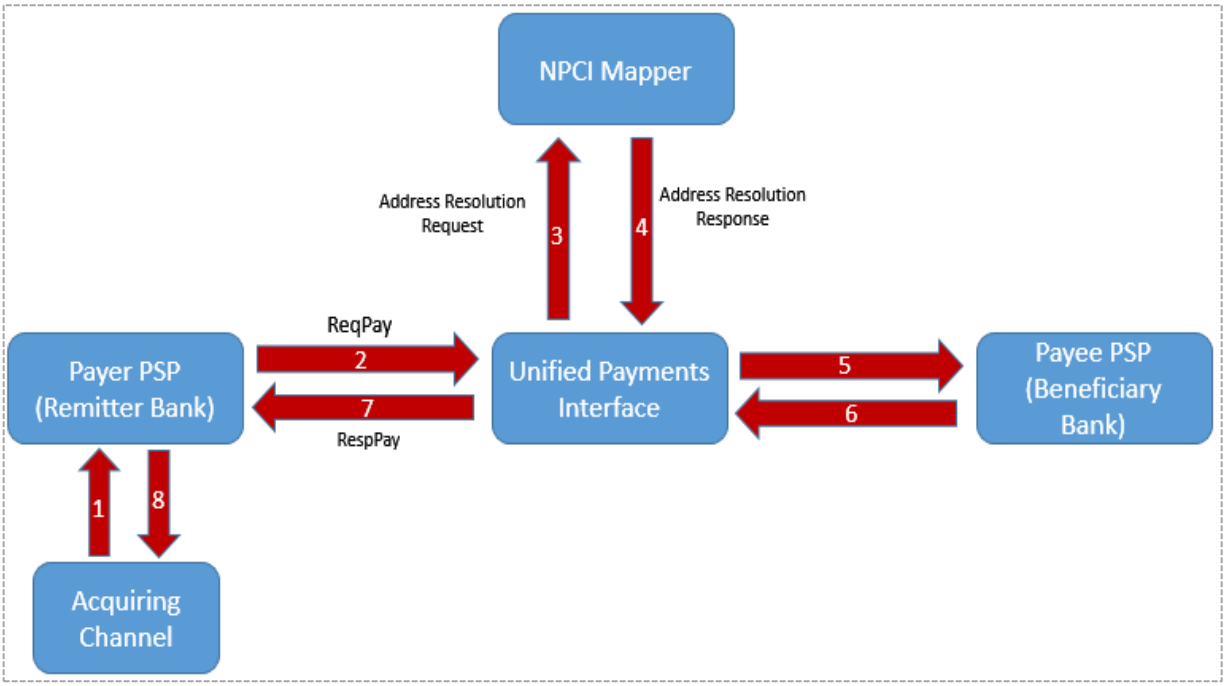
1 Payer enters the Aadhaar Number of the Payee in the PSP app and authorizes the payment by entering the PIN.
2 Remitter Bank debits the customer account and sends the transaction to UPI along with the Payer account details and a global address of the payee
3 UPI sends a query to the NPCI Centralized Mapper to fetch the details of the payee for address transaction
4 Mapper responds with the relevant Account information associated with the queried identifier
5 UPI initiates credit request through IMPS
6 NPCI sends the credit request to the Beneficiary Bank
7 Beneficiary Bank credits the Payee account and responds to NPCI
8 IMPS responds to UPI for the successful transaction
9 UPI responds to the Payer PSP for the successful transaction
10 Payer PSP confirms the same to the Payer customer

Case-2: Where Beneficiary Bank is live on UPI

Steps:

1. Payer enters the Aadhaar Number of the Payee in the PSP app and authorizes the payment by entering the PIN.
2. Remitter Bank debits the customer account and sends the transaction to UPI along with the Payer account details and a global address of the payee
3. UPI sends a query to the NPCI Mapper to fetch the details of the payee for address transaction
4. Mapper responds with the relevant Account information associated with the queried identifier
5. UPI initiates credit request to the Beneficiary Bank.

6. Beneficiary Bank credits the Payee account and responds to UPI
7. UPI responds to the Payer PSP for the successful transaction
8. Payer PSP confirms the same to the customer.



In Push based transactions where the financial address which is used is Mobile Number+MMID, Account+IFSC and Aadhaar Number, UPI will first check if the beneficiary bank is enabled on UPI.

In case the bank is not enabled on the UPI, then IMPS route will be used to process such transactions and they will be considered as a typical IMPS transaction and will be available in IMPS raw data & other reports.

In this case, the Remitter Bank will send the transaction as a UPI XML message, but NPCI will convert the message into the relevant ISO 8583 counterpart and send a Credit Response to the Beneficiary Bank through the IMPS Application.

In case the beneficiary bank is enabled in UPI, then it will be processed through UPI and will be available in UPI raw data and other reports.

D. Push Transactions with Mobile Number & MMID:

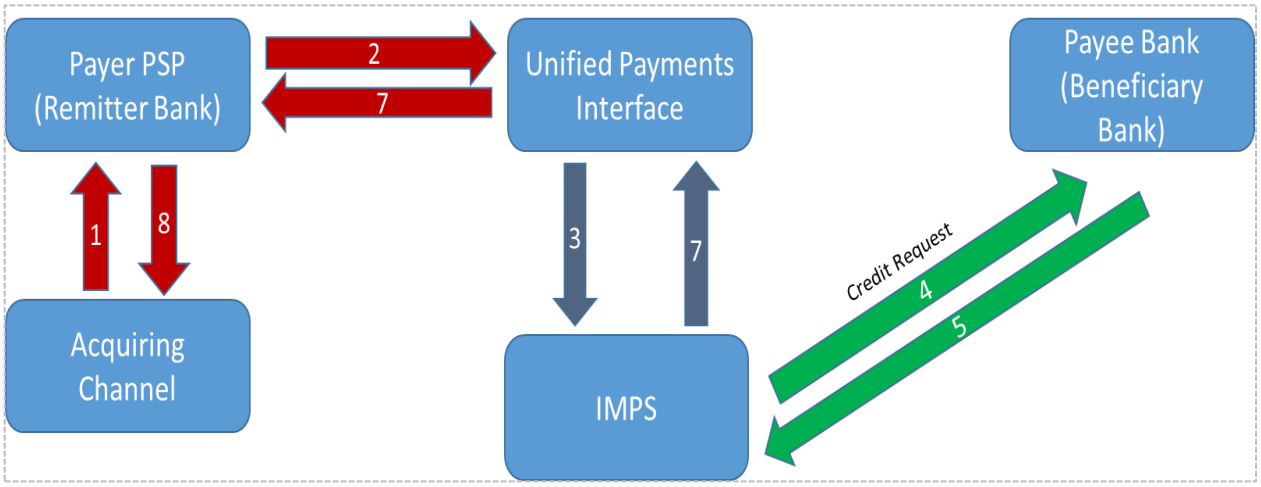
Case-1: Where Beneficiary Bank is not live on UPI, but live on IMPS:

