Unified Payments Interface

(Please send all feedback on this draft Product Document to upisupport@npci.org.in)

Version 1.0

June 29th, 2015

TABLE OF CONTENTS

1. INTRODUCTION 3

1.1 DEFINITION & OBJECTIVES OF UNIFIED PAYMENTS INTERFACE 3

1.2 KEY CHARACTERISTICS OF UPI 5

2. VALUE PROPOSITION OF UNIFIED PAYMENTS INTERFACE 5

3. BASIC STRUCTURE OF UNIFIED PAYMENTS INTERFACE 7

4. MEMBERSHIP REQUIREMENTS 7

5. BENEFITS OF UPI TO BANKS 8

BENEFITS OF UPI TO END CUSTOMERS 9

6. ROLE OF NPCI LIBRARIES 9

6.1 HOW PIN WILL BE CAPTURED? 9

7. PROPOSED FEE & CHARGE STRUCTURE 10

8. BROAD PROCESS FLOW OF CUSTOMER REGISTRATION IN PSP APPLICATION 10

9. UPI FLOWS FOR GLOBAL ADDRESS TRANSACTION USING NPCI MAPPER 11

10. GLOBAL MAPPER UPDATE PROCESS 12

11. FLOWS FOR TRANSACTIONS BASED ON VIRTUAL ADDRESS 13

12. CERTIFICATION OF MEMBERS 15

13. OTHER IMPLEMENTATIONS 15

14. GLOSSARY 17

1. INTRODUCTION

Over decades, India has made slow but steady progress in the field of electronic payments. The innovations in payments have leveraged major technological innovations in each era. However, given the scale of our country, and that so many are unbanked, we cannot rest on our laurels.

The RBI Payment System Vision document emphasizes the mission and vision clearly:

Mission Statement

To ensure payment and settlement systems in the country are safe, efficient, interoperable, authorized, accessible, inclusive and compliant with international standards.

Vision

To proactively encourage electronic payment systems for ushering in a less-cash society in India.

The Mission statement indicates RBI's renewed commitment towards providing a safe, efficient, accessible, inclusive, interoperable and authorized payment and settlement systems for the country. Payments systems will be driven by customer demands of convenience ease of use and access that will impel the necessary convergence in innovative e-payment products and capabilities. Regulation will channelize innovation and competition to meet these demands consistent with international standards and best practices.

It also identifies the challenges very clearly:

1. Currently the number of non-cash transactions per person stands at just 6 per year.
2. A fraction of the 10 million plus retailers in India have card payment acceptance infrastructure – presently this number stands at just over a million.
3. Of about six lakh villages in India, the total number of villages with banking services stands at less than one lakh villages as at end March 2011 and nearly 75 million households (out of 250 million) are excluded from banking. Over the last few years, significant improvements have come in terms of coverage and with Direct Benefits Transfer (DBT) and Jan Dhan Yojana (PMJDY), number of households having bank account has also gone up.

It was against this background, NPCI was set up in April 2009 with the core objective to consolidate and integrate the multiple systems with varying service levels into nation-wide uniform and standard business process for all retail payment systems. The other objective was to facilitate an affordable payment mechanism to have financial inclusion across the country.

In this regards NPCI has taken up new initiative of implementing "*Unified Payments Interface*" to simplify and provide a single interface across all systems. The broad objectives are summarized hereunder:

