Real-Time Payments Systems & Third Party Access

A perspective from Google Payments

November 2019

Google

Contents

Executive summary

Just as digital technologies have transformed so much of our lives, from access to information to communicating, the adoption of digital payments is fundamentally transforming banking systems, commerce, and societies around the world. Digital payments are full of promise. They can bring new levels of convenience and efficiencies, security and transparency, access and growth. Countries that have rolled out payment systems are already reaping the benefits. However, due to the inherent complexities of financial systems and of deploying digital technology, there is no one-size-fits-all model.

Rather, there are multiple models for expanding the adoption and usage of digital payment solutions in a country, from card networks in the developed world to closed loop stored value wallets and **Real-Time Payments (RTP)** systems that facilitate bank account to bank account transactions at relatively low cost.

In this paper, we'll focus on RTP systems. More than 50 countries have rolled them out, with many more in the works. RTP systems are the rails for modern payment infrastructures, offering near-instant transactions with a minimum of friction for all parties. They fundamentally change how payments are made and the ways in which they can become embedded in the new digital economy. They provide a foundation on which groups can build new services that evolve and improve payments for consumers, merchants, financial institutions, and governments.

One example of an especially successful RTP model is in India. In a relatively short amount of time, India has made substantial progress in transforming a complex and convoluted payments infrastructure. An ambitious plan that brought together government, financial institutions, and Third Parties, India's model is now ahead of what most financial systems around the world have achieved. Its success offers lessons for other institutions developing or considering the introduction of an RTP system.

This paper is neither a comprehensive review of India's payment system nor an analysis of policy. The development of any RTP system should be supported by a robust understanding of the key policy and regulatory issues that need to be considered, including aspects of institutional structure, data security, privacy, economics of pricing, disputes handling, and consumer protections.

These are exciting times in the world of digital payments, but in many ways it's just the beginning of a dramatic change in how the world transacts. We hope you find this paper useful and are also looking forward to what lies ahead as the inevitable transformation of digital payments continues to gain momentum.

Google

Terms (Glossary)

API: Application Program Interface. Code that defines a set of functions and procedures to allow two software programs to communicate with one another.

Attestations: public keys that serve as claims that can be cryptographically verified, matched to each attribute of the identity (e.g., verified phone number and separately verified email) or together for a set of attributes of the identity (e.g., device, phone number, and email address, all verified together).

Confirmation of Payee: a way of giving end users of payment systems greater assurance that they're sending their payments to the intended recipient.

Consent architecture: the ability for a Third Party app to get verifiable consent from the user for authentication and authorization. This allows the Third Party app to do actions that previously could only be done from a financial institution app, such as initiating payment.

Conveyance mechanism: tools that communicate coded information to digital devices. They can be either digital, such as NFC (Near Field Communication), or analog, such as a printed QR code.

Deemed transaction: when an RTP system is unable to fetch the status of the credit leg in real time, it marks the transaction as "DEEMED." The transaction is then resolved through manual reconciliation.

Federated identity: a forward-looking model of identity that offers a seamless user experience. It allows users to carry their verified physical identity without having to reverify on every new surface.

Idempotency key: a unique identifier used to guard against network disruptions.

KYC and AML: KYC (Know Your Customer) and AML (Anti-Money Laundering) systems are established by regulators and implemented by banks.

Mandate: permission given by the user to the merchant to pull funds from a user's account. For example, a user may let a subscription service set up a mandate to bill her account monthly for a fixed amount.

PAN: Primary Account Number

PSP: Payment Service Provider

Pull: refers to the act of requesting funds.

Push: refers to the act of sending funds.

RTP: Real-Time Payments. RTP systems are maintained by a central authority.

Settlement: the process of moving money. That movement is complete when the funds are settled among the institutions where customer accounts are held.

Third Party: an ecosystem player that develops financial technology to be used as part of an RTP. They are provided access to the RTP system via APIs. Third Party applications, through mobile payment apps or through a trusted browser, can initiate payments.

Trust Delegation: financial institutions can put trust in other participants of the ecosystem to run risk checks.

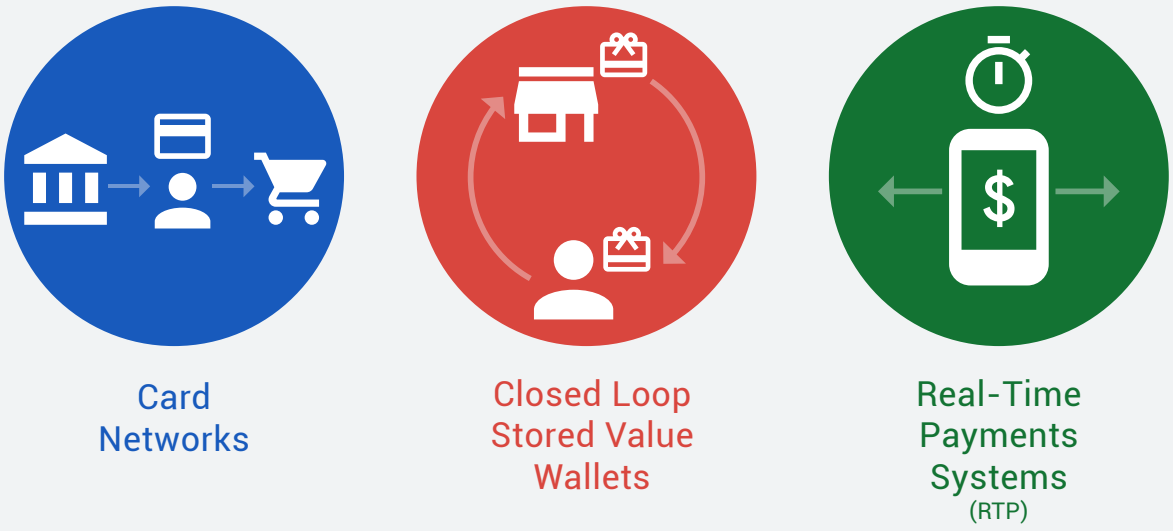
Foreword:

Real-time payments in action

Only a decade ago, a day without cash utilization/transaction was hard to picture. Today, in many countries around the world, there's no need to imagine a cash light society — you just use a card or a mobile device to pay for everything. At its best, the user experience is simple, more secure and nearly effortless. A tap or two and you've paid a merchant or split a bill with friends. But getting to an open, stable, and trusted payment system requires deep thought, smart regulations and significant investment from many committed parties — governments, regulators, and companies.

There are multiple models that can grow digital payments in a country. Card networks are popular in much of the developed world. Other countries have witnessed explosive success with closed loop stored value wallets. Many countries have built out **Real-Time Payments** (**RTP**) systems that facilitate bank-to-bank transactions at low cost.

Three different types of digital payment models

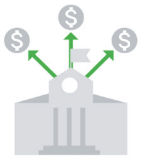


This paper focuses on RTP systems, which form the foundation of modern bank-centric payment systems, laying down the digital rails that allow for nearly instant transactions. Rolling out an RTP system is no small undertaking. Governments must rework regulations, define technical standards and protocols, invest in technology, and align financial institutions with the needs of merchants of — in particular small businesses — and consumers to deliver a trustworthy system that can drive innovation and growth.

Many governments today believe this effort is worth it. Mounting evidence clearly shows payment models such as an RTP system can bring myriad benefits — such as reducing poverty and corruption, and increasing GDP.[1] Foundational services become more accessible for consumers, new services are built, and richer data sources are brought to bear to continually optimize and improve the infrastructure.

The rollout of these digital payment systems aren't just transforming financial banking systems and commerce, but the countries themselves. The Boston Consulting Group estimates "that a move to a cashless model would add about 1 percentage point to the annual GDPs of mature economies and more than 3 percentage points to those of emerging economies.[2]

Stakeholders in the RTP ecosystem:



Governments
accelerate and increase commerce while fostering an accountable and accessible digital banking system for more citizens.

Financial institutions
gain new customers and sell their services.

Third parties
bring innovation to the ecosystem and aid financial institutions to integrate with millions of online and offline merchants, developing a better experience for all parties.

Merchants
get paid faster and spend less time on cash management.

Consumers
make payments quickly, reliably, and safely, and gain more control over their finances.

1 - Capgemini & BNP Paribas: World Payments Report, October 2018
2 - BCG, How Cashless Payments Help Economies Grow, May 28, 2019

So far, at least 54 countries have rolled out RTP systems, and by 2020, that number is projected to grow to 70.[3] With each rollout, countries learn from one another and further develop best practices that others reference. We've brought these learnings from various models into our technical recommendations.

The growth of RTP systems

Today's 54 RTP Systems Include:

Americas

Brazil
Canada
Chile
Colombia
Mexico
Peru
USA

Europe

Bulgaria
Croatia
Czech Republic
Denmark
Hungary
Iceland
Norway
Poland
Romania
Sweden
Switzerland
UK
20 Euro Countries

ME&A

Bahrain
Ghana
Kenya
Nigeria
Saudi Arabia
South Africa
Turkey

APAC

Australia
China
Hong Kong
India
Japan
Malaysia
New Zealand
Philippines
Korea
Singapore
Sri Lanka
Taiwan
Thailand
Vietnam

As millions more around the globe gain access to devices every year, many countries are making the most of mobile to develop innovative fintech platforms for the next billion internet users. For these newly banked consumers and merchants, no physical cards are needed; just a device. In fact, the growth of mobile devices now means systems in many emerging economies are poised to leapfrog ones used in the USA and EU.[4]

3 - FIS Global, Flavors of Fast report 2019
4- Capgemini and BNP Paribas, World Payments Report 2018

India is the primary example of this. Since launching its ambitious plan to use digital payments to transform its banking system, the country's RTP system is now one of the world's leading models. The decision to include Third Parties in the development of the model was key to this growth and has helped spur innovation and adoption on a massive scale. Google has had the opportunity to participate with the launch of Google Pay (formerly known as Tez).