Here, a P2P transaction initiated by the PSP App in XML message. This transaction will be converted to ISO 8583 in case the Beneficiary Bank is not live on UPI, but it is live on IMPS. Below is the transaction flow for such transaction:

Steps:

1. Payer enters the Mobile number & MMID of the Payee in the PSP app and authorizes the payment by entering the 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 initiates credit request through IMPS

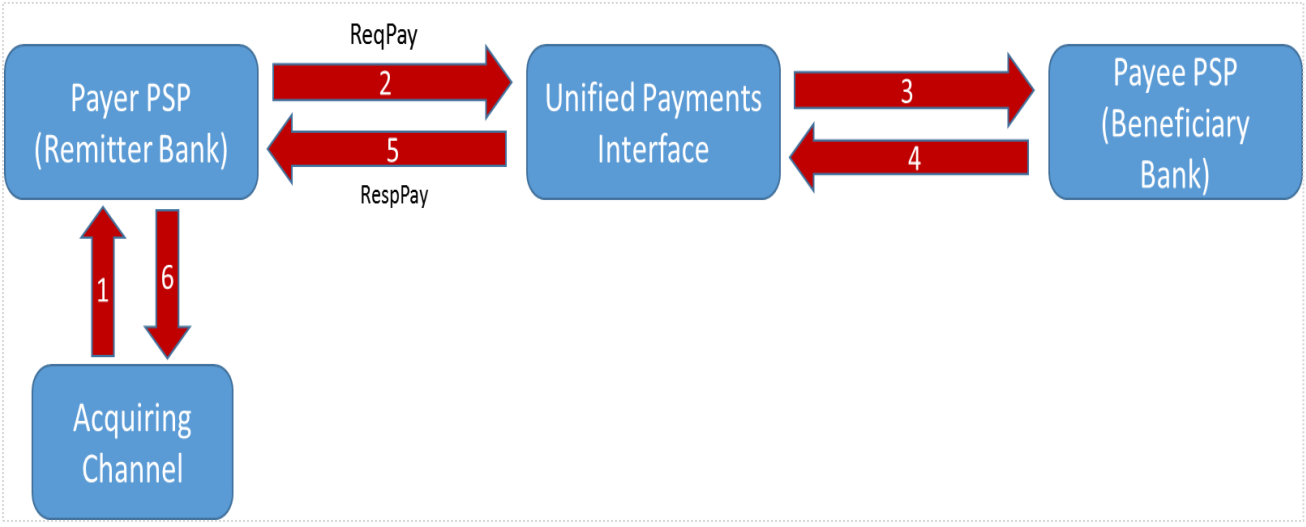
4. NPCI sends the credit request to the Beneficiary Bank
5. Beneficiary Bank credits the Payee account and responds to NPCI
6. IMPS responds to UPI for the successful transaction
7. UPI responds to the Payer PSP for the successful transaction
8. Payer PSP confirms the same to the Payer customer



Case-2: Where Beneficiary Bank is live on UPI:

Steps:

1. Payer enters the Mobile Number & MMID of the Payee in the PSP app and authorizes the payment by entering the 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



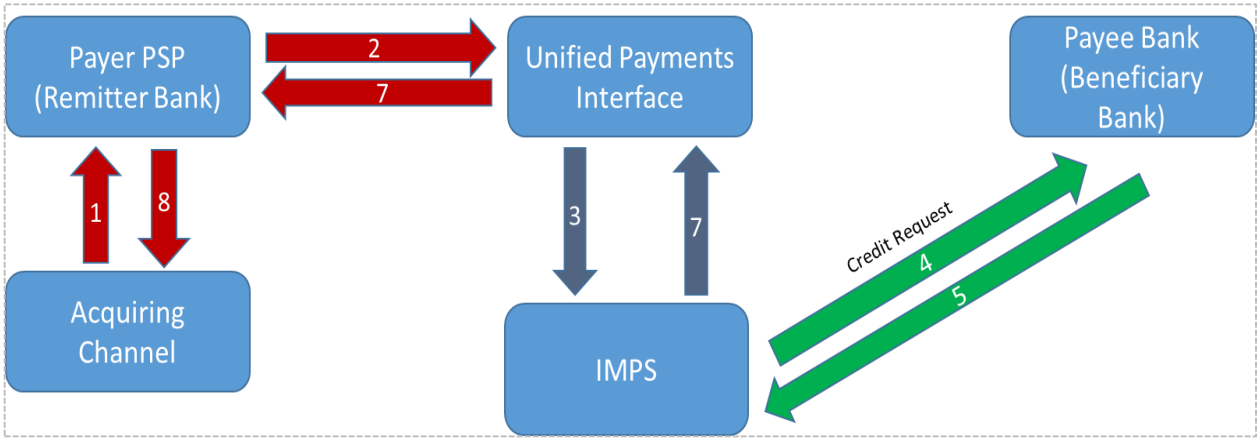
E. Push Transactions with Account Number & IFSC:

Case-1: Where Beneficiary Bank is not live on UPI, but live on IMPS:

Here, a P2A transaction initiated by the PSP App in XML message. This transaction will be converted to ISO 8583 in case the Beneficiary Bank is not live on UPI, but it is live on IMPS. Below is the transaction flow for such transaction

Steps:

1. Payer enters the Account number & IFSC of the Payee in the PSP app and authorizes the payment by entering the 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 initiates credit request through IMPS
4. NPCI sends the credit request to the Beneficiary Bank
5. Beneficiary Bank credits the Payee account and responds to NPCI
6. IMPS responds to UPI for the successful transaction
7. UPI responds to the Payer PSP for the successful transaction
8. Payer PSP confirms the same to the Payer customer

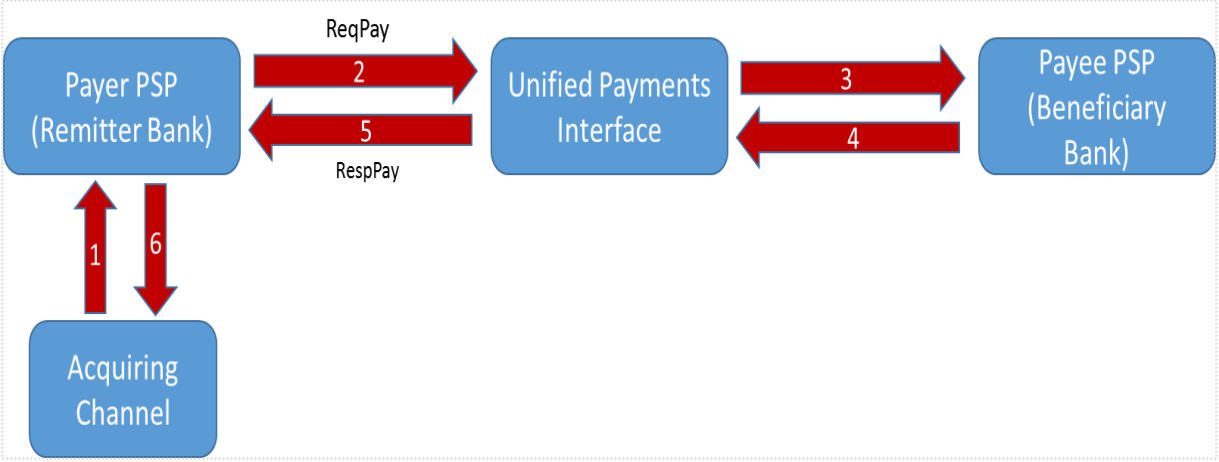


Case-2: Where Beneficiary Bank is live on UPI:

Steps:

1. Payer enters the Account Number & IFSC of the Payee in the PSP app and authorizes the payment by entering the 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

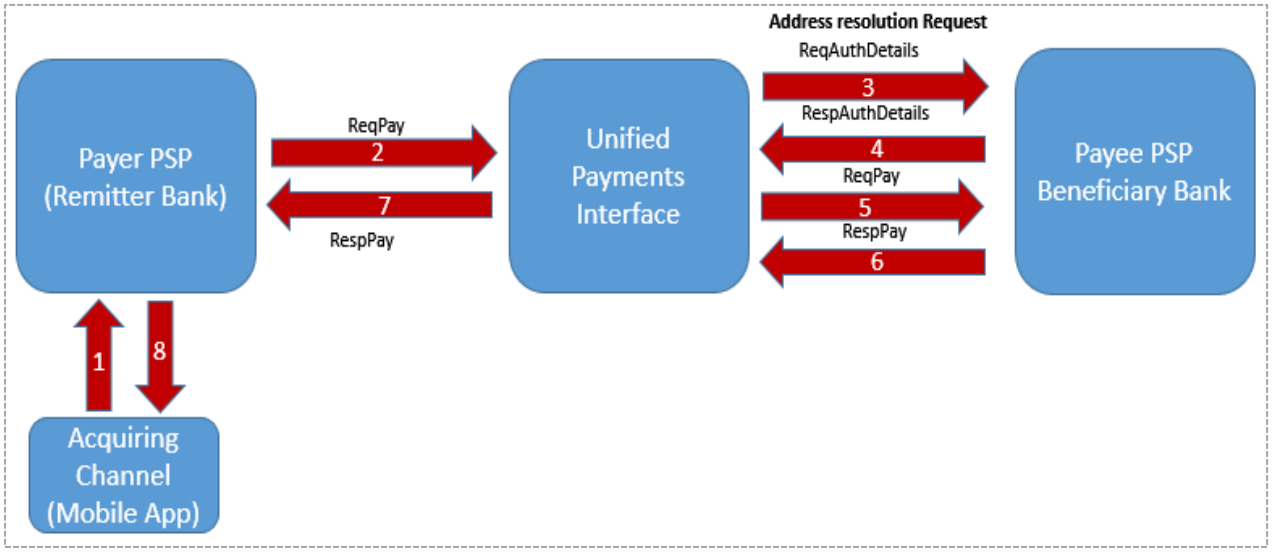


G. Transactions with Virtual Address

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

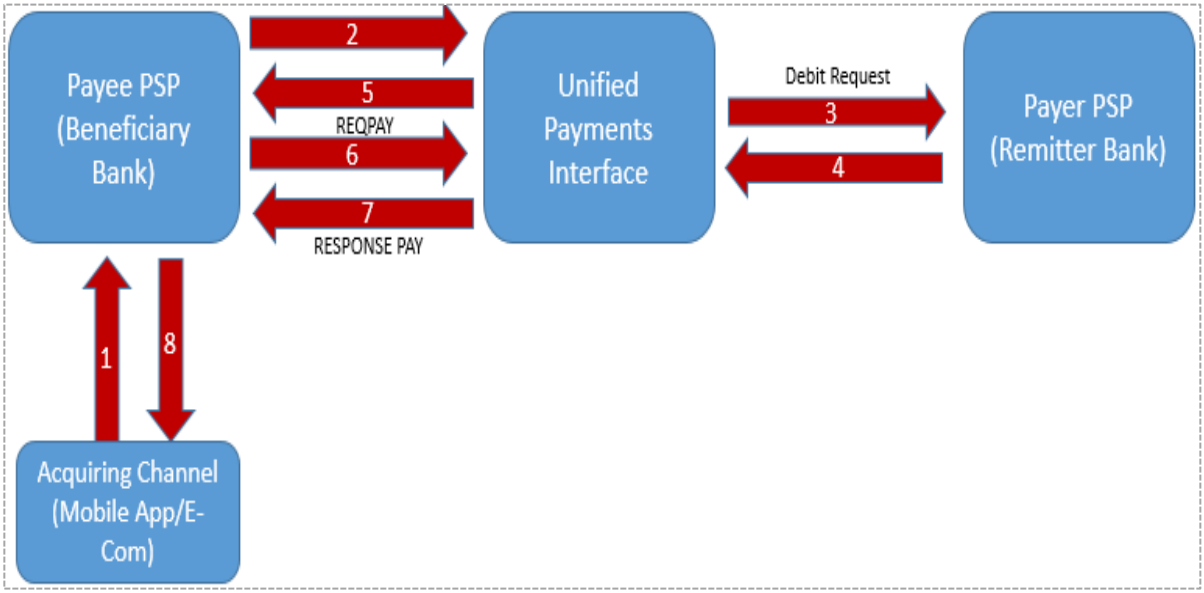
Pay Request:

1. Customer initiates a pay Request by entering the Virtual Address of the Payee
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