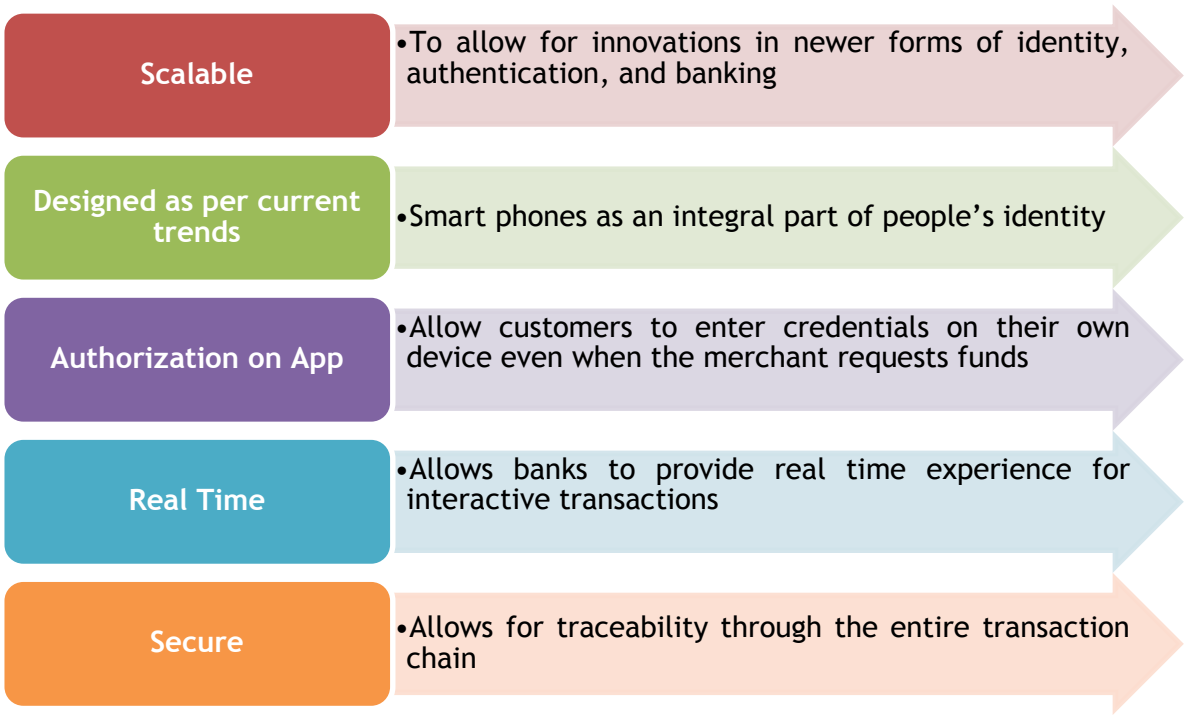
1.1 DEFINITION & OBJECTIVES OF UNIFIED PAYMENTS INTERFACE

The major objective of the Unified Payments Interface is to offer architecture and a set of standard APIs to facilitate the next generation online immediate payments leveraging trends such as increasing smartphone adoption, increasing penetration of mobile data, Indian language interfaces. Following are some of the key aspects of the Unified Payments Interface:

a) The Unified Payments Interface is expected to further propel easy instant payments via mobile app, web, and other applications.
b) The payments can be both sender (payer) and receiver (payee) initiated and are carried out in a secure, convenient, and integrated fashion.
c) This design provides an ecosystem driven scalable architecture and a set of APIs taking full advantage of mass adoption of smartphone.
d) There will be two types of addresses viz. Global address (Mobile Number, Account Number, Aadhaar Number etc) & Local address/virtual payment addresses (abc@psp), 1-click 2-factor authentication, Aadhaar integration, use of payer's smartphone for secure credential capture, etc. are some of the core features.
(**Note**: The Global addresses as highlighted above are proposed to be resolved at the NPCI Mapper level, and the local address, viz. the PSP registered 'virtual address resolution shall happen at the PSP level)
e) It allows banks and other players to innovate and offer a superior customer experience to make electronic payments convenient and secure.
f) Supports the growth of e-commerce, while simultaneously meeting the target of financial inclusion.
g) Proposed architecture is well within the regulatory framework of the mobile and ecommerce transactions having 2 factors of authentication (2FA).

Push & Pull Payments	•The payments can be both sender (payer) and receiver (payee) initiated and are carried out in a secure, convenient, and integrated fashion
Easy Instant Payments	•The unified payments system is expected to further propel easy instant payments via mobile, web, and other applications
Scalable Architecture	•This next generation payment system provides an ecosystem driven scalable architecture and a set of APIs taking full advantage of mass adoption of smartphone
1 Click 2FA & Virtual address	•Virtual payment addresses, single click 2 factor authentication, Aadhaar integration, use of payer's smartphone for secure credential capture, etc. are some of the core features

1.2 KEY CHARACTERISTICS OF UPI



2. VALUE PROPOSITION OF UNIFIED PAYMENTS INTERFACE

a) Simplifying Authentication - India is the only country in the world to offer trusted 3rd party biometric authentication as a utility service. With universal coverage of Aadhaar expected in 2015, PSPs can take advantage of this utility to provide secure, convenient authentication service to a billion people without having the need to do card/PIN issuance lifecycle. Below is the 2FA to be used in UPI which is complied with RBI guidelines:

Authentication	First Txn	Authorised by	Subsequent Txn	Authorised by
1st Factor	Mobile Number (OTP)#	Issuer	Mobile Number/User ID	PSP
2nd Factor	PIN/Biometrics* matched against UIDAI	Issuer	PIN/Biometrics* matched against UIDAI	Issuer

* In case of Biometric, confirmation will be provided by UIDAI and on the basis of that, Issuer will debit the customer
# The PSP also checks the veracity of the person registering on its App by sending an OTP and verifying it

b) Simplifying Issuance Infrastructure - Usage of virtual addresses and payment addresses in conjunction with mobile as the "what you have" factor helps banks to create token-less infrastructure reducing the costs.

c) Simplifying Acquiring Infrastructure - Use of mobile as the primary device for payment authorization can completely transform the issuance infrastructure to be easy, low cost, and universal. Considering the fact that India has nearly a billion phones and 150 million smartphones (expected to be at 500

million in next 4-5 years), massive scale can be achieved if effective use of mobile is made compared to creating costly physical acquiring infrastructure.

d) Flexibility for PSPs - Payment system players (RBI regulated entities such as banks, payment banks) can offer superior mobile experience to their customers. In addition, this unified interface still allows a fully on-us scheme if both payer and payee are on their network.

e) Flexibility for Users - Customers get the ability to make payments securely to their friends, relatives, pay to merchants, pay bills, etc. all using their mobile phones without having to share any account details or credentials with others. In addition, innovations such as reminders, using multiple accounts via single mobile applications, using special purpose virtual addresses, etc. allow users to enjoy superior experience.