Following our rollout of Google Pay, we've learned a lot as we worked across the ecosystem. As more and more countries develop RTP systems, we've been asked lots of questions about implementation, both strategic and tactical. We've evaluated a range of models, taking into account issues such as existing infrastructure, global standards, and societal needs. While there are various approaches governments can take, we believe many of the innovations and features we've pioneered with Google Pay in India will work globally.

To help answer those questions and share our learnings, we've put together this perspective, outlining technical principles and considerations for the ecosystem and offering recommendations for building a robust, scalable Real-Time Payments system.

The first section, "Case study: India transforms its banking system by rolling out the Unified Payments Interface system," highlights our experience deploying Google Pay in India, and offers a general overview of the major contributors to India's success. This section aims to aid governments and regulators' efforts to better understand what worked in India and how this may apply to similar initiatives in other countries.

The second section, "Our technical recommendations for an RTP system," contains detailed recommendations for building out its components. This section is aimed at empowering technical implementers of RTP systems to ask the right questions during setup, to ensure operational goals are achieved.

Overall, our experience and this paper suggest that in order for other countries to replicate India's success, building an open layer on top of any RTP system to allow for Third Parties to initiate payments is strongly recommended. The rails of an RTP are the foundation, but it is the overlay of services that improve usability and give consumers the frictionless payments they need and want. This drives participation at scale, transforming the entire payments ecosystem.

As evident with forward-looking countries like India, with the right regulations and technical infrastructure, RTP systems can catapult countries into the digital economy. This paper does need to be supplemented with a robust understanding of the key policy and regulatory issues, including aspects of institutional structure, data security, privacy, economics of pricing, disputes handling, and consumer protection.

I would like to thank Harish Natarajan and Ivan Mortimer-Schutts of the World Bank Group for sharing their perspectives and inputs with the team who prepared this paper.

This paper represents early inputs to the evolving understanding of policy and regulatory issues, including aspects of institutional structure, data security, privacy, economics of pricing, disputes handling, and consumer protection.

We hope you find this perspective useful, and look forward to working with present and future partners in the public and private sectors to help make money simple in countries around the world.

Caesar Sengupta

GM & VP, Payments & Next Billion Users, Google

Case study:

India transforms its banking system by rolling out the Unified Payments Interface

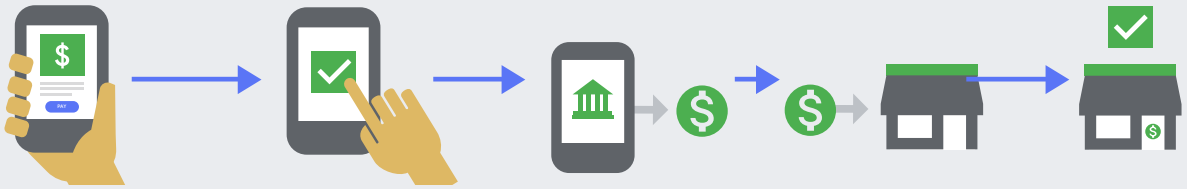
Google

Overview

India rolled out its **Unified Payments Interface (UPI)** system in 2016. Today, UPI is an impressive success. Thousands of merchants and millions of people use it every day, and 141 banks are live on the system.[5] UPI has been ranked as the top RTP system in the world on the basis of the system's standards, published **Application Program Interface (API)**, and participation of Third Party vendors.[6] UPI experienced a tenfold increase in value and an eightfold increase in transaction volumes in 2019 alone.[7] By 2025, digital transactions in India could be worth $1 trillion annually, with four out of every five transactions being made digitally.[8]

The introduction of Third Parties into India's RTP ecosystem was one of the most important developments, significantly accelerating adoption among both consumers and merchants. Google was among the first Third Parties and one of the first global technology companies to take part with the launch of Tez, now called Google Pay.

User Journey For An UPI Payment



Checkout

Consumer pays with his or her mobile device.

Consumer Initiates Payment

Using the Third Party app, the consumer initiates the payment and authenticates.

RTP Instruction

The instruction is sent to the bank to move money in the RTP system.

Payment

Money is moved from consumer's bank account to the merchant's bank account.

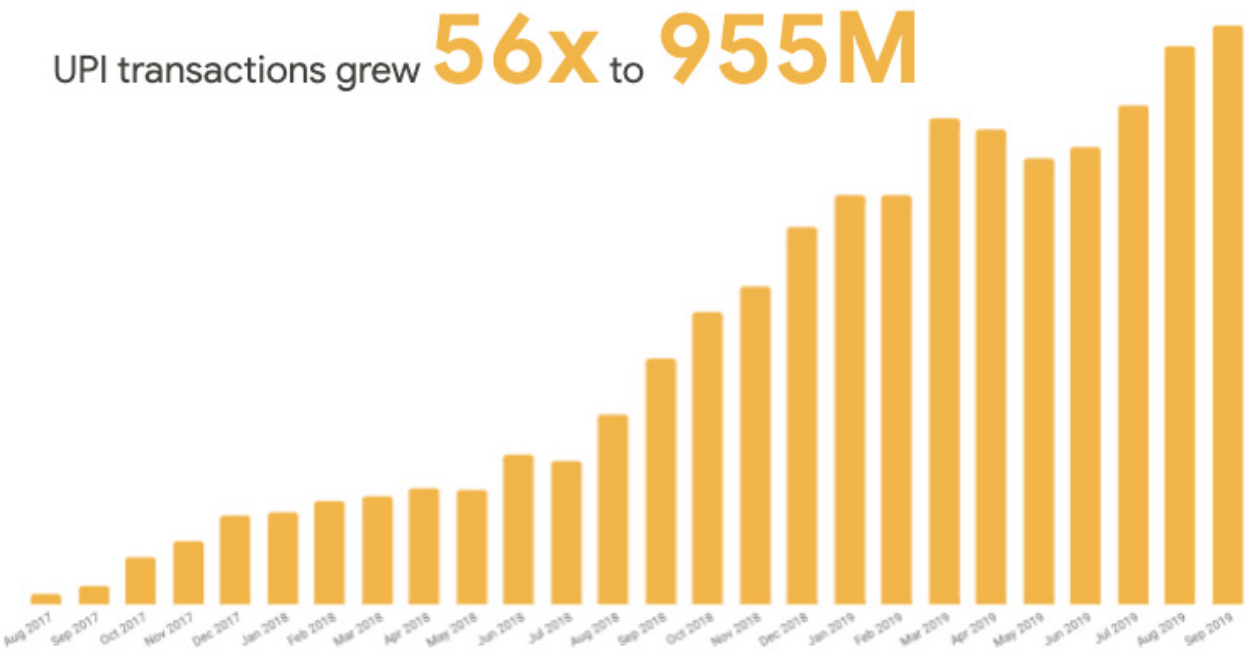
Merchant Confirms Transaction

The merchant sees that the money has been received into his or her bank account.

5 - NPCI Product statistics, https://www.npci.org.in/product-statistics/upi-product-statistics
6 - https://gomedici.com/status-check-real-time-payment-systems-across-world/
7 - FIS Global, Flavors of Fast Report 2019
8 - ACI Worldwide & AGSTTL Highlight Megatrends Shaping India's Digital Payments Revolution

The RTP journey for India

India's monthly UPI transactions have grown 56 times in just two years, from 17M in August 2017 to 955M in September 2019.[9]



India's journey to reinvent its payments system was incredibly ambitious. Until then, India had never been a reference model for payments. The country's payments infrastructure was archaic, with a limited regulatory structure and limited oversight, a norm of deferred transaction settlements, and a complex network of inefficient clearinghouses.
India began taking steps to modernize its payments leading up to the 2007 Payment

and Settlement System Act, which in turn led to the creation of the **National Payments Corporation of India (NPCI),** which oversees retail payments and settlement systems in India. The NPCI has been instrumental in fueling innovation through digital payments.

