The future of RTP systems: The case for 3P payment initiation

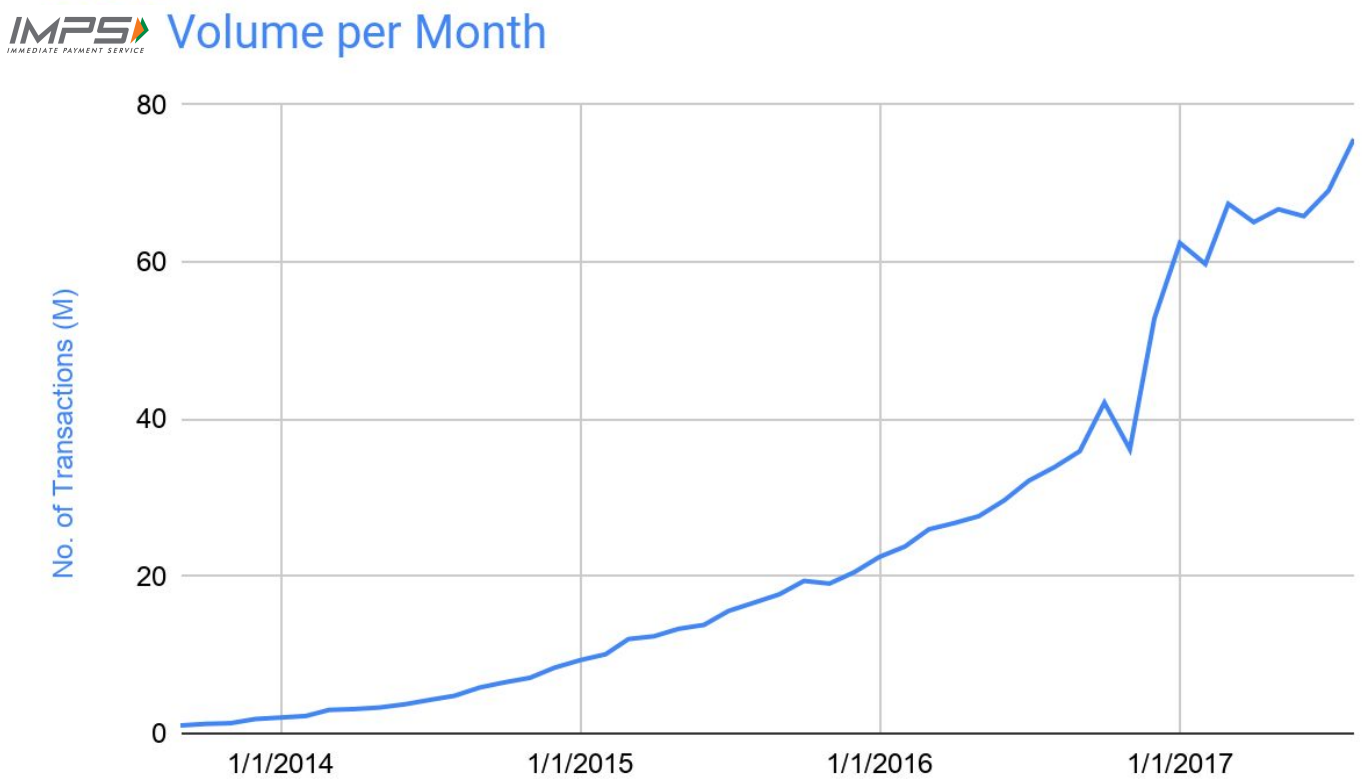
Mojaloop Phase Four Conference

January 2020

How many of you have heard of ?

India’s RTP system, launched Nov 2010
High banked population
Government support to digitize
Support for pay to phone number

Modest Growth



Source: National Payments Corporation of India (NPCI)

How many of you have heard of ?

API layer for third parties to initiate payments over the RTP system
Launched Aug 2016