f) Enabling 1-click 2-FA Transactions - This proposal allows all transactions to be at least 2-FA using mobile and another factor (PIN and Biometrics). Since mobile number is bound to the device, explicit SMS based OTP need not be used every time which makes authorization simpler. When biometric sensor integrated mobiles start becoming available, payments can be done with no data entry making electronic payments extremely convenient, but still providing full 2-FA security. This is aligned with the extant regulatory guidelines for financial transactions through Mobile banking in India.

g) Stimulating Innovation - This interface provides a very simple API that is minimalistic, fully functional, and allowing innovations in various aspects such as user interface, convenience features, authentication schemes, and mobile devices to be brought in without having to change the core API structure.

h) Embracing Mobile Adoption - This interface truly embraces mobile and low cost smartphone adoption in India allowing phones to be the primary device for all payments and integrating mobile numbers by allowing paying to/from a mobile number.

i) Embracing Aadhaar Adoption - Universal digital identity is fast becoming a reality with Aadhaar adoption crossing 750 million. With Aadhaar e-KYC allowing paperless, anytime anywhere e-KYC services, the use of Aadhaar as a payment destination using APB, and usage of Aadhaar authentication as a trusted 3rd party authentication, large scale electronic payments can be achieved unlike ever before.

j) Creating National Interoperability - With introduction of new payment service players such as payment banks, PPIs, and others, it is necessary that India adopt an interoperable mobile payment strategy to allow customers to send and receive from any other customer within the PSP or across PSPs in a seamless fashion. Proactively creating this unified interoperable interface allows all players to innovate and provide superior customer experience and still provide a secure, standard based, interoperable payment scheme.

3. BASIC STRUCTURE OF UNIFIED PAYMENTS INTERFACE

NPCI Services covered under Phase I

- IMPS

Security

- HTTPS, PKI Infrastructure, (PIN on mobile and OTP is encrypted), Underlying Product Security Mechanisms, Device fingerprinting

Addresses allowed

- Aadhaar Number, Mobile Number, & Virtual Address

Resolution of addresses

- **Global Addresses**: Resolved by NPCI, Aadhaar Number & Mobile Number
- **Virtual Address**: Resolved by PSPs, using Address Translation API, @psp handle

4. MEMBERSHIP REQUIREMENTS

With the enablement of the unified API, it is perceived that the ecosystem members authorized by the RBI will integrate into the payments processing domain and the P2P transfers – both 'Push' and 'Pull' shall be enabled through bio-metric authentication, registered with their respective Banks.

The participant member must have enabled the 'Generate PIN and Change PIN' functionality being offered by NPCI through the National Unified USSD platform (*99#) for their customers.

The participant member should be live on IMPS credit messaging (Mobile & Account based).

The Participant members may enable the Mobile banking registration on NFS network.

Other broad Requirements for On-boarding:

We have the following guidelines to abide to become a participant for the Unified Payments Interface:

1) Direct members (Issuers/Acquirers as applicable):

a) Banks authorized by RBI for providing mobile banking service in terms of RBI circular RBI/2008-09/208 dated October 8, 2008
b) Members having RTGS membership are eligible to participate in IMPS network as a direct or indirect member
c) The participants must have enabled the 'Generate PIN and Change PIN' functionality being offered by NPCI through the National Unified USSD platform (*99#) for their customers.
d) The member should be live on IMPS inward/credit messaging.

2) Indirect members/sub-member banks/Payment System Players through Direct members

a) Banks:
   i. Banks authorized by RBI for providing mobile banking service in terms of RBI circular RBI/2008-09/208 dated October 8, 2008.
   ii. Banks sponsored by another existing IMPS direct member banks having RTGS membership for clearing and settlement purpose with RBI. These banks will be connected through their sponsor banks on IMPS and the sponsor will be responsible for all their settlement operations