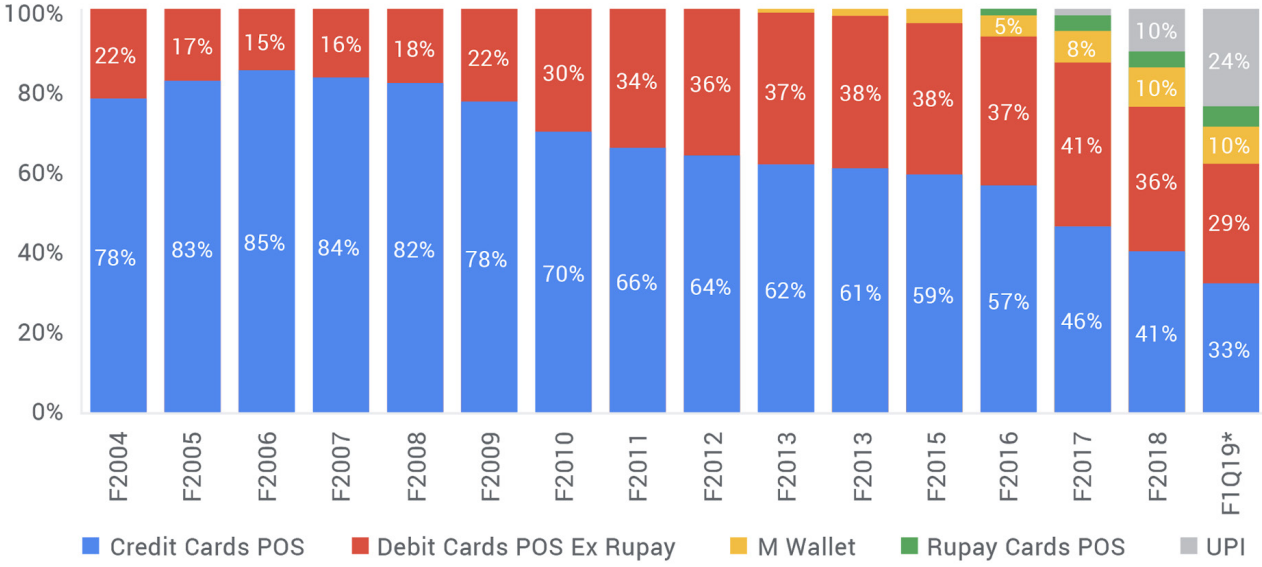
India took steps to innovate with the launch of the **Immediate Payment Service (IMPS)** in 2010 and followed it up with multiple interdependent initiatives to drive more people into the banking system and increase cashless transactions.[10] These initiatives included, for example, an effort to drive bank account penetration by mandating state banks open at least one bank account for each unbanked household.[11]

9 - NPCI Product statistics - https://www.npci.org.in/product-statistics/upi-product-statistics
10 - https://indiastack.org/about/
11 - https://www.pmjdy.gov.in/account

On the back of these initiatives, the number of people with bank accounts grew from 53% in 2014 to 80% in 2017.[12] Allowing users to send money bank to bank was only possible because of India's highly banked population.

The last critical cog in this initiative, UPI, was launched in 2016.[13] UPI is an overlay on IMPS, which exposes an API so that Third Parties can initiate payments.[14]

India digital payments mix

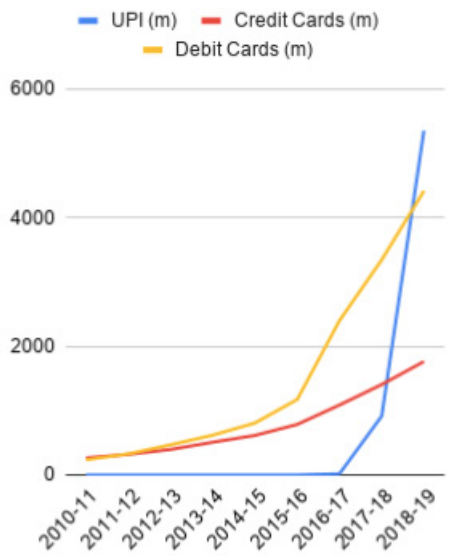


Along the journey, the Reserve Bank of India, the country's central bank, made several key decisions in its model. It took considered and ambitious steps to drive consumer adoption by mandating that payments made over UPI be free of charge for the first few years. RBI also helped to develop payment aliases (VPAs) for easy peer-to-peer payments. It invited all major banks to take part, and convinced the banks to agree to a common authentication system. The bank provided support to merchants with request to pay, in-app, and QR payments. And it designed UPI to include Third Party technology players.

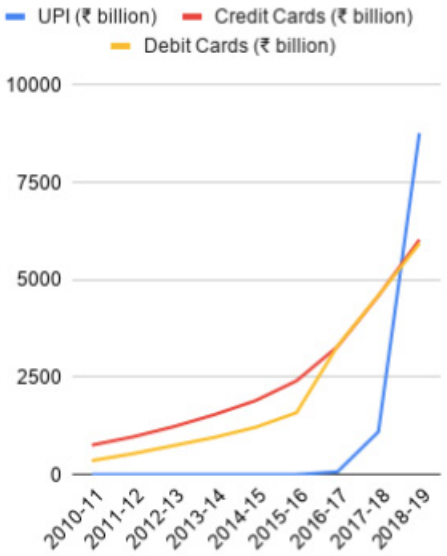
There were also areas that needed to be corrected. Deemed transactions proved challenging to deploy — ideally, the RTP system should query the status of the beneficiary account before initiating a transaction and then consider a transaction as successful as soon as a debit occurs. A central place could have been built to sandbox banks and conduct proactive health checks in order to avoid blocking threads/systems and affecting other bank payments. The system had some initial trouble scaling with the quick increase in transaction volume, and registration wasn't as smooth as many would have liked.

12 - WorldBank Findex Database, 2017
13 - https://indiastack.org/about/
14 - https://www.npci.org.in/upi-faq-s

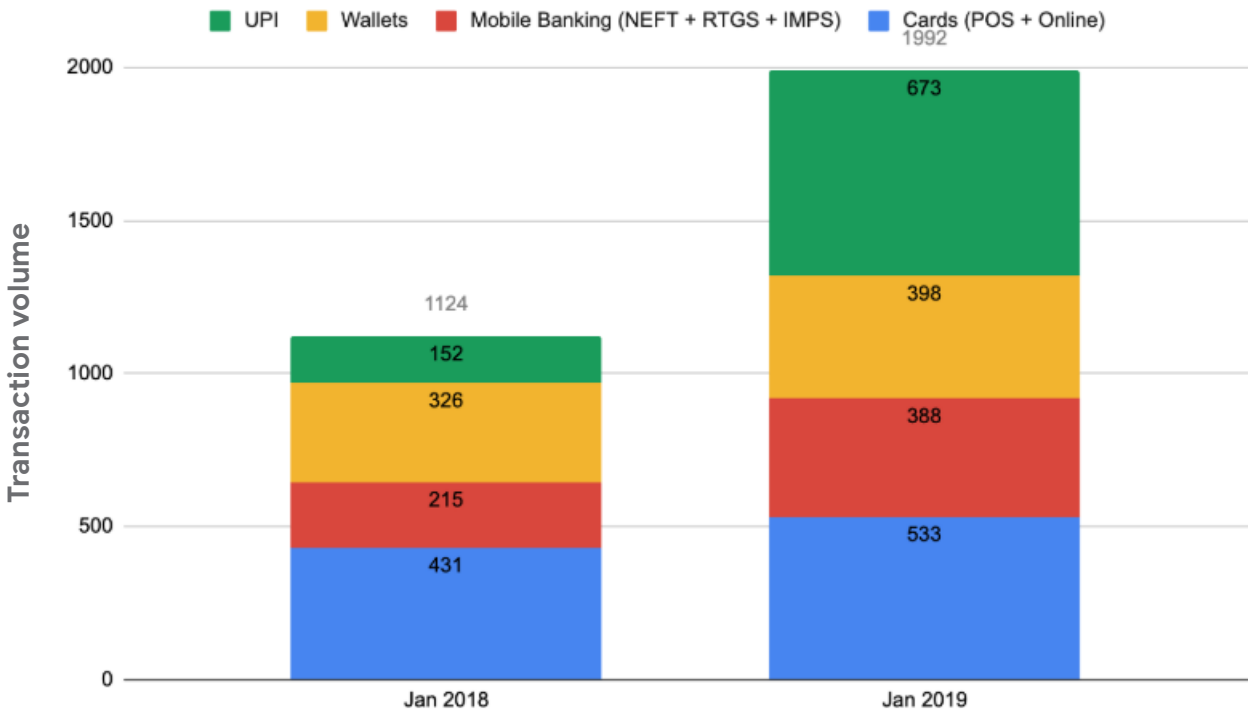
UPI, Credit Cards, Debit Cards Growth by Volume



UPI, Credit Cards, Debit Cards Growth by Value



Today, UPI is looked to as a reference model, but it took many iterations to get to where it is today. Through the vision of the government, RBI, and the participation of the whole ecosystem, the UPI has become one of the world's most advanced digital payment infrastructures. More than Rs 1.6 trillion (US$22 billion) a month now flows through the system.[15]



15 - https://www.npci.org.in/product-statistics/upi-product-statistics

Users can initiate transactions directly from their bank accounts, making paying someone as simple as handing over cash, whether online or offline. Merchants, whether small corner stores or nationwide retailers like BookMyShow, have found solutions like Google Pay significantly improve the payments experience for their customers.

