India readies Unified Payment Interface for mobile payments

The National Payment Commission of India ('NPCI') has implemented a 'Unified Payment Interface' ('UPI') to help consolidate payment systems in India. The UPI uses a single application programming interface ('API') - with a series of supporting APIs - to allow users to utilise their mobile phone as the primary device for all payments. The initiative could significantly bolster the use of m-payments in India, as Satish Padhi and Vaibhav Parikh of Nishith Desai Associates explain.

The Reserve Bank of India ('RBI') released a payment system vision document during the period of 2012-15 to proactively encourage the implementation of electronic payment systems, with the aim of ushering in a cashless society in India. While doing so, the RBI's mission was to ensure that payment and settlement systems in the country are safe, efficient, interoperable, authorised, accessible, inclusive and compliant with international standards.

Against this backdrop, the NPCI, which was set up in order to consolidate and integrate the multiple systems with varying service levels into nationwide uniform and standard business processes for all retail payment systems, took the initiative to implement a UPI to simplify and provide a single interface across all systems. Key features of the initiative are as follows:

- Simplicity - Paying and receiving money should be easy and everyone who has an account should be able to send and receive money from their mobile phone with just an identifier, without having any other bank/account details to hand, at a simple click.
- Innovation - The solution should be minimal, functional, and layerable so that innovations on both the payee and payer side can evolve without having to change the whole interface.
- Adoption - The solution should be scalable to a billion users and to large scale adoption. This should allow gradual adoption across smartphone and feature phone users and provide full interoperability across all payment players, phones, etc.
- Security - The solution should provide strong end to end security and data protection.
- Smartphone prevalence - Considering the fact that about 150 million smartphone users exist today and that number is expected to grow to 500 million in the next five years, the solution should offer a mechanism to take full advantage of that.

The UPI aims to offer a platform to facilitate the next generation of online immediate payments, leveraging trends such as increasing smartphone adoption, Indian language interfaces, and universal access to the internet and to data.

The UPI banks on certain industry trends that have/are expected to have a large-scale impact on financial transactions. These trends include smartphone adoption in India, which is exploding at a rapid pace; ubiquitous connectivity, with telcos aggressively expanding their 2G and 3G coverage across the country; the implementation of Aadhaar (a unique identification number for Indian citizens) by the Unique Identification Authority of India ('UIDAI'); and the fact that the existing systems offer very limited interoperability between the payment instruments like cards, mobile numbers, and Aadhaar numbers, and do not offer any mechanism to use 'virtual payment addresses' that can be used for various electronic transactions in an interoperable way across all banks and regulated players.

The RBI has taken steps towards improving cashless transactions; for instance, the Pradhan Mantri Jan Dhan Yojana, a financial inclusion scheme, is one example of such a development, and provides access to various financial services, such as basic savings accounts for low-income groups.

The opportunity is immense as e-commerce, both online and via mobile, offers a potential area for exponential growth in electronic payments. Payment is a large issue for the players in this segment and they will continue to look for technology that will improve the payments process. Thus, the NPCI has come up with the UPI, which is aimed at providing a platform that is unified, expandable, adaptable to the current scenario, real time, secure and can be monitored.

The working of the UPI

The core features of the UPI include, *inter alia*, the use of a single API with a series of supporting APIs to enable the use of the personal mobile phone as the primary device for all payments, including person to person, person to entity, and entity to person payments. It also involves the use of mobile devices to 'pay' ('push') someone as well as 'collect' ('pull') from someone, the use of Aadhaar numbers, mobile numbers, card numbers, and account numbers in a unified way, allowing payments to be made just by providing an address to others without having ever provided account details or credentials on third party applications or websites. It pre-authorises multiple recurring payments, similar to a electronic clearance service ('ECS'), using a standard set of APIs for

any-to-any push and pull payments; uses a fully interoperable system across all payment system players without having siloed and closed systems, and makes payments using one-click two-factor authentication all using just a personal phone without having any acquiring devices or physical tokens.

The architecture of the UPI involves a third party API integration, which can 'collect' payment from 'an address,' avoiding the need to share account details or credentials on third party applications or websites. Within this solution, payment authentication and authorisation are always carried out using a personal phone. Since this layer offers a unified interface, any-to-any payments can be carried out using a standard set of APIs.

The aforementioned architecture has three key essential features:

1. Every payment transaction must have source (payer) account details (for debit) and destination (payee) account details (for credit). 'Payment address' is an abstract form to represent a handle that uniquely identifies the account details in a 'normalised' notation.

2. One authentication is required to be performed by the payment service provider ('PSP') - for instance, verification that the correct mobile phone is being used - while the other authetication requirements are performed within the domain of the account provider. In this unified architecture, the objective is to enable multiple authentication schemes (account provider as well as trusted third parties like UIDAI's Aadhaar authentication) without tightly coupling with account provisioning and management so as to enable, in the future, one or multi-factor authentication schemes to be plugged into the architecture, as long as account providers allow such trusted external authentications.

3. Adopting third party authentication and using tokenless payment schemes, thus allowing banks to reduce the overall issuance (card, PIN, etc.) cost while still keeping authorisation and account management within their control.

With new players entering the payment landscape, it is to be expected that they will innovate to differentiate their services and to improve customer experience. Thus, the role of the NCPI becomes all the more important in order to ensure that the participants continue to innovate while staying interoperable with existing systems

Advantages

The UPI provides a significant advantage over current systems and can take mobile payments to the next level. Its value lies in using the customer's mobile phone as the primary device for all authentications and for authorisation for both 'Direct Pay' and 'Collect Pay' transactions. The value proposition of UPI includes simplifying authentication, simplifying issuance and acquiring infrastructure, flexibility for PSPs, flexibility for users, enabling one-click two-factor authentication transactions, stimulating innovation, embracing mobile adoption, embracing Aadhaar adoption and creating national interoperability.

The supporting infrastructure used by the UPI is the Aadhaar System. Aadhaar is based around there being a Unique Identification Code for each Aadhaar holder and through this, it is ensured that each transaction happens between two unique identities.

Data security

The primary challenge pertaining to the UPI is data security. For this purpose, information has been classified into three basic categories: Sensitive Data, Private Data and Non-Sensitive Data. Some pertinent concerns, and the methods being deployed to handle them, are as follows:

a. Account details are to be protected by verifying the account details with the account provider.

b. Authentication credentials must be encrypted during capture using the public key of the authentication provider and must remain encrypted until their use.

c. Measures should be specific and distinct for individuals and entities to protect against phishing. It must also be ensured that whenever a collect payment request comes, the PSP application should show the know-your-customer information of the requester, whitelisting information from the central system, and the transaction reference number (sales order number, transaction note, etc.) to help the payer make the decision whether to accept or reject the request.

d. Message security, trust and non-repudiability - Every message must be digitally signed and have a unique transaction ID. Also, all APIs must be done over a secure channel.

Conclusion

With new players entering the payment landscape, it is to be expected that they will innovate to differentiate their services and to improve customer experience. Thus, the role of the NPCI becomes all the more important in order to ensure that the participants continue to innovate while staying interoperable with existing systems.

The proliferation of smartphones, the availability of an online verifiable identity, universal access to banking, and the introduction of biometric sensors in phones provides India with a unique opportunity to take the lead in e-payments and to provide customers with enhanced security and unparalleled ease of use.

Satish Padhi Associate
Vaibhav Parikh Partner
Nishith Desai Associates, India
satish.padhi@nishithdesai.com
vaibhav.parikh@nishithdesai.com