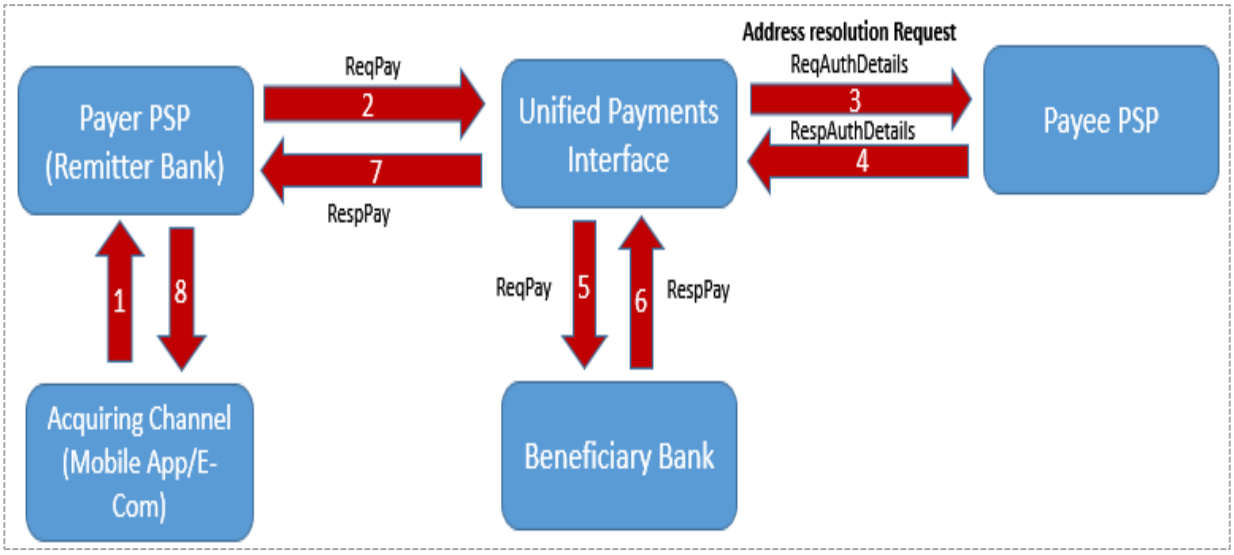
Collect Request:

1. Customer sends a Collect Request by entering the Virtual Address 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 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)

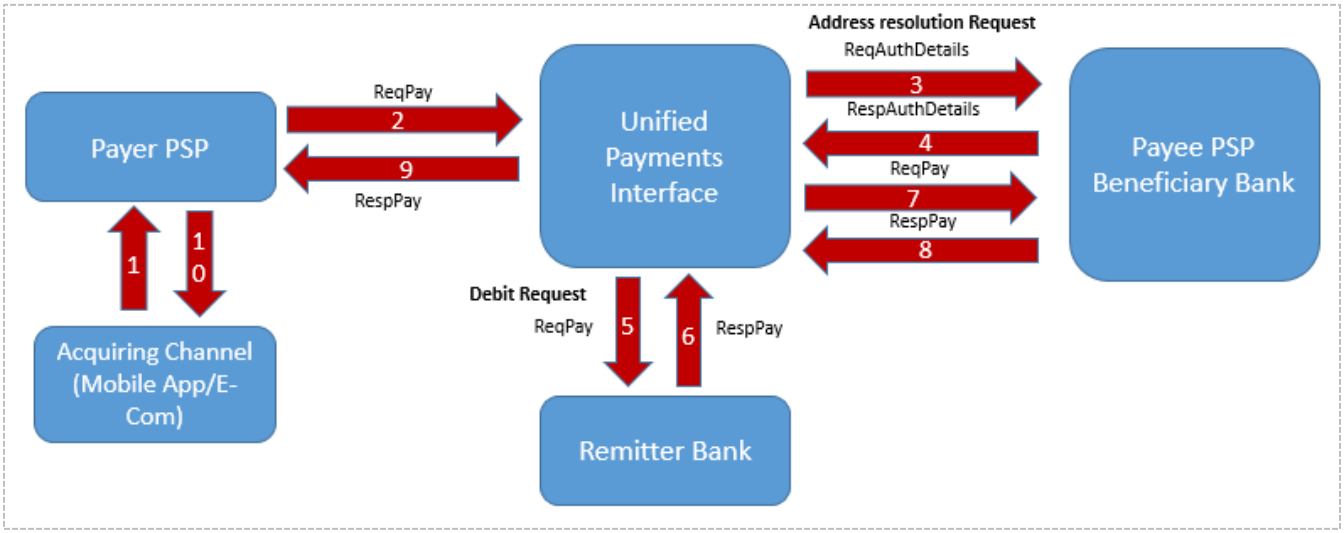
1. Customer initiates a Pay Request by entering the Virtual Address of the Payee customer and PIN.
2. Payer PSP/Remitter Bank debits the customer's account & sends the same to UPI
3. UPI routes it to the respective Payee PSP
4. Payee PSP identifies the Address and sends the relevant account information 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)

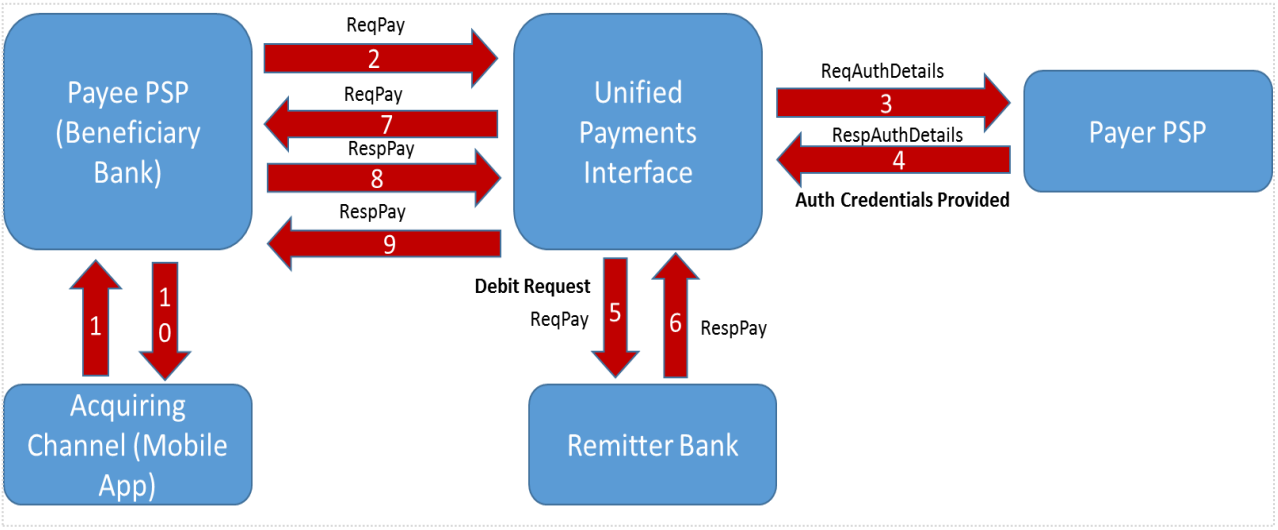
1. Customer initiates a Pay Request by entering the Virtual Address of the Payee customer and PIN.
2. Payer PSP sends the Request Pay along with customer's credentials to UPI
3. UPI sends address resolution request (ReqAuthDetails) to payee PSP.
4. Payee PSP identifies the Address and sends the relevant account information to UPI
5. UPI sends the debit request to payer 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 Virtual Address of the Payer customer.
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 Payer 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