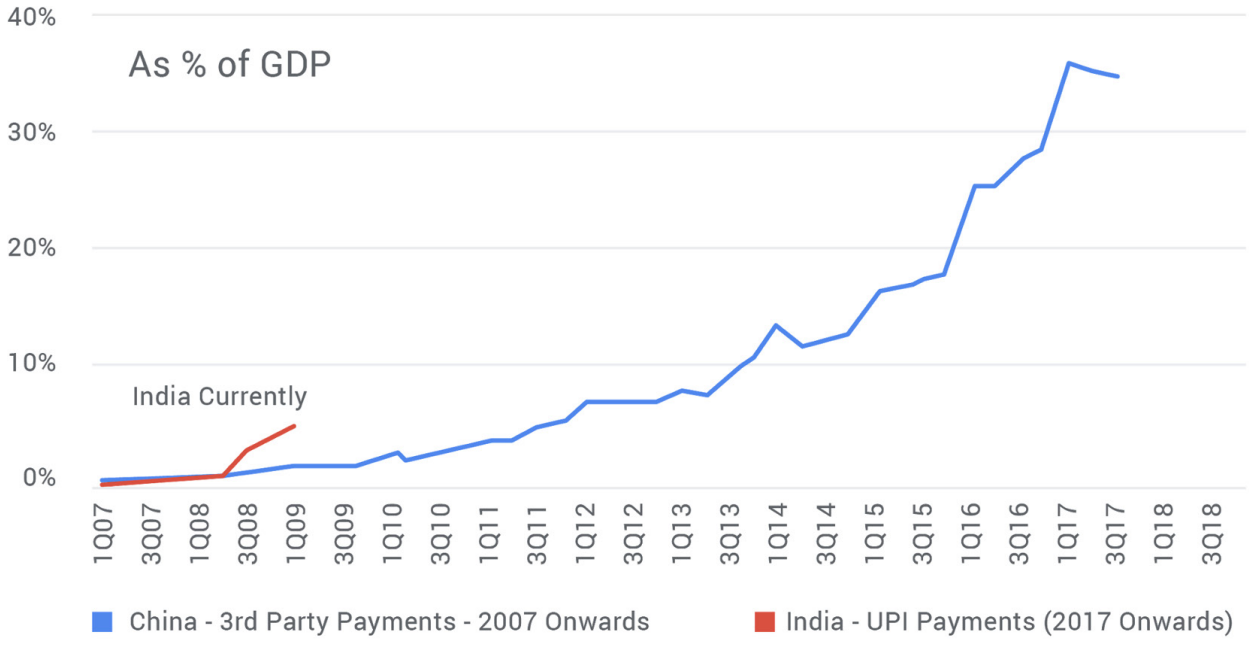
The introduction of Third Parties into India's RTP ecosystem significantly accelerated adoption. The UPI rollout has made India one of the world's leading innovators in digital payments, and many other major fintech companies, both domestic and international, have joined the UPI network, further strengthening the ecosystem.

> UPI has transformed the way people pay and transfer money digitally, making the entire process more seamless and secure.
>
> We believe UPI will continue to substantially drive the shift in customer behavior from cash to cashless, especially with merchant transactions on UPI being the next phase of growth.

Sanjeev Moghe

Head, Card & Payments, Axis Bank

Google Pay looks forward to continuing our work with our partners to support India's digital transformation, and to help other countries make the most of their RTP systems.



Source: IResearch, Morgan Stanley Research. Note: We have annualized Otober 2018 data for UPI to get 4Q18 data.

India and China — "India's UPI compared to China's third party payments (as a percentage of GDP); we expect UPI to be at 10% of GDP in five years."

What went well

Key success factors in the development of UPI:

Welcoming consumers:
To encourage usage, RBI mandated that payments made over UPI would be free of charge for consumers for the first few years.

Welcoming banks:
NPCI invited all major banks to take part in the ecosystem. The business model helped preserve an income stream for the **PSP (Payment Service Provider)** banks.

Welcoming merchants:
Merchant support includes request to pay, in-app, and QR payments.

Welcoming Third Parties:
UPI was designed to include Third Party technology players.

Authentication:
Banks agreed to a common authentication mechanism with a good user experience for all members.

Payment aliases:
UPI uses payment aliases (VPAs) for easy peer-to-peer payments, with interoperability between UPI apps through VPAs.

Learnings

There were several learnings along the journey that can be leveraged for future RTP systems:

Transactions:
Make sure the RTP system can support different payment types and processes, particularly request to pay, mandates, and refunds.

Painless registration:
Make the registration process as smooth as possible. Registration failures frustrate end users and test their trust in a system.

Design for scale:
Transaction volume can increase very quickly. The system needs to keep up to deliver on user expectations.

Prepare for instability:
Networks are unreliable by nature, and transactions can become stuck. Take steps to anticipate and plan for these occurrences.

Maintain a healthy RTP system:
Proper sandboxing of banks and proactive health checks can be built in a central place to avoid blocking systems and affecting other bank payments.

Over $110B in transaction value flows through Google Pay in India

67M
Monthly
Active Users

$110B
TPV ARR
Total Payment Value:
Annualized Run Rate

Google Pay

Google partnered with regulators and the payments ecosystem to launch Google Pay. This helped drive and scale UPI usage through the Google Pay app, which currently has 67 million monthly active users. Google Pay has enabled more than 2.5 billion transactions, and now has an annual run rate of over US$110 billion in transaction value. This drove not just basic payment services like peer-to-peer and peer-to-merchant, but it also paved the path to value-added services like instant loans.

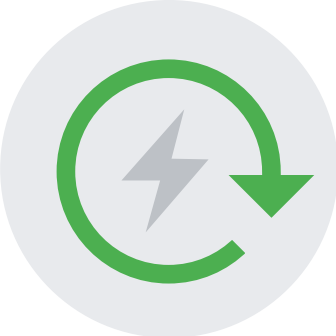
Since launch, we've been working with a range of partners, from merchants to large banks, to build out new features that drive growth and financial inclusion.

With Google Pay, we want to make sure there are as many places as possible for users to pay. In India, we've worked closely with large and small merchants. Google Pay users can now pay at more than 200,000 stores in more than 3,500 cities and towns, and more than 2,700 online merchants. Because of UPI interoperability, the actual number of merchants that accept Google Pay is much higher — more than 1.2 million small businesses use it.

Going forward, we at Google Pay are thinking about how we can go beyond payments to help SMBs grow and accelerate financial inclusion for consumers. We've rolled out a dedicated merchant experience with a rewards system, helping them communicate with their customers through messages and offers. We've also launched the Spot Platform, a digital storefront on Google Pay that allows merchants of all sizes to create, brand, and host however they choose, making them discoverable online as well as through a physical spot. And we're working with banks to connect with their customers in new ways and offer preapproved instant loans within Google Pay, without the need for additional documents.

Flexible Loan Amount

No Additional Paperwork



Funds Deposited Instantly

> Google Pay contributes a significant portion to our overall UPI transactions. The half-screen checkout on the Google Pay app makes the product easier to adopt, thus leading to a simple, hassle-free, and great user experience."

Marzdi Kalianiwala
Head of Marketing & Business Intelligence for the ticket-seller BookMyShow

Real stories

Vijay Babu owns a small laundry shop in Bangalore. Though he can't read or write, he was eager to go digital in order to cater to smartphone-savvy millennials.

A year back, he would have had to pay $100 for a credit card terminal, worry about printed receipts, and wait days to get paid.

With the help of his daughter, he set up Google Pay on his Vivo smartphone.

Today he's able to keep track of his transactions better, accept payments remotely, and build relationships with his customers through Google Pay's chat-based interface.

Sudhi, a shared auto-rickshaw driver in Kerala, actively asks his customers to install and pay him via "Tess," as he calls it (referencing Google Pay's earlier name, Tez). In fact, he even accepts payments from his employer the same way, citing speed and convenience as the most important reasons. And he likes not having to worry about carrying exact change.

Youraj, who runs a bhel puri shop in Telangana, prefers Tez/Google Pay over other digital wallets. "With other apps, I need to transfer money from my digital wallet to my bank account, which takes a lot of time. But with Tez, whether it's 10 rupees or 20, the money goes directly into my bank account, which is good!"

Mohammed Ahmed, a tea seller in Hyderabad, is replacing cash with Tez. "Most of the customers are asking if I have Tez. Out of curiosity, I asked one of my customers, and he explained that I can use this app to receive payment directly to my bank account without any charges. Since then I'm using this and getting all my payments directly to the bank account."

Technical recommendations for RTPs

Google

Technical Recommendations for the Building Blocks Of An RTP System

Transactions: Push or request

To best serve end users, RTP systems should support many types of transactions. To build out a robust merchant ecosystem, there should be secure mechanisms for all parties to both send (known as push) and collect funds (known as pull). Ideally, RTP systems should start out with a real-time, push-payment system.

Merchants should be able to request payments easily. For this use case, there might not be any need to support pull in the RTP system itself. The payment system could merely support an API call for "request for payment" from the payee to the payer.

Mandates

Mandates allow users to delegate permission to the merchant to pull money directly from their accounts. This is especially useful for recurring payments initiated by the merchant, where the user isn't in session. For example, a user can let a subscription service set up a mandate to bill him or her monthly for a fixed amount.

A mandate is set up during the initial payment time, at which point an identifier can be agreed on. During this setup, the user can be challenged to authenticate to ensure he really is the owner of the account setting up the mandate.

Once confirmed, the mandate is a proof of authorization, and should define terms of payments associated with it, such as limiting the amount of each transaction (example payment terms are listed below). Mandates should behave like promissory notes or traveler checks, honored by a bank on presentation.

Possible terms of payment include:

- A restriction on overall money exposure on the mandate. The user could specify the limit for either a specified time period, a total limit on this mandate without a time period, or a fixed amount. This could even allow one-time mandates to block funds with an end date, thereby reducing the available balance.
- Specifying the frequency and recurrence of the mandate.
- Users should be able to revoke a mandate, akin to revoking a standing instruction at a bank.

The Importance of refunds

If an RTP system allows user-to-merchant purchases, it needs to allow refunds in accordance with individual merchant's policies. Unlike purchases, it is important that refunds do not require user interaction. In a payment system, refunds are distinct from disbursements, and RTP systems should consider both.

Recommended principles:

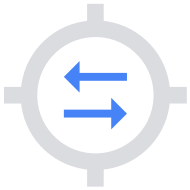
- Every refund should have a unique identifier.
- Refunds should be linked to the original transaction through a unique identifier.
- Refunds can be a partial value or multiple partial values of the original transaction.
- Online refunds should not require human interaction.
- The RTP system should allow delegated refunds, so an employee who does not own the account can initiate a refund on behalf of that business.

Clear & traceable merchant settlement

Settlement for merchants is the process of moving money from one party to another. That movement is complete when the funds are settled among the institutions in which customer accounts are held. It's critical to relay the right amount of data in the transaction so the merchant can properly reconcile its accounts.