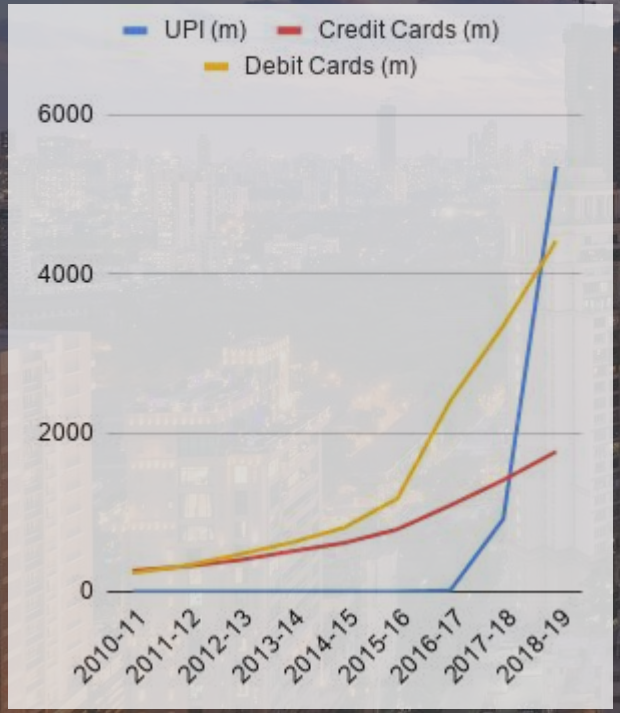
UPI's explosive growth

Source: National Payments Corporation of India (NPCI)

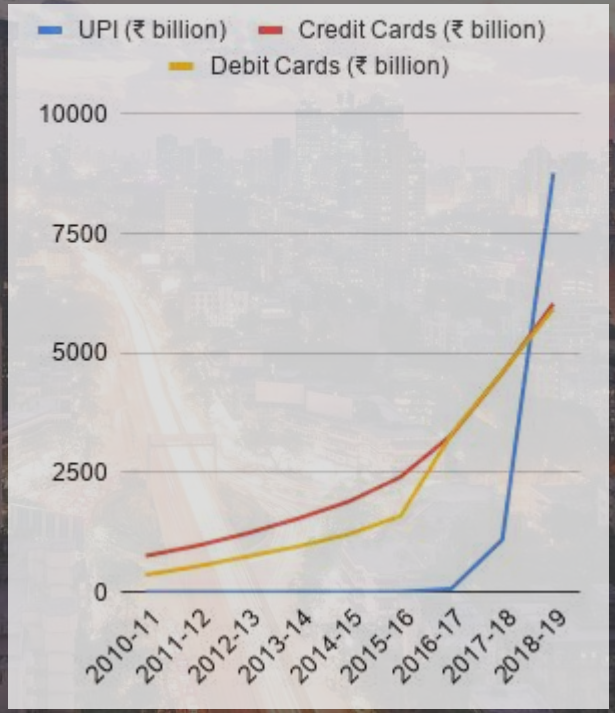
Digital payments volume now ~10% of GDP

UPI, Credit Cards, Debit Card Growth

Volume



Value



Google

Source: Reserve Bank of India Annual Report, Aug 29, 2019

Google Pay in India

67M

2019 monthly active users

$110B

2019 transaction value annualised

Data as of Sept 2019

3P access is not new...

[EU] Regulations enabling open APIs can drive innovation

Infrastructure foundations & open regulations allowed ecosystem growth

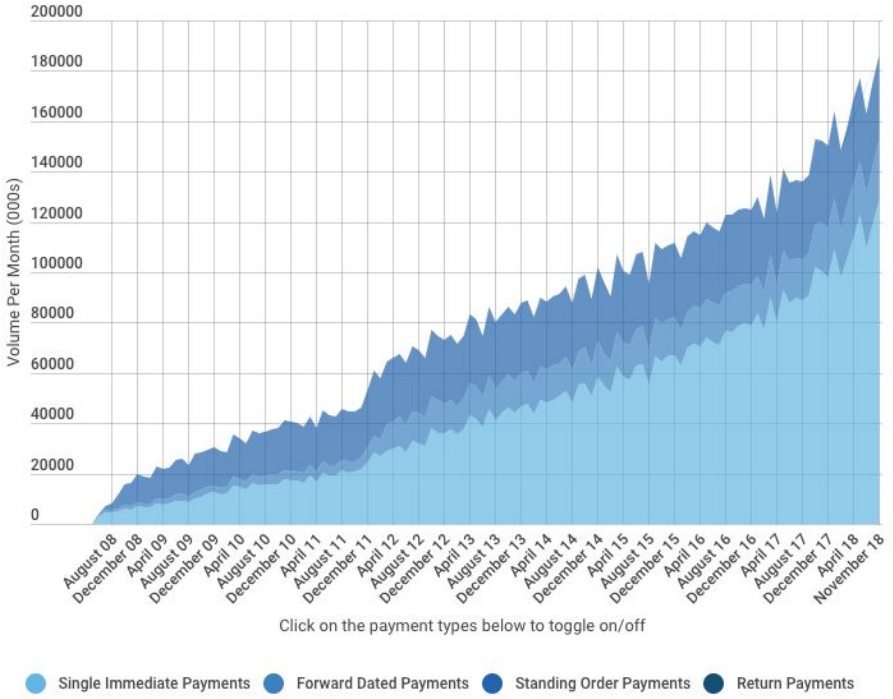
UK FPS transactions grew **18x to 180M per month in 10 yrs**

Development of instant payments systems

- UK: Faster Payments System
- EU: SEPA instant credit transfer (in all countries by 2020)

Open banking under PSD2 regulation

- Banks must open APIs so technology players can
  - initiate payments
  - get account information



How is open banking doing in Europe?