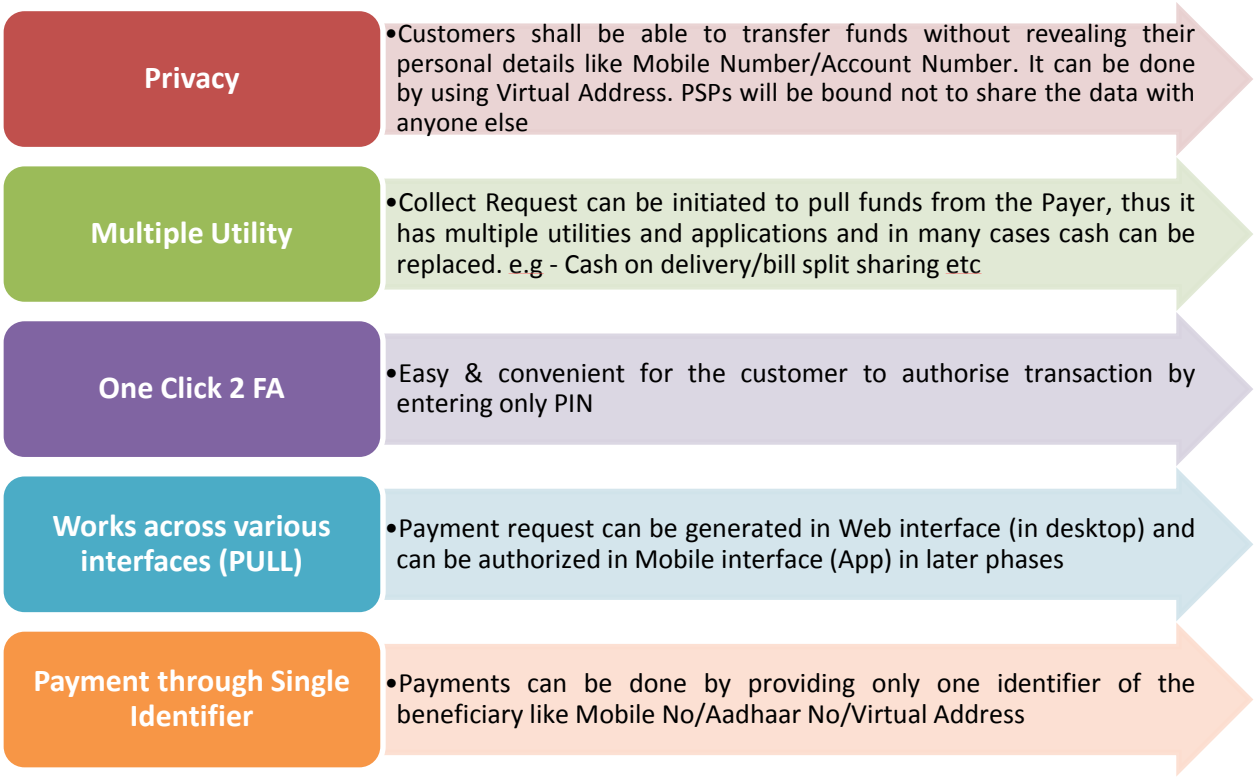
b) In case of non-banking entity providing App support development to Banks:
   - For non-bank entities who will be developing the PSP Application on behalf of the banks, due diligence shall be done by their respective banks in all aspects. The roles, responsibilities, obligations and liabilities will be detailed in the Procedural Guidelines.

5. BENEFITS OF UPI TO BANKS

For banks, UPI can be the real facilitator for mobile payments. Banks may leverage the exiting infrastructure and develop use cases for mobile payments. As smartphone penetration has grown tremendously over the years, there is an ever growing need of simplified, secure and easy to use mobile payment system. Banks can use UPI to cater these needs. It will facilitate the below:

a) Universal App for Payments
b) Security
c) Payments basis Single/Unique Identifier
d) Opportunity to tap Customer to Business (C2B) segment
e) Opportunity to tap E-commerce & M-commerce (PULL Initiated) transactions
f) Simplified (Single click 2FA) authentication

BENEFITS OF UPI TO END CUSTOMERS



6. ROLE OF NPCI LIBRARIES

NCI Libraries will be a set of utilities which will be available to the UPI Members which can be embedded into the PSP App. These libraries will be XML based and will be available for all the three major mobile operating systems viz. Android, iOS & Windows/Windows Phone. These libraries will facilitate communication with UPI and will allow secure capture of credentials like PIN. The PIN will always be captured by the NPCI helper utility (part of NPCI libraries) which will use PKI Encryption. NPCI libraries will also capture the secure credentials like OTP, Card Number, Expiry date etc when PIN is generated througn PSP App

6.1 HOW PIN WILL BE CAPTURED?

a) PIN is to be captured in the NPCI helper utility which will be embedded in the PSP app which is certified by NPCI.

b) NPCI will be using Public Key Infrastructure (PKI) to encrypt the PIN using Public Key stored locally. This encrypted block will be sent to the issuing bank which will decrypt & validate with the Private Key.

c) Banks should have a standardized PIN which will be 4 digit numeric.

d) Biometrics will also be captured in a similar way in a secured way.

7. PROPOSED FEE & CHARGE STRUCTURE

Non-Financial Transactions will include Balance Enquiry, Mini Statement, OTP Generation, Generate PIN, Change PIN, Mobile Banking Registration etc. and will not be limited to these transactions. In future, new transactions may be added.

NPCI will charge a flat switching fee for every successful transaction whether it is Financial or Non-financial transaction to the Initiator which will hit UPI. This charge will be in addition to the underlying product switching fee if the underlying product is used for credit leg.

8. BROAD PROCESS FLOW OF CUSTOMER REGISTRATION IN PSP APP

The customer who initiates the transaction should be registered for Mobile Banking service. Mobile Banking registration may also be possible by the customer through the PSP app whereby the customer will authenticate himself and then register for mobile banking alerts & alternate authentication. The respective issuer bank should provide this facility as complied with RBI guidelines. The below User Interface (UI) guidelines are only for reference purposes. PSP can do the innovation on the user experience part as they deem fit. The UI is fully flexible and PSP can create most intuitive user interface. But it should cover the below broad guidelines.