Settlement often happens in bulk; one money movement for many customer transactions with that merchant. Whether the money is moved in bulk or individually, more data is needed for reconciliation than a programmatic bank statement can offer. To enhance this programmatic bank statement, data from a settlement channel should be provided.

Settlement data per transaction includes:



Transaction identifiers (provided at transaction time) to identify transactions that are being settled

Fees associated with those transactions

Taxes withheld (if applicable) for those transactions

This allows the merchant's accounting system to account for and reconcile all money received through this bank statement.

Conveyance mechanisms

There are multiple conveyance mechanisms available to implement a transaction.

Conveyance mechanisms are tools that communicate coded information to digital devices, and can be either digital or analog. Digital examples include NFC (near field communication) or proximity-based audio QR, used to transmit coded information via ultrasonic frequencies between devices.[16] An analog example is a printed QR code. Various conveyance mechanisms can be used to facilitate payments in the RTP system.

To facilitate e-commerce, there should be a mechanism for merchant apps to transfer to payments apps to accept payments. This should be done through a signed intent.

QR codes

QR codes are one of the most popular conveyance mechanisms, especially in emerging markets. Google supports a common standard for QR codes that can be used by all players in the RTP system. Regulators, banks, and merchants need to agree on the common QR code standard. There needs to be a consistent definition of which type of entities can receive payments through such QR codes.

We recommend building support for identifiable Confirmation of Payee. Confirmation of Payee is a way of giving end users of payment systems greater assurance that they're sending their payments to the intended recipient, which helps to counter fraud. For example, the QR code could be populated with merchant metadata such as business name, business registration number, merchant category code, and contact details. This metadata allows users to easily verify the QR code prior to payment and can help avoid payments being misdirected due to errors.

If banks aren't comfortable with sharing the Confirmation of Payee, signed QR codes can be used. The "signature" to sign the QR code would be generated by registered merchant acquiring entities, such as a bank or Third Party. The public keys used in the verification of these signed QR codes should be published via a single central and trusted repository.

These signed QR codes can be verified at the time of scanning to ensure the codes haven't been tampered with. To help users recognize the difference between a signed and an unsigned QR code, they should be shown a unique visual indicator that differentiates the QR codes. Dynamic QR codes are more resistant to fraud than static QR codes. A complete solution would have a dynamically generated QR and a basic point-of-sale system to confirm the transaction.

For more about QR codes, see this document's Annex.

16 - https://india.googleblog.com/2017/09/introducing-tez-mobile-payments-and.html

Tiered KYC

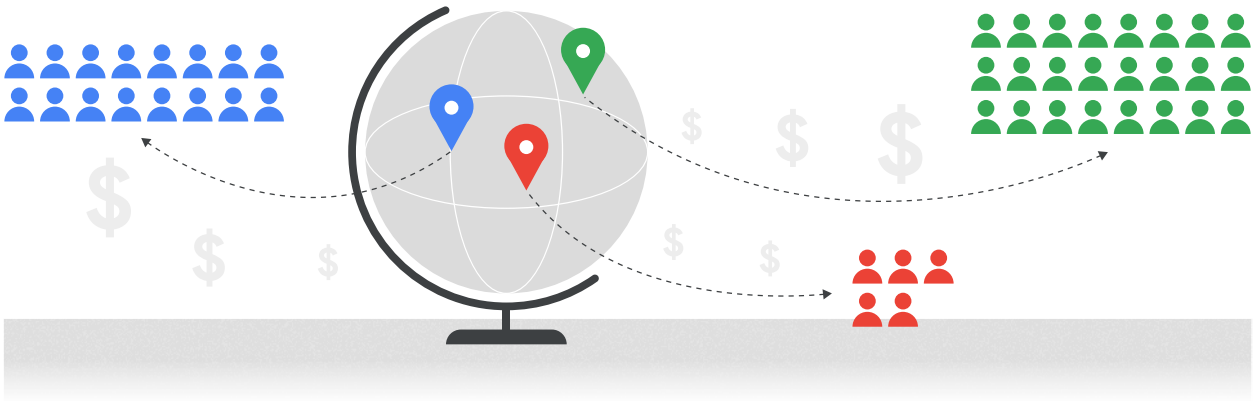
Consumers and merchants are subject to **KYC (Know Your Customer)** and **AML (Anti-Money Laundering)** requirements.

According to the Bill & Melinda Gates Foundation, "Tiered KYC can dramatically increase access and financial inclusion . . . 'micro-tiers' that enable those people lacking documentation to open basic accounts and manage the risk related to these accounts by imposing strict maximum account balance and transfer limits."[17]

Standardized authentication and biometric-enabled National IDs can also help to enable electronic KYC methods. KYC can in turn enable the lower tiers of tiered KYC, which make it easier for consumers to open bank accounts to make digital payments.

As for merchants, there should be a clear standard for how to become a merchant, agreed upon by all players in the ecosystem. Once payees identify as merchants, they are subject to different and specific KYC and AML requirements than consumers are, with the requirements depending on the volume of money they move. Small- and medium-sized businesses may not be able to comply with all the existing requirements. Tiered KYC requirements for merchants can help here, as can methods to onboard merchants digitally through eKYC.

The option of onboarding merchants via eKYC also has the potential of serving as a disruptive innovation, driven by Third Parties.[18] With adequate access as well as limited system trust (to update specific information pertaining to the merchant in the system), select Third Parties can develop more cost-effective ways to reach low-income retailers.



17 - https://leveloneproject.org/the-guide/payment-systems-lessons-learned-and-highlights/
18 - http://documents.worldbank.org/curated/en/765851467037506667

Deterministic status of transactions

An RTP system should ensure the transaction reaches a terminal state of Success or Failure in real-time. Transactions being in an "unknown" state can be an issue for the end user. For example, if the credit leg of a transaction times out and the RTP system is unable to fetch the status of the credit leg in real-time, the transaction ends up stuck. Often, the only way to resolve this is through manual reconciliation, which involves work from the end user and the bank. This can undermine confidence in and satisfaction with the system, and thus frustrate attempts to expand uptake and usage by underserved consumers and merchants

There are some ways to avoid and reduce unknown states in an RTP system:

If the RTP system uses Real-Time Gross Settlement (RTGS) for settlement:

We can use RTGS for small value transactions as well. The advantage of RTGS is that all the banks have their accounts with a central bank, so debit/credit happens within the central bank accounts in a transactional way instead of two separate calls, first debit and then credit.

If the RTP system uses batch settlement or netting:[19]

Proceed with dry credit and process as debit:

- Check if the payee account is good for receiving payments with details of the transaction (dry credit).
- If so, execute the debit.
- The transaction can be considered complete now, and the credit can be triggered in an async fashion.

Add-on commit message by coordinator (optional):

- This is an extension of dry credit on the lines of a two-phase commit protocol.
- The central network can play the role of the coordinator.
- The initial prepare phase will be a dry debit and dry credit, as above.
- If both dry debit and credit succeeds, the network can commit the transaction and send updates to both remitter and beneficiary (i.e., attain finality of payment).
- If either of the dry legs fail, the network considers the transaction failed and notifies the remitter and beneficiary accordingly.
- The remitter/beneficiary always check with the coordinator if there is no commit message after the initial dry credit. This obviates the need for manual reconciliation, making the protocol scalable from an operations perspective.

19 - https://www.bis.org/cpmi/glossary_030301.pdf

Idempotency

Networks are often unstable and unreliable. This causes issues for payment systems, as a flaky network connection leaves the initiator wondering if a payment has gone through, or if it should be retried. There is no getting around network errors. In order to solve indeterminate states with a payment, idempotency must be used.

Using this method, each network call has a unique idempotency ID. If the initiator of a network call provides an idempotency ID for the same network call twice, the receiver should only ever take action on that call once.

In addition, adding an API to get the status of the call using the unique ID can help players build out idempotency.

Financial institution uptime & health

Central systems and FIs should spend time investing in the right infrastructure to support a high volume of transactions. With proactive health checks of each FI, the system can make sure it doesn't send through a transaction that might not get completed. With proper sandboxing of FIs, the health of one bank will not affect the uptime of the whole system.

Recommendations for a National Addressing Database (NAD)

As countries enable digital payments, they need a way to identify a user and link that user with a financial institution. The Bill & Melinda Gates Foundation states that "the use of a persistent identifier for end users (both individuals and enterprises) is important for fraud control."[20] Live examples include PayNow in Singapore, PromptPay in Thailand, and DuitNow in Malaysia.

We recommend that governments use a central body to maintain a **National Addressing Database (NAD)** to map each user's identity to a financial institution account. A central body can give permission to various payment providers and financial institutions to add and update fields in the NAD. Any addition or update to the NAD should ideally be done with strong customer authentication.

Identifiers should be:

- Easy to remember
- Easy to share without risk
- Interoperable

Creating new IDs specifically for using a payments system is onerous for users. Additionally, using national IDs or bank account numbers leads to user concerns about the privacy and security of sharing these numbers (as with identity theft).

We strongly support a directory service that allows RTP systems to route end-user payments using the recipient's alias, such as email address or phone number, which can serve as an identifier, rather than their bank routing and account information.

Instead of storing the real bank account number or PAN, the NAD should store an "Account Reference," which can be sent to the financial institution to look up the payee account. This Account Reference should be generated by the payee bank.