The UK has not “seen the hockey stick of growth in disruptive new players everybody was predicting. Everybody was expecting PSD2 to happen and all these companies would be fighting with each other to provide services to customers.” (source)

PISPs: 5, AISPs: 40+

Open banking: why the revolution is behind schedule

Written by FinTech Futures 2nd May 2019

Money 20/20 Europe 2019: Is Open Banking a complete fiasco?

04 June 2019 6 8 0

Europe begins Open Banking era in subdued style

Learnings from Europe

+ Single license for a tech player → use APIs of any bank
+ Tech player → initiate payments and read account information
+ Free to end users

- Authentication only on bank surface breaks user experience.*
- 3Ps must individually integrate with each bank, even with standardized APIs (in the UK)

*According to the European Commission, the Euro Retail Payment Board, the CGAP and the FIDO Alliance

What about Southeast Asia?

Simple RTP through phone directories...

Coupled with removal of digital txn fee in ‘18, TH’s Promptpay txns **grew 26x to 166M per month in 9 yrs**

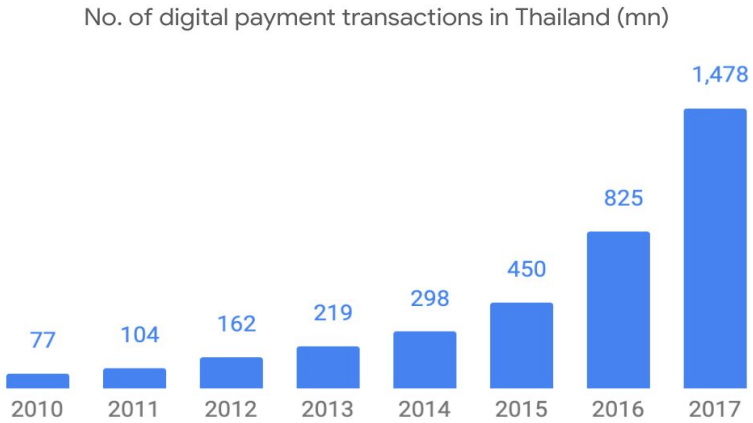
SEA markets built directories to map phone #s to bank accounts

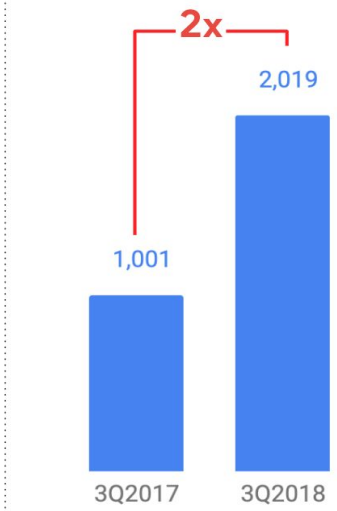
- Users can simply enter in a friend’s phone number to send a payment.
- In some cases, users can also pay to national ID or unique merchant identifier

PAY NOW *SG*

DuitNow *MY*

PromptPay *TH*





SEA's approach: Simple RTP through phone directories

- Users use their bank apps to pay
- Because of varying user experiences, concentration is mostly in P2P transactions
- Users are still not using this payment method for merchant payments

Singapore

Malaysia

Thailand

Why was India so successful?