The PSP shall be updating the Account/IFSC/Mobile number/MMID details against the virtual address assigned by the PSP to the customer. These fields available shall form the local mapper at the PSP end for which it may have the customer agree to specific 'Terms & Conditions'

Step – I PSP Profile Creation (Registration):

1. Customer discovers the PSP application on the platform specific App Store / PSP Site etc. PSP is responsible for customer education.
2. Customer downloads the PSP application. Application has NPCI Utility embedded into it. Customer starts the configuration process
3. Customer specifies his mobile number
4. PSP server sends an SMS to the mobile phone to strongly bind the device. (PSP Objective is to verify the mobile number of the customer). The SMS may be read automatically or entered manually in the application depending on the OS capability.
5. PSP authorizes the mobile phone basis the SMS. (The user now creates a 'profile' with the PSP and Selects a user name / Virtual Address. He may also enter additional details like Aadhaar Number).
6. Configures anti-phishing protection (Recommended for PSP).
7. Customer selects password / other unlocking mechanism for the application. The PSP must provide the option for "Change Password" and "Forgot Password" option in the app.
8. Customer adds in any other information that his PSP may require to complete the process.

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 of the banks certified on UPI & available in the PSP app).
3. Mobile number is used implicitly basis the profile created.
4. An OTP request is initiated by the PSP app to the Issuer through UPI.
5. The app automatically reads the OTP or the customer enters it manually. It is once again verified with the Issuer through UPI.

6. When it is verified, the Issuer Bank sends the full details of the accounts including Account Number & IFSC registered for that mobile Number to UPI.
7. Customer selects the Account Number & IFSC which he wants to authorize for addition to the PSP application. Customer may be shown the masked data instead of full details.
8. The PSP app asks the user to enter the PIN to authorize.
9. 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
10. The PSP stores the account details received by the Issuer Bank in its database which will be mapped against the customer's profile, Virtual Address, Mobile Number, Adhaar Number etc.

Step –III Generate PIN:

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. UPI requests an OTP to the Issuer Bank on the basis of the account details entered by the customer.
3. The customer is asked to enter the last 6 digits of Debit card number, expiry date and the OTP (which is received by the customer).
4. The PSP app, using the NPCI utility captures the last 6 digits of Debit card, Expiry Date & the OTP.
5. The issuing bank will only allow the PIN to be set after validating both factors - Card details / OTP.
6. The customer enters the requested PIN (using the NPCI helper application) (Perhaps, enters it twice to confirm).
7. The PSP application sends it to the UPI and UPI sends it to Issuer bank by encrypting it with the public key using PKI.
8. The bank completes the request by decrypting the same with its Private Key and confirms the setting of the PIN.