The NAD should provide APIs to:

- **Register**: Link a user's identity with a financial account
- **Lookup**: Query using a user's identity & return the linked financial account
- **Delete**: Remove the user's entry in the NAD

20 - https://leveloneproject.org/the-guide/payment-systems-lessons-learned-and-highlights/

Recommendations for including Third Parties

Companies with financial technology (fintech) expertise are an important part of the RTP ecosystem. These Third Parties put their resources toward developing innovative services and apps that work on top of the rails of an RTP system. By making the most of mobile and online operating systems, they can distribute and market these services at scale, helping drive adoption of RTPs.

Competition among Third Parties leads to innovation within the ecosystem, which benefits consumers, merchants, financial institutions, and governments. As more consumers take to RTPs, their needs encourage Third Parties to improve usability, leading to easier, simpler services. Third Parties can help move RTPs beyond just P2P payments and into more sophisticated B2C and C2B real-time settlement services, such as tax refunds and disbursements for insurance or medical claims. More data becomes available as more people user RTPs, and this can be used to improve and diversify services, better manage fraud, and strengthen trust.

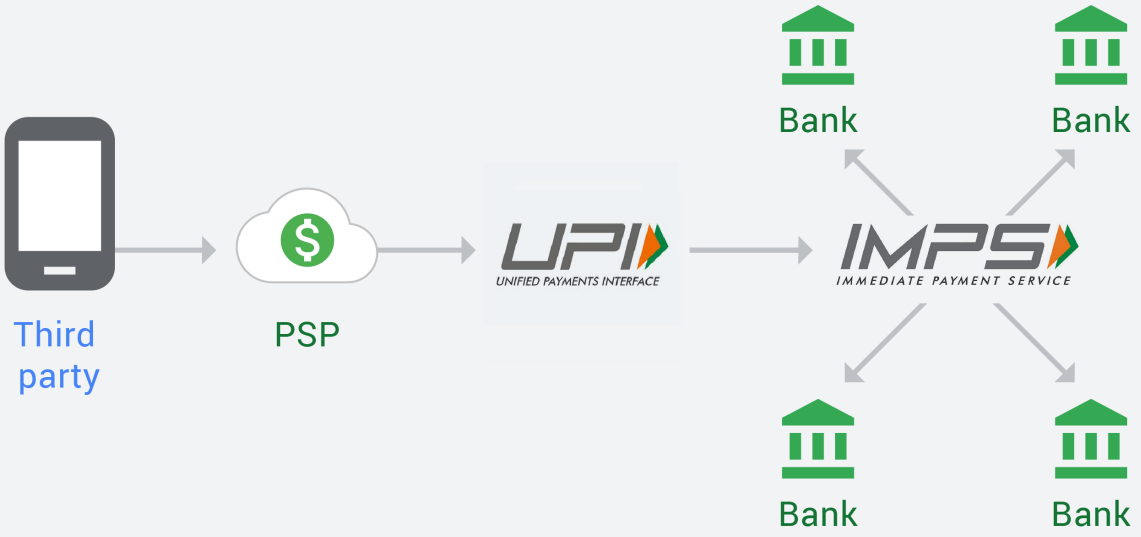
Other groups support this approach as well. For example, the Level One Project, an initiative from the Bill & Melinda Gates Foundation that seeks to create inclusive, interconnected digital economies in every country around the world, recommends that payment systems allow non-banks to transfer value.

> Often, these non-bank providers can access consumer populations that branch banking cannot or doesn't reach. An increasing sophistication of thought among regulators seems to be leading to the conclusion that allowing non-banks as direct participants in payments systems may promote competition and innovation, leading to better and lower-cost services for consumers and businesses. [21]
>
> **Level One Project**

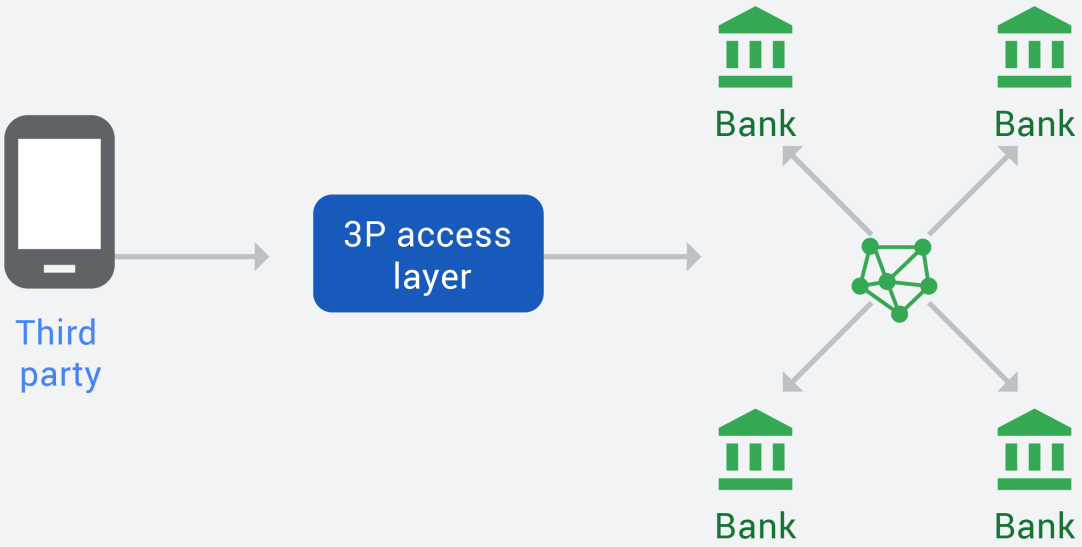
We've put together recommendations around how to best design an RTP system that includes Third Parties, covering solutions in the areas of authentication, identity, and trust.

21 - https://leveloneproject.org/the-guide/payment-systems-lessons-learned-and-highlights/

India's implementation



Our recommendation



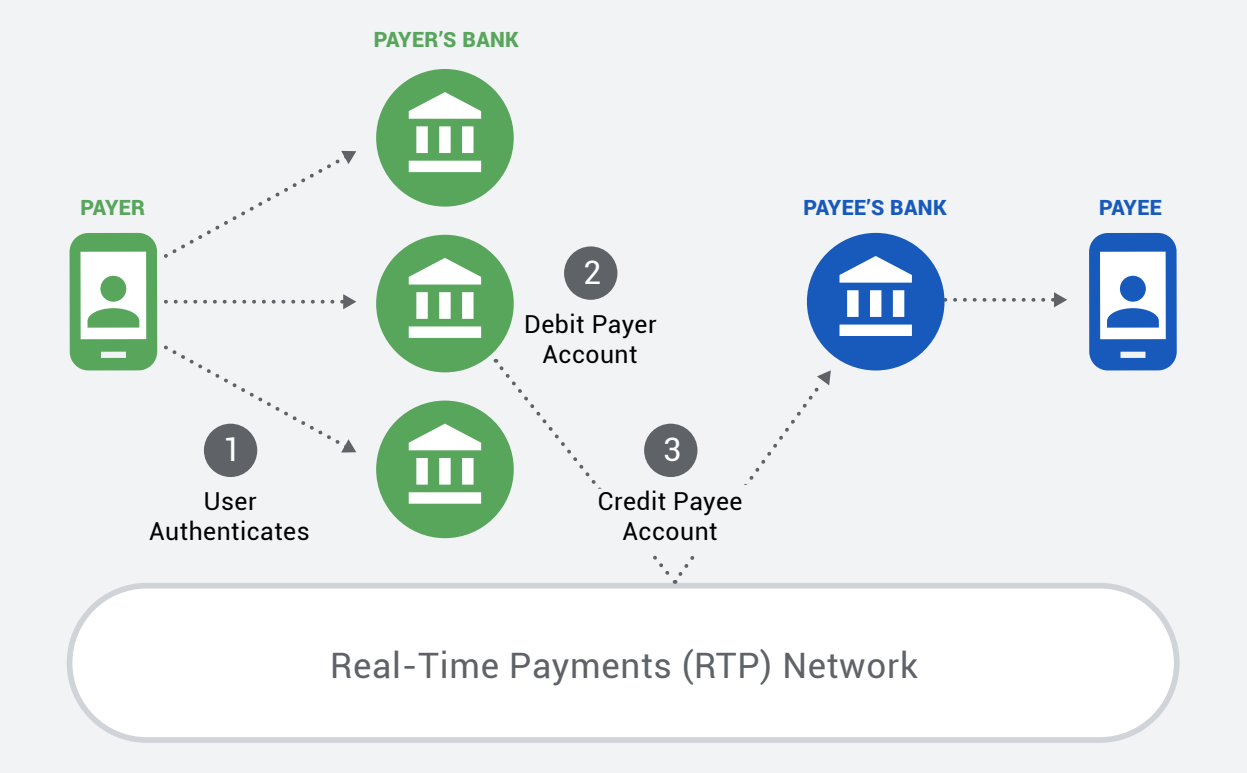
Direct access to the RTP system with a standardized API

We view standardized APIs as the best way for Third Parties and FIs to gain access to an RTP system. Standardized APIs offer a consistent, programmatic way to access the resources of the system, and — as the Gates Foundation points out — also "lower the costs of innovation and access." [22]

In many countries, Third Parties can move money on the RTP system by making an API call to a connected financial institution. However, this has some limitations. Integrating with each FI only allows Third Parties to move money from that FI's users, and Third Parties need to integrate with each bank individually.