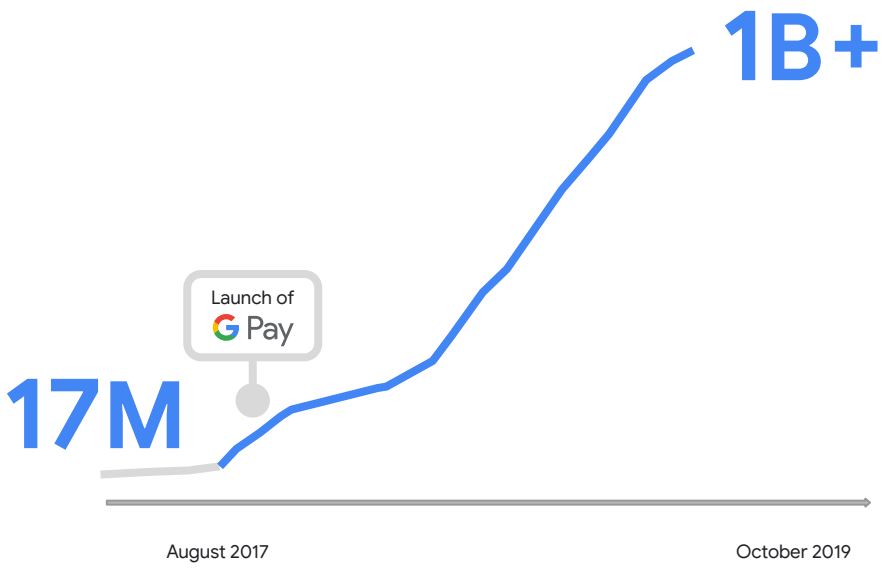
India leveraged 3P tech players to turbo charge growth

UPI transactions grew 67x to 1.15B per month in 2 yrs

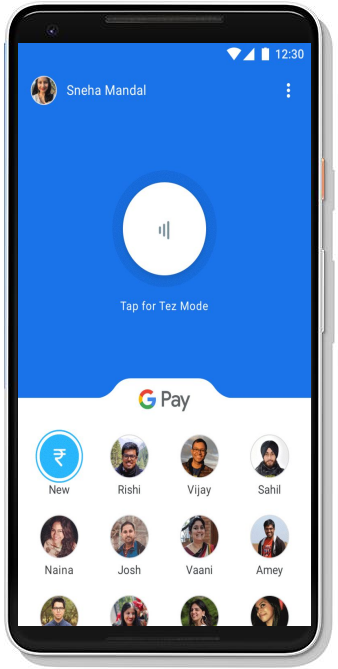
UPI made it easy for 3P tech players to initiate payments on the RTP system

Single API integration enabling tech players to move money for 140+ banks

Authentication on tech player's surface allows for better user experience and drives adoption



3Ps can build unique user experiences and use cases



G Pay India

Conversational UI

Built on UPI

Partner with Banks

All Things Money

Power Businesses, Large and Small - Spot Platform

Hot off the press...

We have collated our recommendations

Our technical recommendations for RTP Networks

- Authentication and adequate trust delegation important to find balance between safety and convenience for adoption
- Third party access: Standardized APIs the best way to provide access to both FIs and third parties
- National addressing database: Identifiers that are (i) Easy to remember, (ii) Easy to share without risk, (iii) Interoperable (e.g., email addresses, phone numbers)
- Tiered KYC: Build tiered levels of KYC/ AML for consumers and smaller merchants; upgrade KYC with scale
- Conveyance mechanisms: Build ecosystem for multiple ways of transacting, including QR Codes & NFC

What problems are we trying to solve in Mojaloop?

3rd Party Payment Initiation

The proposal contains the list of concrete modifications to Mojaloop API and the Switch architecture for adding support for non-ledger holding participants, PISPs, to the RTP network. The 3rd party payment initiation flow is similar to “request-to-play” flows which ML already supports.

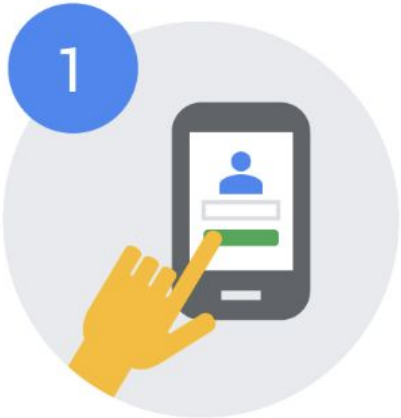
Account registry which enables conveyance mechanisms

Add ability to hide the sensitive financial accounts details (i.e. PAN) from PISP and its users. This is driven by explicit account registration step in which “virtual” account numbers/handles are generated.

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 which previously could only be done from a financial institution app.