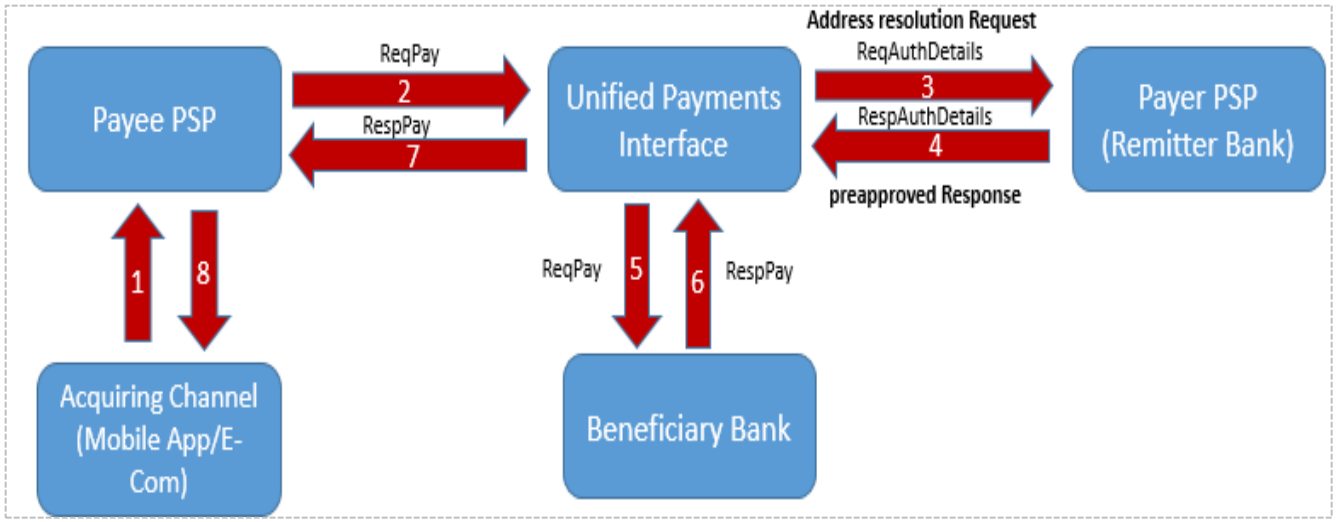


Three Party Model

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

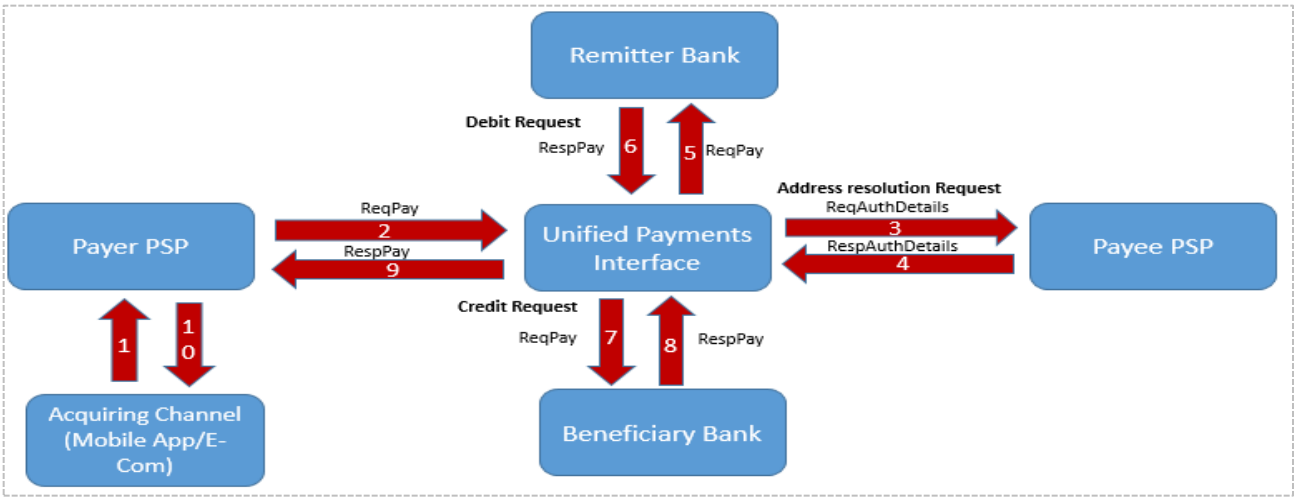
1. Customer sends a Collect Request by entering the Virtual Address of the Payer customer.
2. Payee PSP sends the same to UPI
3. UPI sends it to the respective Payer PSP for address resolution and authorization
4. Payer PSP sends a notification to the Payer customer for authorization. Customer enters 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)

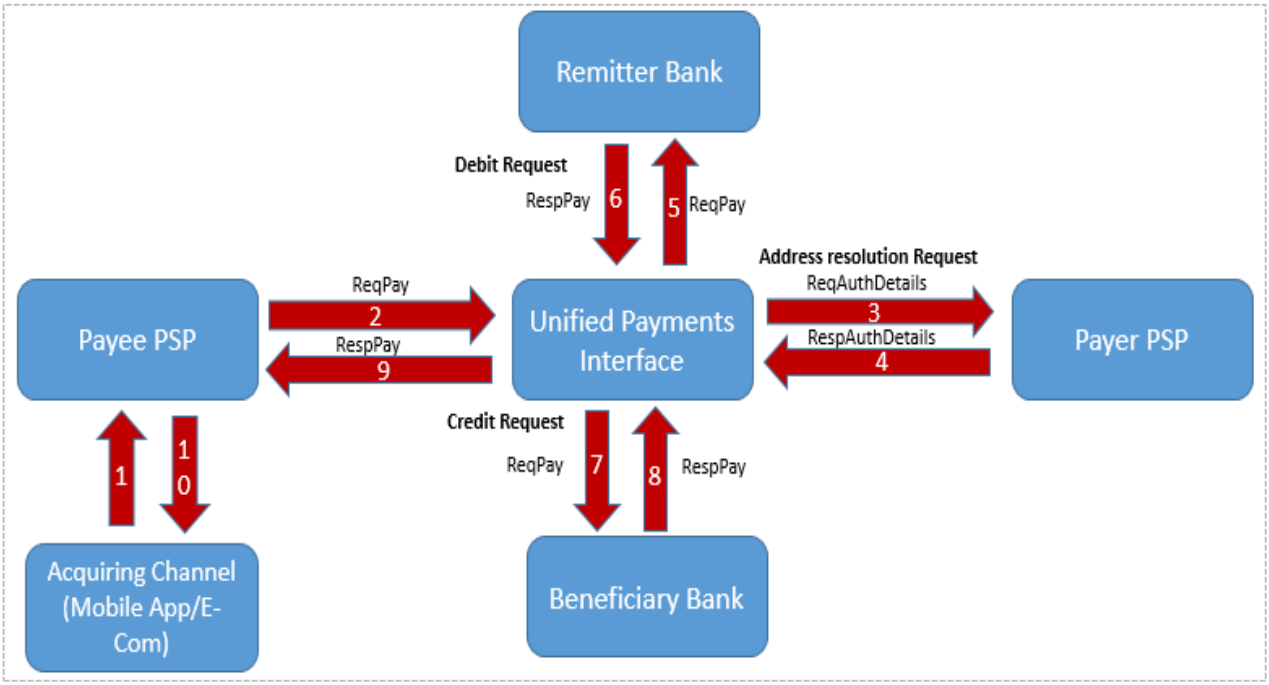


1. Customer sends a push Request by entering the Virtual Address of the Payee
2. Payer PSP sends the same to UPI
3. UPI sends it to the respective Payee PSP for address resolution and authorization
4. Payee PSP sends relevant account details of the Payee to UPI
5. UPI sends the debit request to Payer 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