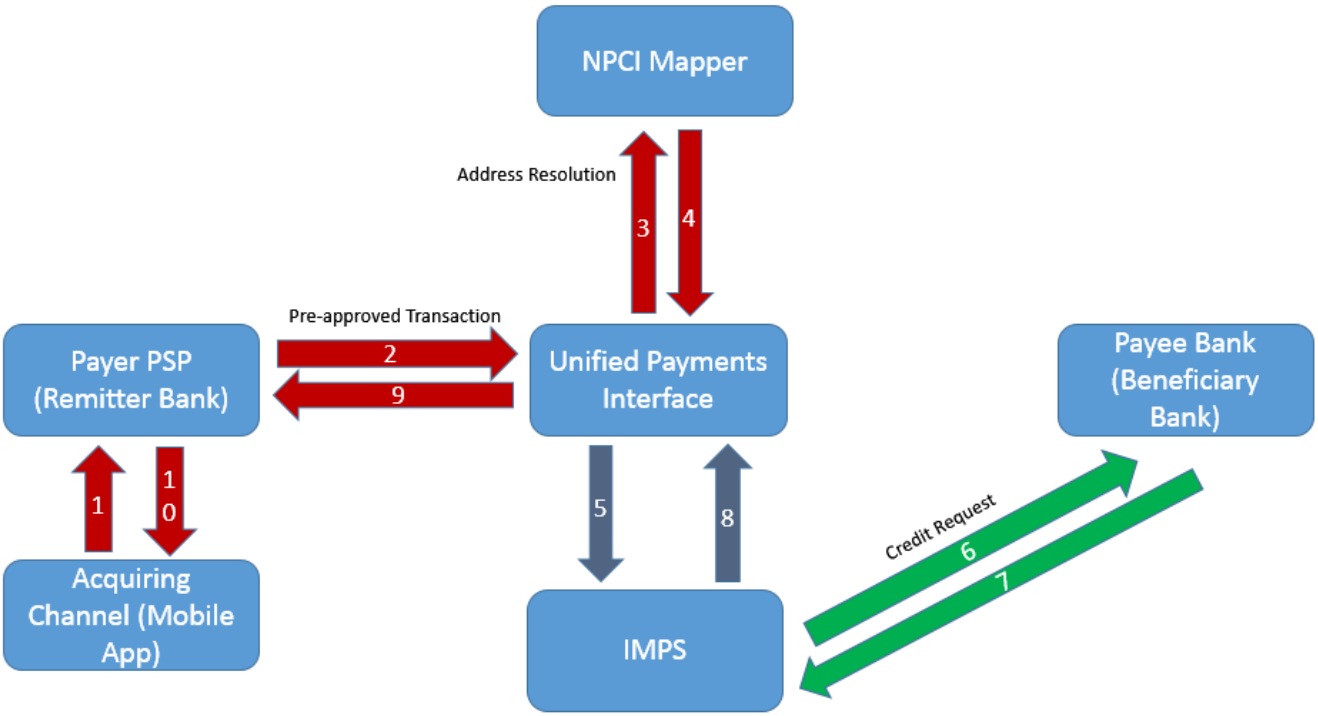
9. UPI FLOWS FOR GLOBAL ADDRESS TRANSACTION USING NPCI MAPPER

Global Addresses includes Mobile Number and Aadhaar Number. These global identifiers to account details will reside in the NPCI Mobile Mapper database which will be linked with UPI for resolving the account details when a request for routing comes with a global address. Below are some sample transaction flows.

Pay Request [Payer PSP & Remitter Bank are one entity]

Steps:

1. Customer enters the Mobile number/Adhaar Number of the intended Payee in the PSP app and authorizes the payment by entering the PIN.
2. PSP app 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 Mobile Mapper to fetch the account details of the payee for address transaction
4. NPCI Mapper responds with the relevant Account information associated with the queried identifier
5. UPI wil send a credit request IMPS
6. IMPS sends a credit request to the Beneficiary Bank
7. Beneficiary Bank credits the customer's account and responds back to IMPS
8. IMPS responds the same to UPI
9. UPI responds the successful credit to the Payer PSP
10. Payer PSP confirms the successful transaction to the customer



The above flows will be same for Aadhaar Number as well.

10. GLOBAL MAPPER UPDATE PROCESS

Aadhaar based payments are currently being processed using NACH application. For this purpose idea of mapping Aadhaar with Bank was first conceived and was institutionalized by NPCI. Aadhaar is predominantly being used for transferring all types of government benefits. However recently Government also mandated that benefits can be transferred using Account Numbers as well.

Further considering the other financial revolution and reengineering which is currently going on in our country like UPI, IMPS, NUUP, NPCI Central Mapper can be used for fetching and routing their payments. Hence having such a common repository can create a great process value add, for overall payment ecosystem and as a consequence to the end customer.

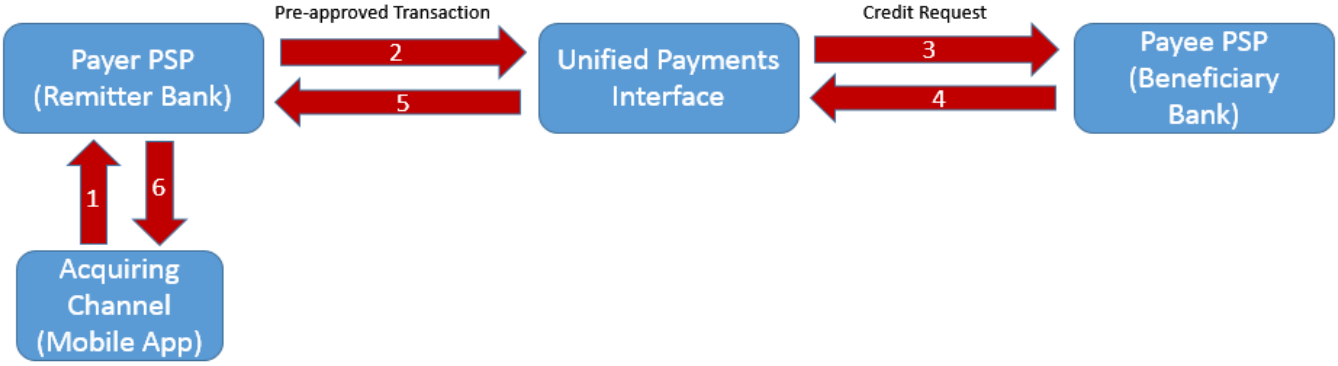
It is being explored if the member banks can utilize the existing process of Aadhaar seeding in NPCI Mapper and if the file formats can be same with the only addition being Mobile Number, customer name, Account Number, IFSC and other customer details. If this is agreed and approved by the appropriate committee(s), NPCI may release a Mapper upload document stating the file formats, new column additions etc. Banks may have a detailed process in discussion with NPCI for updating the mapper database through regular customer database updates, similar to the present NACH mapper update where the data is provided by the Banks for updating the fields.