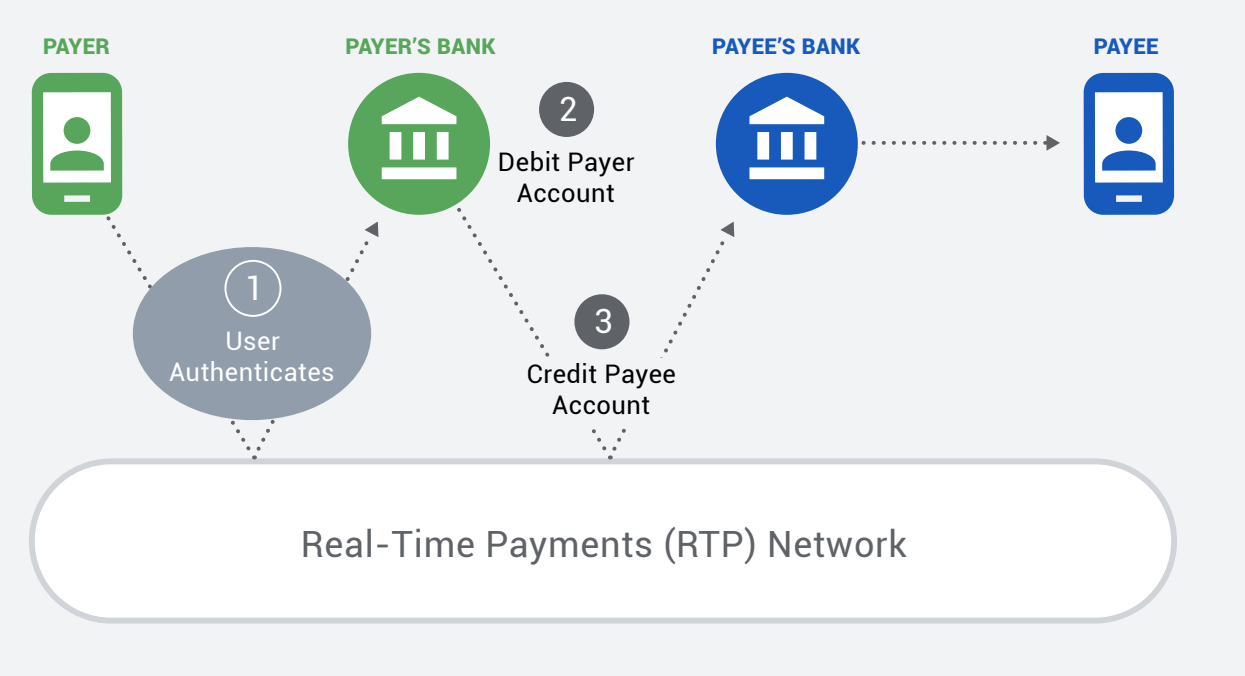
There are two ways this can work. We recommend the second approach where feasible.

1. Some countries, including the UK with its use of the Open Banking Standard, have tried to mitigate this work by mandating all banks comply with predefined standards.[23] Standardizing APIs across banks for payment initiation leads to lower friction for both financial institutions and Third Party participants. It allows fintechs with knowledge in building standard APIs to help banks where needed. It also reduces the need for bespoke integration. However, Third Parties still must commit time to quality assurance and testing with each bank.



22 - https://leveloneproject.org/the-guide/payment-systems-lessons-learned-and-highlights/
23 - https://www.openbanking.org.uk/about-us/

2 The RTP system can expose one central API for money movement. Ideally this API can be exposed directly from the RTP system, but it could also be done through a PSP (usually a financial institution). With one secure integration, the Third Party is able to move money to and from any connected financial institution. In UPI, by integrating with one PSP, Third Parties can now move money through 144 banks. Direct access is better than access via a PSP as it reduces dependency in case one or more of the relevant PSPs go down.



Furthermore, the API layer can go beyond initiating payments, delivering innovative use cases that upsell bank products like Paylater (a service that allows consumers to delay payment or pay by installments), instant loans, and personal financial management. UPI 2.0 supports the ability to pay later. [24]

> By standardizing messaging, UPI has allowed for an unbundling of accounts from customer experience and the rapid adoption of payment apps like Google Pay. It has already massively changed the way digital payments are made in India, and use of the service is still growing rapidly. [25]
>
> **William Cook & Anand Raman**
> *"National Payments Corporation of India & the Remaking of Payments in India"*

24 - https://www.cgap.org/sites/default/files/publications/2019_05_07_NPCI_Working_Paper.pdf
25 - https://www.cgap.org/sites/default/files/publications/2019_05_07_NPCI_Working_Paper.pdf

The right approach to authentication

Secure authentication is critical to any RTP system and should be developed to deliver the best user experience. Authentication proves that the user is who she says she is, and that she owns the account at an FI.

Recommendations include:

User experience

- Authentication can be done from many surfaces, including a Third Party surface, without having to redirect into an FI surface. An "embedded" experience is most seamless for the end user, and can still meet security requirements (see the point on security below). The European Commission mentioned in Article 32-3 of the Regulatory Technical Standards that redirecting may be considered an "obstacle to the provision of payment initiation and account information services."[26] The **Euro Retail Payment Board (ERPB)** also makes the recommendation in its November 2017 report on payment initiation services[27] that "The PSU [user] should not be required to access an ASPSP [FI] webpage as a part of the authentication process or any other relevant function as this would limit the PISP [Third Party] in the innovative design of its customer interfaces."

- Develop one authentication standard, regardless of the user's FI. FIs can pick a few factors they want to verify for the user.

- Create a tiered authentication model, so that a second factor can be called in for risky transactions.

Security

- Strong device binding between a user's device, phone number, FI account, and some other form of digital ID can be the basis for secure authentication. If an RTP system identifier exists, it should also be included.

- We recommend leveraging a user's smartphone as a hardware token. The user can also set up an additional factor, with forward-looking authentication models such as biometrics built on top of trust delegation and leveraging FIDO standards.[28] (FIDO is an alliance that uses standard public key cryptography techniques to provide stronger authentication.)

- Requiring device unlock (via PIN, fingerprint, or Face ID) means a form of "something you know" or "something you are" is also included.

- Consider a trust expansion model: Once one device is verified to be trusted, that trust can be transferred to more devices using that first device, provided they meet security standards. It should be simple for the user to revoke the trust at any time.

26 - https://fidoalliance.org/wp-content/uploads/FIDO-PSD2-customer-journey-white-paper.pdf
27 - https://www.ecb.europa.eu/paym/retpaym/shared/pdf/8th-ERPB-meeting/PIS_working_group_report.pdf
28 - https://fidoalliance.org/how-fido-works/

Strong device binding, or a 'tied device' between a user's device, phone number, FI account, and some other form of digital ID can be the basis for secure authentication.

In a working paper published in May 2019, CGAP highlights the approach to authentication as a key part of the success of UPI. "Through a mandate issued in 2013, RBI requires that payment transactions in India use two-factor authentication. UPI transactions use the physical phone as the first factor (the "what you have" of a registered device)."[29]

Strong device binding is a form of digital authentication. Digital authentication generally involves users electronically presenting one or more "factors" or "authenticators" to prove or "assert" their identity — i.e., prove they are the same person to whom the identity or credential was originally issued. These factors can include something you are (e.g., fingerprints), something you know (a password or PIN), or something you have (an ID card, token, or mobile SIM card).[30]

In the case of strong device binding, the process of linking a device utilizes a number of these factors for authentication, depending on the type of phone being used. For example, feature phones would be limited to authenticating via something the user has (the SIM/phone), as well as he or she knows (a password or PIN). More advanced phones could also leverage factors pertaining to physical qualities (fingerprints, facial recognition, etc.). Regulation may therefore choose to treat a user authenticated through a feature phone differently than one authenticated by a smartphone.

In addition, leveraging the **Trusted Execution Environment (TEE)** during the user registration process can help detect compromised devices. Available on most mobile operating systems, TEEs require hardware-based authentication, are physically on board devices, and are highly resilient to software-based attacks. These environments can therefore keep sensitive information secure even when a third-party app has been compromised.

29 - https://www.cgap.org/sites/default/files/publications/2019_05_07_NPCI_Working_Paper.pdf
30 - https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf

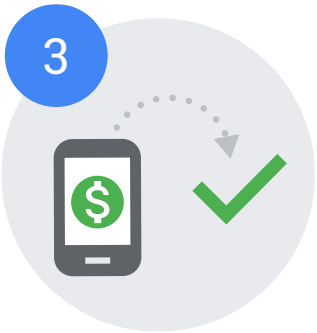
Authentication is needed at the time of payment or viewing account information. We can set up secure authentication in three stages:

User registration

Establishes strong device binding between the digital identity and the device, which is mapped to an RTP system identifier in the RTP system

Financial instrument binding

Establish a binding between the device, RTP system identifier, and a bank account



Payment

The payment initiation request comes from a trusted device. An additional factor can be triggered as necessary.

Trust delegation

Trust is a key component of any financial ecosystem when it comes to payments. Trust today is mainly between users and their **financial institutions (FI)**. FIs don't expand this trust to other parties even though the user might have already trusted them in some form. For example, a Third Party may have verified a user's digital/real-world identity, but a FI usually reverifies it.

By delegating trust to the Third Party as an identity provider and leveraging concepts like trusted devices, the user experience can be improved significantly without compromising the security of the payments. FIs make use of attestations Third Parties can provide about the user's digital and/or real-world identity. Liability for these situations can be negotiated between the FI and the Third Party — both parties may be willing to compromise for a simpler, more secure user experience.

When it comes to getting access to financial information based on the digital and real- world identity, it is essential to prevent social engineering and maintain trust. Having strong ties between multiple elements of identity (e.g., having a device, phone number, email are all verified together) and a way to securely delegate trust between devices represents a key strength of an RTP system solution.