Four Party Model

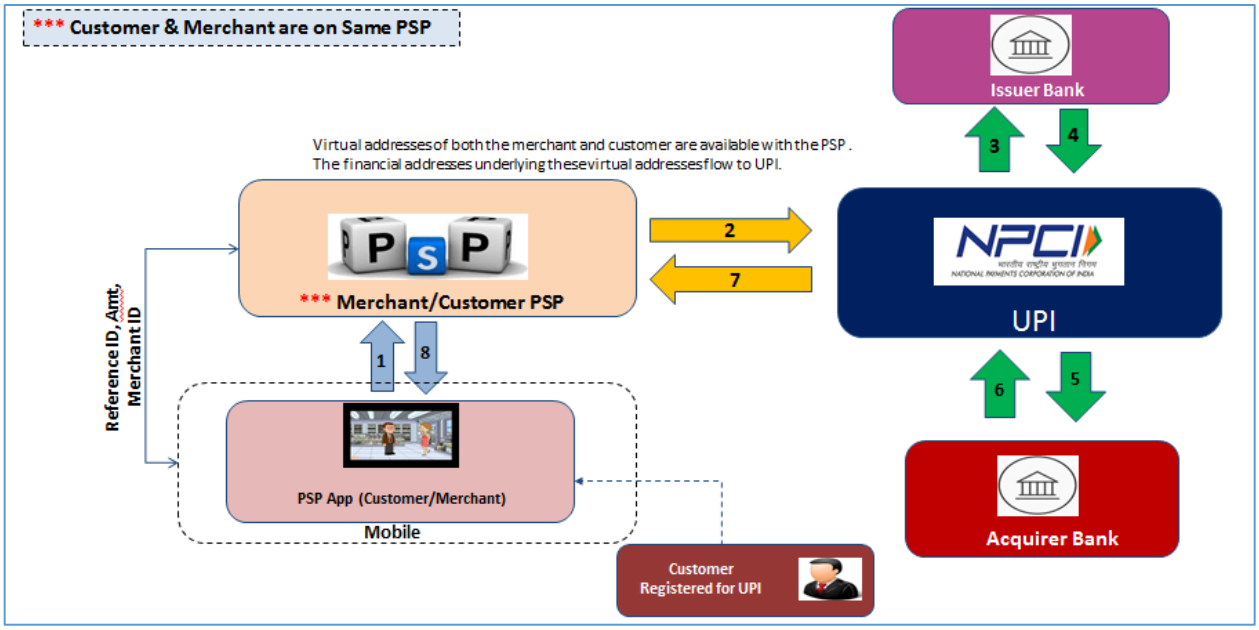
(Pull : Remitter Bank & Payer PSP are separate entities, Payee Bank & Beneficiary Bank are separate entities. It is applicable only for Person to Person transactions)

1. Customer sends a Collect Request by entering the Virtual Address of the Payer customer.
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

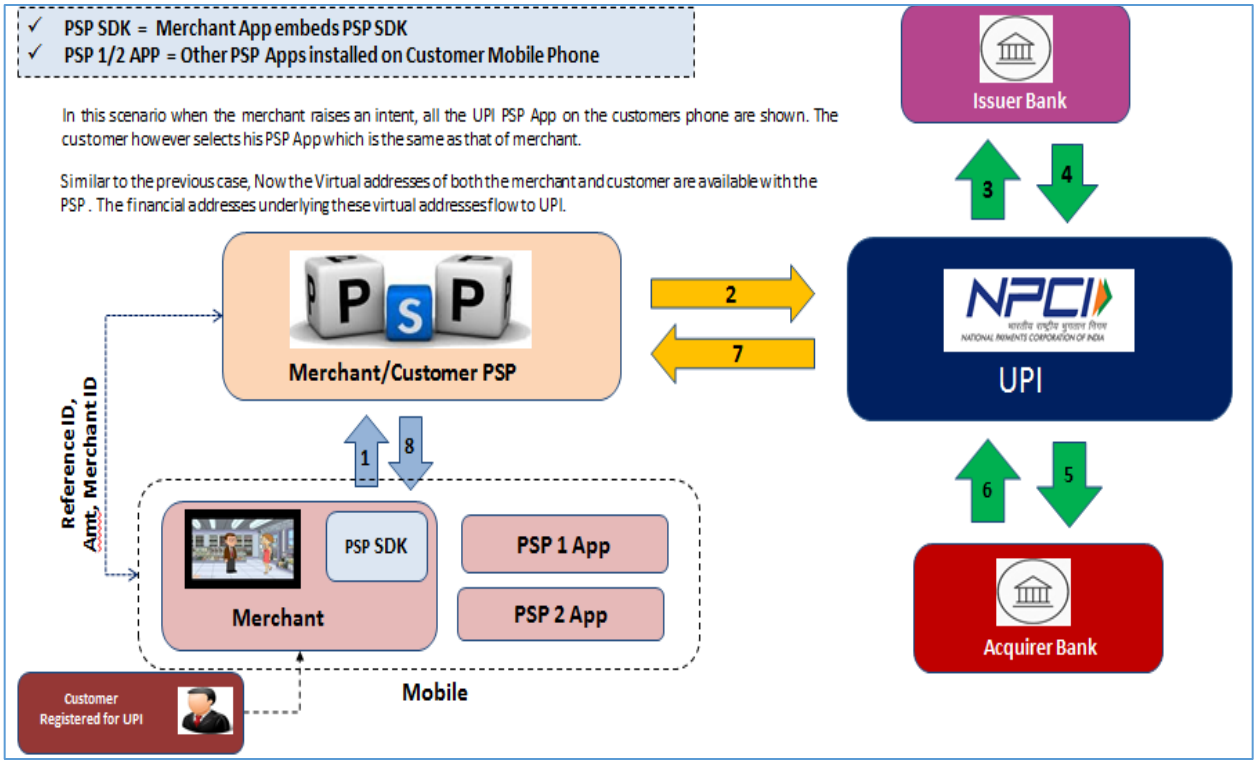


Merchant Transaction Flows:

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



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 & ISO 8583 or such other standards as may be 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 150 transaction per second (TPS), 5,00,000 transactions per day 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, 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/IMPS.

i) The PSP hereby agrees to abide by the dispute management rules and regulations specified by NPCI in document UPI/IMPS 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/IMPS shall be encrypted using suitable mechanism and that 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/IMPS 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. The security of transactions at the NPCI network and NPCI server level would be the responsibility of NPCI

s) PSPs undertake to update the global address in the NPCI Centralized Mapper regularly

t) 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

u) 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

v) 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

w) 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 which will be advised shortly.

x) 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.

y) 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

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

aa) 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.

bb) PSP should place a moratorium of at least Two (2) Years in case a 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 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/IMPS 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

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/IMPS network and subsequently, as per periodicity defined by NPCI

e) All sub-member banks participating in the UPI network to comply with data integrity 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 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/IMPS should comply with the message specifications, as specified by UPI/IMPS, based on XML/ISO 8583 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 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 -X (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	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 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. For the pilot period, it has been decided to allot a maximum of 3 handles per bank. Bank has to ensure that under no circumstances, PSP handle allotted by NPCI to be transferred to any other entity/bank. The 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.