11.FLOWS FOR TRANSACTIONS BASED ON VIRTUAL ADDRESS

TWO PARTY MODEL [Payer PSP & Remitter Bank are one entity AND Payee PSP & Beneficiary Bank are also one entity]

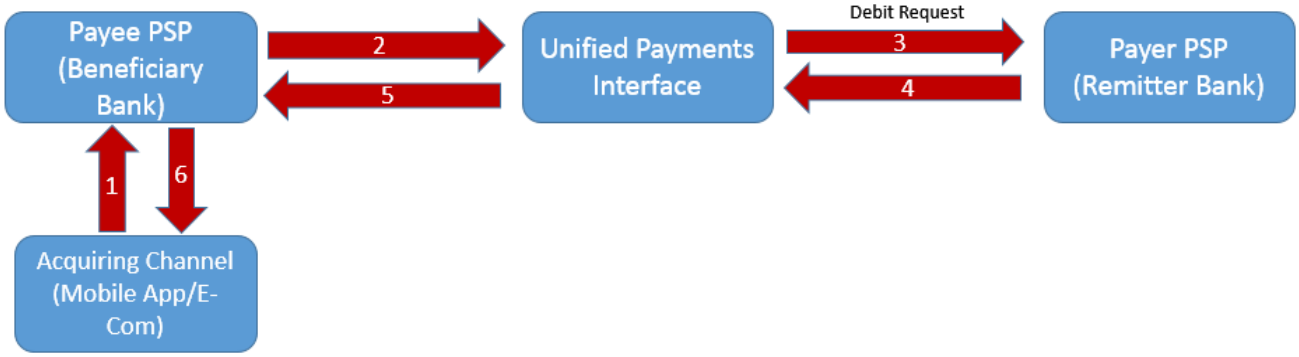
Pay Request (Steps):

1. Customer initiates a Pay Request by entering the Virtual Address of the Payee customer and PIN.
2. Payer PSP 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 credits the Payee Account & responds to UPI
5. UPI sends a successful confirmation to the Payer PSP.
6. Payer PSP sends the confirmation to the customer



Collect Request (Steps):

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 routes it to the respective Payer PSP basis resolution of the handle.
4. Payer PSP 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 confirmation to UPI.
5. UPI sends the debit confirmation to the Payee PSP
6. Payee PSP credits the customer's account and sends the confirmation to the customer

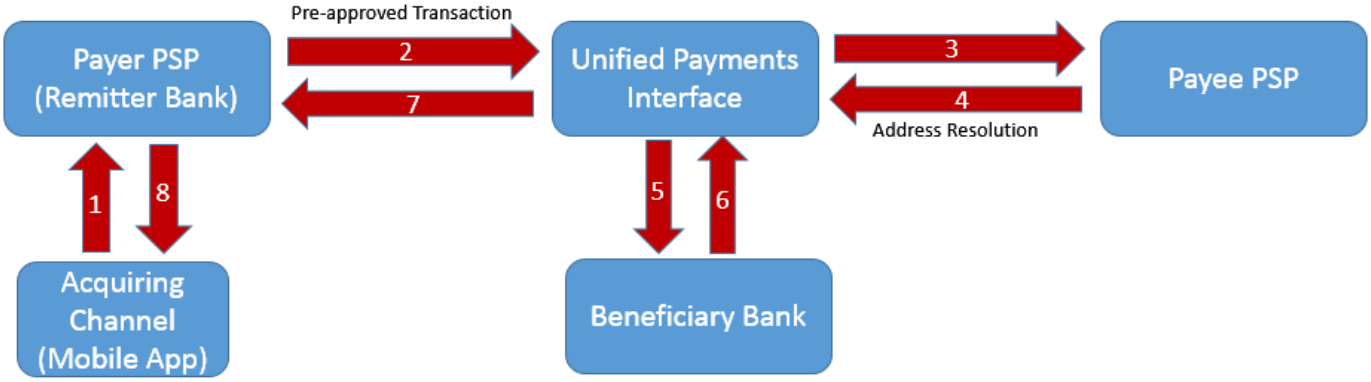


THREE PARTY MODEL:

In Three Party Model, Payer PSP & Remitter Banks are same entity AND Payee PSP & Beneficiary Bank are separate entities.

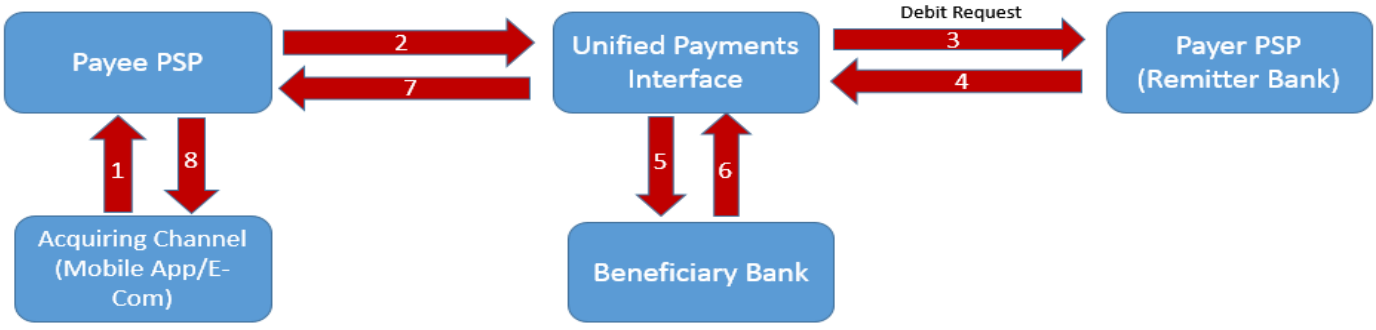
Pay Request (Steps):

1. Customer initiates a Pay Request by entering the Virtual Address of the Payee customer and PIN.
2. Payer PSP 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 and 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.