As each financial institution in the RTP system will have checks on fraud, we should be able to use the correct identifiers to make a risk-based decision at transaction time while avoiding having to unnecessarily send sensitive data across the RTP system.

We are a strong proponent of a model where trust delegation is a key pillar of the RTP system solution. It makes the whole ecosystem more robust, as FIs can leverage other party's strengths without having to implement an entire suite of security, privacy, and compliance solutions. FIs can put trust in the Third Parties to run risk checks and trigger second factor authentication only where needed. By using delegation and a Third Party risk engine, an RTP system can achieve better protection for the FIs and minimize the amount of data shared, while speeding up implementation and rollout.

> No fraud detection system based on data from a single system participant can come close to the effectiveness of one that uses data from all participants. [31]
>
> **Level One Project**

Including Third Parties in the ecosystem can help better map out the key areas of authentication, identity, and trust and create an RTP system that's more stable, efficient, secure, and easy to use for all groups.

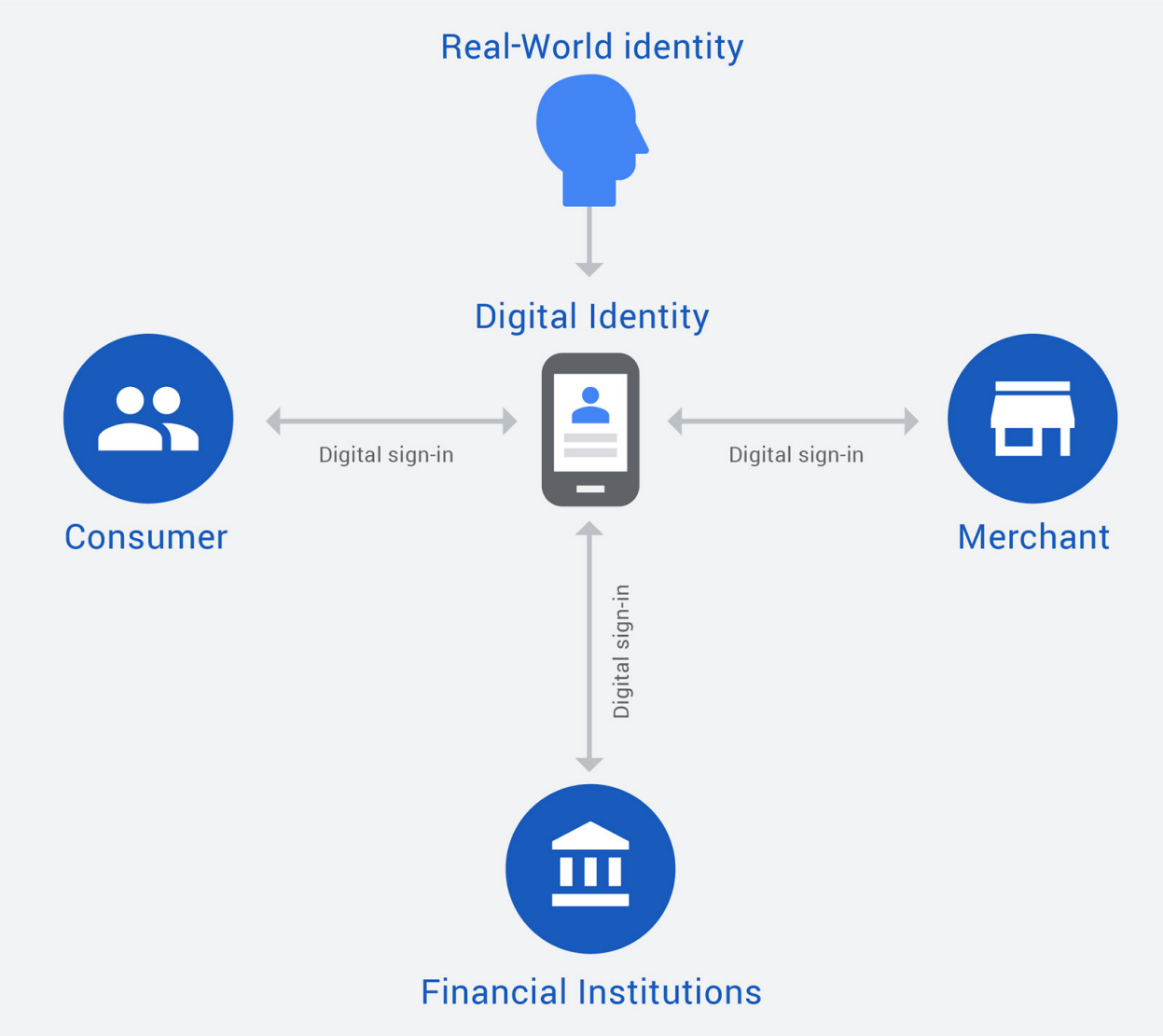
Matching digital identities to real-world identities

A digital identity and a real-world identity are complementary and together form a key set of attributes that identity providers can relay to interested parties, with the user's consent. Having users logged in to their digital account enables them to have their entire identity carried with them and gives them access to their payment instruments and valuables. Digital identity has become more and more used, for example when financial institutions and merchants allow access to their accounts using a Google or Facebook sign-in.

In an RTP system, to confirm that an attribute of a real-world identity (often used by FIs) matches a digital identity (used by a Third Party app), attestations can be used — claims that can be cryptographically verified. The attestations go along with each attribute of the identity (e.g., verified phone number and separately verified email) or together for a set of attributes of the identity (e.g., device, phone number, and email address all verified together).

31 - https://leveloneproject.org/the-guide/payment-systems-lessons-learned-and-highlights/

Real-world identity is primarily used when opening accounts with financial institutions for the purpose of regulations, such as KYC and AML. Each financial institution is trusted by the central authorities with the KYC and AML processes, and with the fact that it requires certain information about the user's real-world identity (e.g., name, address) and specific attestations (e.g., national ID, driver's license) along with it. By analogy, technology companies have built the capability to verify individuals' and organizations' real-world identities. Technology companies often employ mechanisms that prevent the same real-world identity from being used across multiple digital identities.



Federated identity

Federated identity is a forward-looking model of identity that unlocks value for the user, merchants, financial institutions, and Third Parties. If the user uses the same digital identity across many surfaces, they can carry their verified physical identity without having to reverify on every new surface. Through this, Third Parties can bridge the gap between the digital and real-world identity by bringing them together and enabling a secure and seamless user experience for commerce, both on- and offline.

For example, a Third Party could verify a key identity element, such as a national ID or form of payment, when the user logs in with an email address. If the user uses that email address to sign in to a merchant or financial institution, their verified national identity or form of payment could be ported over. Thus, the merchant or financial institution would not need to reverify the national identity or form of payment.

The importance of privacy

Privacy is a top concern for the ecosystem. Third Parties should give users full transparency and control over which data is stored, used, and shared within the system. Similarly, Third Parties should leverage the most advanced technologies in security to protect user identity and information. For example, Google uses the industry's leading phishing-resistant two-factor authentication Titan devices that implement FIDO standards. Second-factor authentication using a FIDO authenticator represents an innovative solution that addresses regulatory requirements while also delivering a seamless user experience.

Conclusion

As more and more countries embrace RTP systems, we hope this paper can serve as a useful reference when considering how to best develop a system. RTP systems are no small undertaking, but when designed well can generate important benefits for governments, financial institutions, merchants, consumers, and Third Parties. Each group plays a vital role in enabling financial services to embrace and support the broader transition into the digital economy. We look forward to working with all of them to make money simple in more countries around the world.

Annex

Google

Annex

What are QR codes?

QR codes are similar in concept to bar codes — they contain coded data that conveys information when scanned. But in this case, the code is made up of black squares arranged in a square grid on a white background. They can store a hundred times more information than a barcode, and the scanning device is a smartphone.

QR codes are especially useful in their ability to store numeric, alphanumeric, byte/binary, and kanji (Chinese characters used in a Japanese writing system) very efficiently, making it easy for anyone with a smartphone to quickly access the information, which is typically a locator, identifier, or tracker that points to a website or application.

QR codes can be a very useful tool in scaling digital payments, as they can be used to initiate payments across a range of mediums, from social media to local vendors. RTP systems should consider supporting Confirmation of Payee and using dynamic QR codes to reduce risk.

Strong customer authentication

2 factors from 3 categories

Knowledge

Something the customer knows

(e.g., password or security question)

- Password / PIN
- National ID
- Debit card number
- GAIA
- Address

Possession

Something the customer has

(e.g., phone or hardware token)

- Phone number
- Device

Inherence

Something the customer is

(e.g., fingerprint or face ID)

- Biometrics
- Liveness check
- Behavioral biometrics (e.g., location)

Strong customer authentication is needed to get meaningful consent from the user for authentication and authorization for a Third Party to link to a financial institution. The user needs to verify two of three factors — in different categories.

- Required for secure payments
- Required to meet regulatory mandates, such as PSD2
- Enables fraud mitigation based on risk assessment
- Enables new use cases for account linking, transaction data (e.g., open banking, access to RTPs systems)
- Current ways to link financial institution are not user-friendly

The EU's **Second Payments Services Directive**, known as **PSD2**, began to be enforced in September 2019. It creates opportunities for new payments services and also establishes rules for strong customer authentication on existing payment methods in Europe.

The regulatory goals of PSD2 are to:

- Facilitate innovation, competition & efficiency
- Give consumers more and better choice in the EU retail payment market
- Introduce higher security standards for online payments

New Payment types such as IDeal in the Netherlands and Trustly in Sweden establish a payment link between the payer and the online merchant via the payer's online banking module.