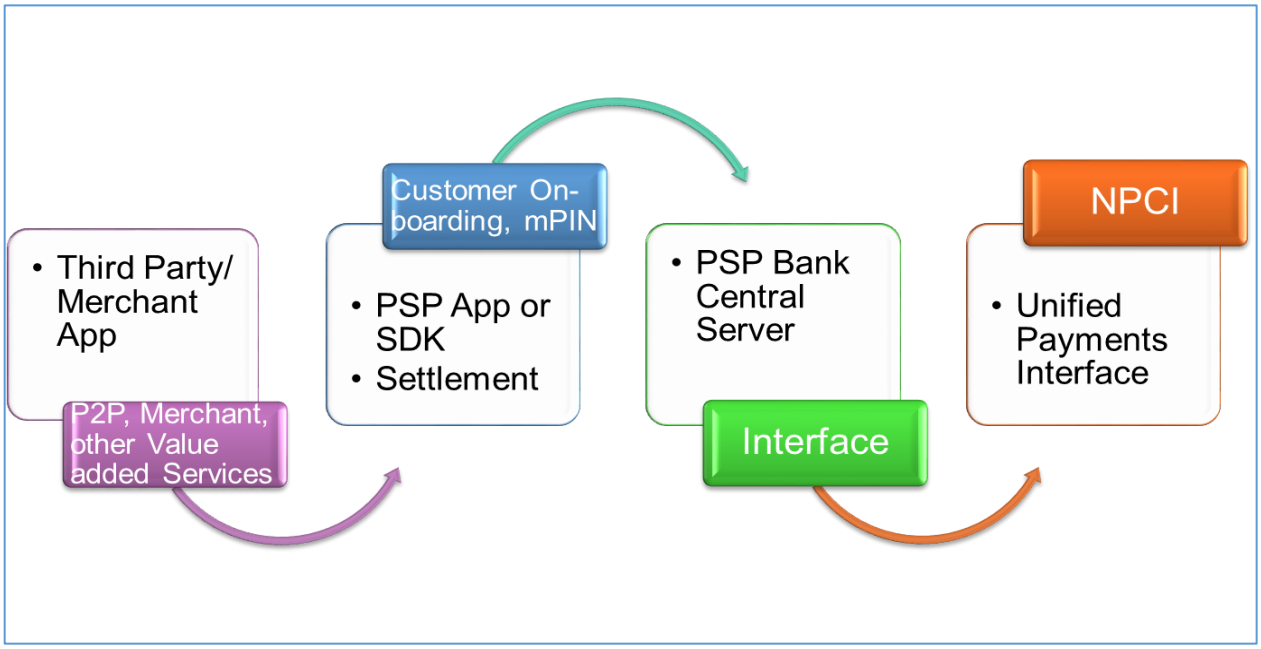
8. Portability of handles

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 for pilot period, the same will not be provided by NPCI.

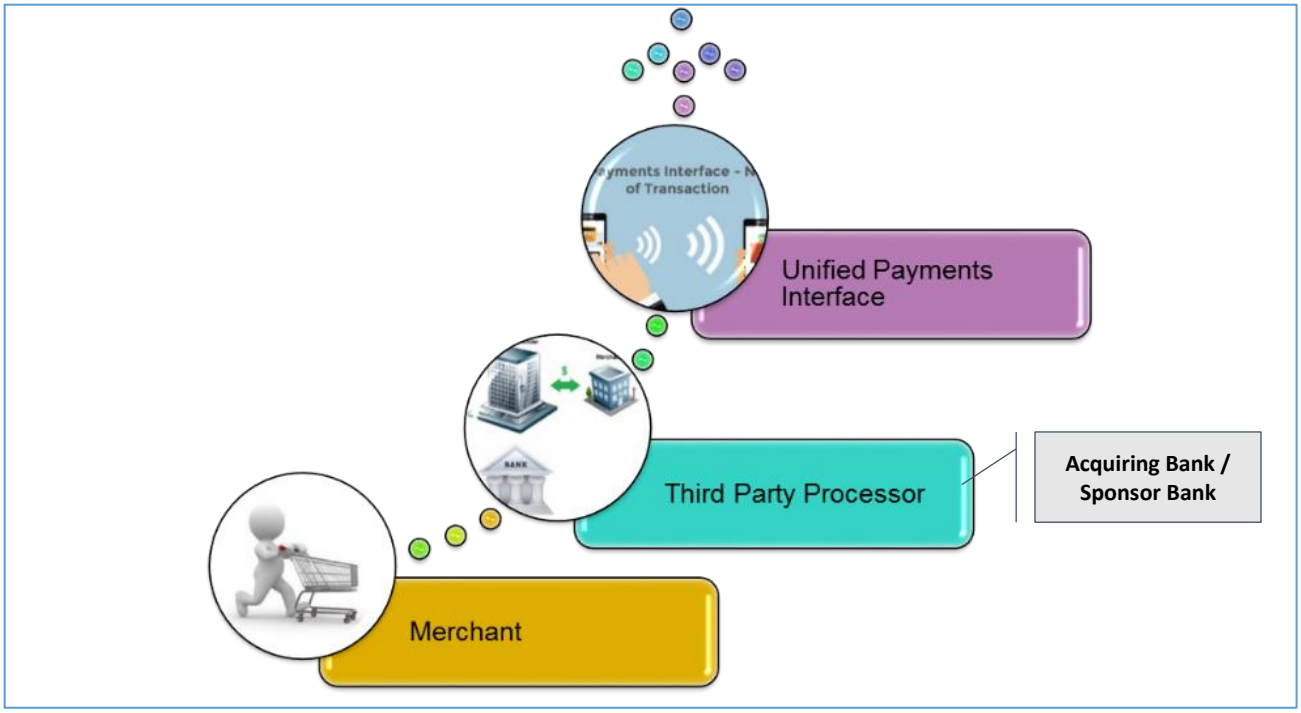
The broad approved architecture of UPI shall be as under:



10. UPI transactions through Third Party Processor for Merchant Payment

For merchant on-boarding in UPI, it is possible for he 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 / 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 Mpin and initiate a Debit on the account.

   b) The Push transaction – Where-in the customer knows the 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. The large merchants would ideally include the likes of "IRCTC", "Flipkart", "Amazon", "Snapdeal" and "BookMyShow" etc.