Collect Request (Steps):

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 routes it to the respective Payer PSP
4. Payer PSP 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 confirmation 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



12. CERTIFICATION OF MEMBERS

a) It is imperative that the members joining UPI are certified by NPCI. The process and the modalities along with the requisite test cases shall be finalized basis discussions and implemented accordingly.
b) It is also being explored if there is a need to certify every PSP Application that will talk to UPI. If the decision is in favor of certifying an application of the PSP, we will finalize the modalities thereto.

13. OTHER IMPLEMENTATIONS

It will be the responsibility of the PSPs to communicate the application to their customers, the process flow, education of the benefits and the features and related activities will be the sole responsibility of the PSP and NPCI has no role in it.

A. Liability clause for Banks & for Technology Service Provider:

a) NPCI will take the responsibility of the security of data when the data reaches UPI and is in NPCI Network. When the data is outside the reach of UPI and NPCI Network, its security & authenticity will be the responsibility of the entity on whose possession the data is.
b) Security & integrity of the data will be the responsibility of the PSP/Bank even in cases where the Bank/PSP & the outsourced technology service providers are different entities. Therefore, it is recommended that the banks do full due diligence of the outsourced technology service provider as they are dealing with sensitive customer data.

B. Due Diligence of Technology Service Providers:

A 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.

Among other things, the bank should also consider the following during due diligence:

a) Legal and Regulatory Compliance
b) Financial Position
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.

C. Broad Roles & Responsibilities Of the Members:

Below are indicative roles and responsibilities of the members.

The members shall 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/or frauds.
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 Member/outsourced Technology Service Providers.
h) The Member should inform NPCI in case of cessation of the sponsorship arrangement between the Member 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.
i) The Member 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.
j) The Member should carry out its activities under the regulatory supervision of NPCI. NPCI will periodically review operations of the Member with respect to sponsorship scheme from the point of view of risk and security, operational, and technical issues that are deemed important.
k) Member will ensure that they have a board resolution or approval from similar authority to that effect of adding outsourced Technology Service Providers/sub-members. Moreover, it will ensure that a copy of this resolution/approval is submitted to NPCI along with their letter requesting NPCI to include the outsourced Technology Service Providers/sub-members into the UPI Network. Member may periodically keep their board/management updated on the outsourced Technology Service Providers/sub-members added on their network.
l) Member 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. Member may conduct this due diligence annually or as per directions from their board
m) If any outsourced Technology Service Providers/sub-members 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 Member. In such a case, funds available in the bank's settlement account will be used to settle the claims of UPI member banks
n) The Member using the dispute resolution mechanism as detailed in the UPI Settlement Procedures document would be used to resolve exception transactions related to its outsourced Technology Service Provider/sub-member. Member would be held directly responsible for any discrepancies pertaining to reconciliation and adjustment
o) Member 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.

Member should also report to NPCI, any incidents causing operational risks encountered by its outsourced Technology Service Provider/sub-member with respect to UPI transactions

p) Member 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.
q) Member should comply with all such requirements, existing and future, with regard to the appointment and continuance as sponsor bank on behalf of its outsourced Technology Service Providers/sub-members
r) Member should only use infrastructure facilities and equipment provided by NPCI for the purpose for which they are permitted to be used
s) Member would be responsible for its outsourced Technology Service Provider/sub-member settlement and dispute management. Member will provide the reports to its outsourced Technology Service Providers/sub-member for reconciliation. Member would raise the dispute on behalf of its outsourced Technology Service Providers/sub-members in the stipulated time as per the UPI-PG
t) Settlement would happen through the respective Bank's RTGS settlement account maintained by RBI, DAD
u) 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.

14. GLOSSARY

Payer	Person/Entity who pays the money. Account of payer is debited as part of the payment transaction.
Payee	Person/Entity who receives the money. Account of payee is credited as part of the payment transaction.
Customer	An individual person or an entity who has an account and wishes to pay or receive money.
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.
Payment System Player	Banks and Payment Banks or any other RBI regulated entity that is allowed to acquire customers and provide payment (credit/debit) services to individuals or entities.
NPCI	National Payments Corporation of India.
RBI	Reserve Bank of India.
UIDAI	Unique Identification Authority of India which issues digital identity (called Aadhaar number) to residents of India and offers online authentication service.
IMPS	Immediate Payment Service, a product of NPCI, offering an instant, 24X7, interbank electronic fund transfer service through multiple channels.
2-FA	Two factor authentication.
PIN	Personal Identification Number should a four digit numeric PIN
OTP	One Time Password should be a six digit numeric OTP basis the existing validity period & usability defined by the banks
Remitter PSP/Payer PSP	The entity on whose interface PIN/Biometric authorization credentials will be captured
Remitter Bank/Payer Bank	The entity that will process the debit request
Beneficiary PSP/Payee PSP	The entity who will provide the Account details against a virtual address credit request
Beneficiary Bank/Payee Bank	The entity that will process the credit request