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.

(Note: Names have been used only for representation purpose)

4. Name Check for 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 VPA 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 VPA
2) Not more than 25 transactions in a week on the same 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 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 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 biding" 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)

The purpose of the below Checklist is to ensure that the UPI based Application have the same look and feel across applications of different entities. The Field Marked with * has to be filled by NPCI official only after ensuring sanctity of product.

Note: -
1. Application release in public domain cannot happen without this Checklist clearance.
2. 'M' implies Mandatory functionality
3. 'O' implies Optional functionality

Level 1:- How to Download an UPI enabled Application.

Sr.	Location	Bank/PSP Name in the App name	Mandatory* /Optional	Yes / No*
a	Play Store		M	
B	App Store		M	
C	Windows Store		O	

* - As per the UPI PG

Level 2:- Home screen checklist

Sr.	Transaction Type		Mandatory / Optional	Yes /No*
a	Send(Push)	1. Virtual Address (VPA) 2. Account /IFSC 3. Mobile No/MMID	M M O O	
b	Collect	1. Virtual Address 2. Aadhaar	M O	
c	Add/Link a Bank A/C		M	
d	Transaction history		M	
e	Mobile Banking registration	1. Card No. & Expiry is manual entry. 2. Picture/Scan	M O	
f	Generate Mpin/ Set Mpin	1. Card No. & Expiry is manual entry. 2. Picture/Scan	M O	
g	Change Mpin	Old mPIN & new mPIN is manual entry	M	
h	Change Application Password		O	
i	Log a complaint		M	

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

Sr.	Action	Mandatory/Optional	Yes /No*
a	Encrypted SMS from App without User	**M**	
a.1	Type of Encryption	**M**	**PKI**
a.2	Choice of SIM Selection should be there in case of Dual SIM phones.	**M**	
b	Profile Creation	**M**	
c	VPA Creation	**M**	
d	Application password	**O**	
e	Login Page to restart application	**O**	
f	Deregistration from PSP	**M**	
g	Deletion of Account linked to VPA	**M**	
h	Deletion of VPA	**M**	

Level 4:- Total User entry

Sr.	Action	Mandatory/Optional	Yes /No*
a	Entry of Mobile No	**M**	**No**
b	Virtual Payment Address	**M**	**Yes**
c	Debit Card entry /Scan	**O**	**Manual /Scan**
d	SET MPIN	**M**	**Yes/No**
e	Whitelisting of Collect Requestor **(good**	**O**	**Yes/No**
f	Whitelisting of Merchant **(good to have)**	**O**	**Yes/No**
g	Storing of Beneficiary by nick name for following • VPA • IFS + A/C No • Aadhaar	**O**	**Yes/No**
h	Having the Favorite Selection of Beneficiary	**O**	**Yes/No**
i	Restoring of VPA by PSP in case of deletion of VPA by user	**M - at least 2 years Moratorium**	**Yes/No**

Level 5:- Add a bank Account / VPA & Account handling

Sr.	Actions	Mandatory/Optional	Yes / No*
a	List of bank 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 to be search by start letter of the bank	**M**	
c	If customer registered for MB display Set Mpin transaction based on Debit card last 6 digit & expiry date followed by OTP from Issuer **OR** If customer has MPIN, app should provide option – "Continue with Existing MPIN".	**M**	
d	If customer not registered for MB customer should be routed to MBR transaction with the same details required for Set MPIN	**M**	
e	One VPA to multiple Account (Default VPA selection) - **Optional**	**O**	
f	Multiple VPA to Single Account	**O**	
G	One PSP APP to register Multiple bank account with multiple VPAs	**M**	
h	Generate OTP	**O**	
h.1	OTP read by the App OR entered Manually	**O**	

Level 6:- Pay Transaction

Sr.	Actions	Mandatory/Optional	Yes/ No*	Remarks
a	Pay using VPA	**M**		
b	Pay using a/c & IFSC	**M**		
c	Pay using mob & MMID	**O**		
d	Pay using Aadhaar	**O**		
e	Mpin Preapproved	**M**		
f	Mpin non pre-approved	**O**		
g	Transaction online Confirmation	**M**		
h	Methodology of invoking Common Library • Mpin preapproved / onus transaction invocation of common library • Mpin non-preapproved / off us transaction	**O** **M**		

	invocation of common library. • Ref URL in common library on clicking should take customer to relevant page with complete detail (For example Bill no, amount, transactions id and complete bill details).	**M**		

Level 7:- Collect transaction

Sr.	Actions	Mandatory/Optional	Yes/ No*	Remarks
a	Collect using VPA	**M**		
b	Mpin Preapproved	**M**		
c	Mpin non preapproved	**O**		
d	Transaction Status Confirmation	**M**		
e	Display of VPA 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	**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 • Mpin preapproved / onus transaction invocation of common library • Mpin non-preapproved / off us transaction invocation of common library. • Ref URL in common library on clicking should take customer to relevant page with complete detail (For example Bill no, amount,	**O** **M** **M**		

	transactions id and complete bill details).			

Level 8:- Balance Enquiry

Sr.	Action	Mandatory/Optional	Yes/ No*	Remarks (If Any)
a	Select Account	**M**		
b	Mpin Preapproved	**M**		
C	Mpin Non Preapproved	**M**		

Level 9:- Check Transaction Status / Raise Query/ log a complaint

Sr.	Action		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 VPA/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 10:- Hot listing/Deletion

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

Level 11:- 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**		**Nomenclature is to be decided by the bank**
C	Reject Collect request	**M**		**Nomenclature is to be decided by the bank**

Level 12:- QR Code based enablement

Sr.	Action	Mandatory/Optional	Yes/ No*	Remarks (If Any)
a	Customer being able to generate the QR Code within his App (Which Merchant can scan for payment)	**O**		**Merchant based Pull Payments**
b	Customer should be able to scan the QR Code of a Merchant / Another Person for making payments	**O**		**Push payment - Merchant / P2P**
c	It is mandatory to display to the customer at least VPA, Amount and name in QR based payment.	**M**		**Push payment - Merchant / P2P and Merchant based Pull Payments**

Level 13:- Raising Intent Call

Sr.	Action	Mandatory/Optional	Yes/ No*
A	The App to support Intent Call request from the Merchant Apps		
a.1	Android	**M**	
a.2	IOS	**M**	
a.3	Windows	**M**	

Additional Comments (if any):-

Sign off

National Payment Corporation of India