User Journeys

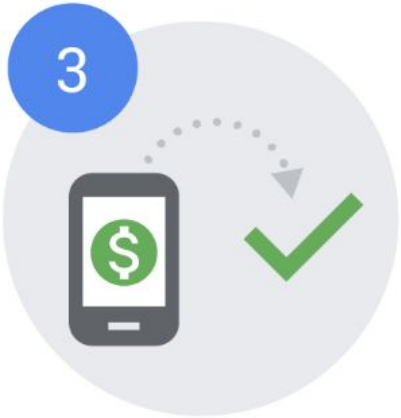


User registration

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

Bank account binding

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

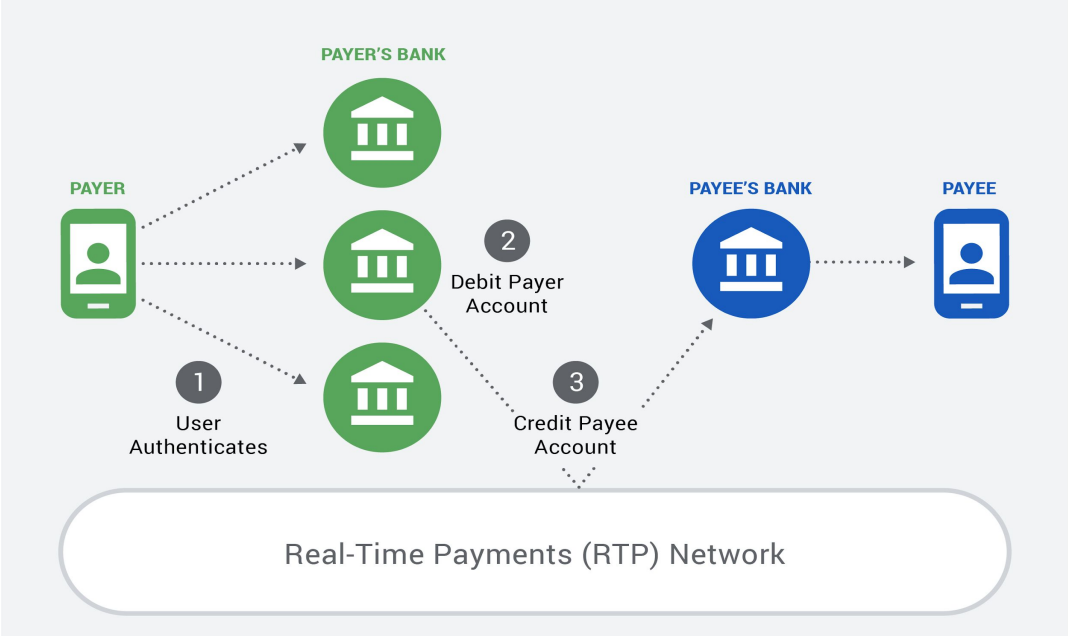


Payment

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

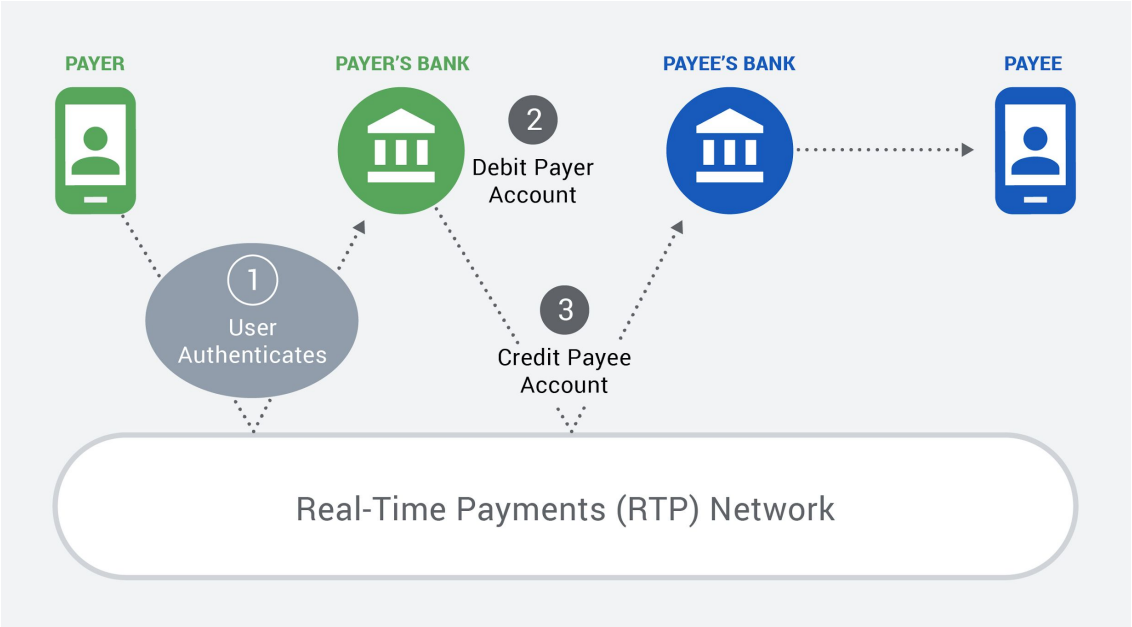
Third Party Support, Approach #1

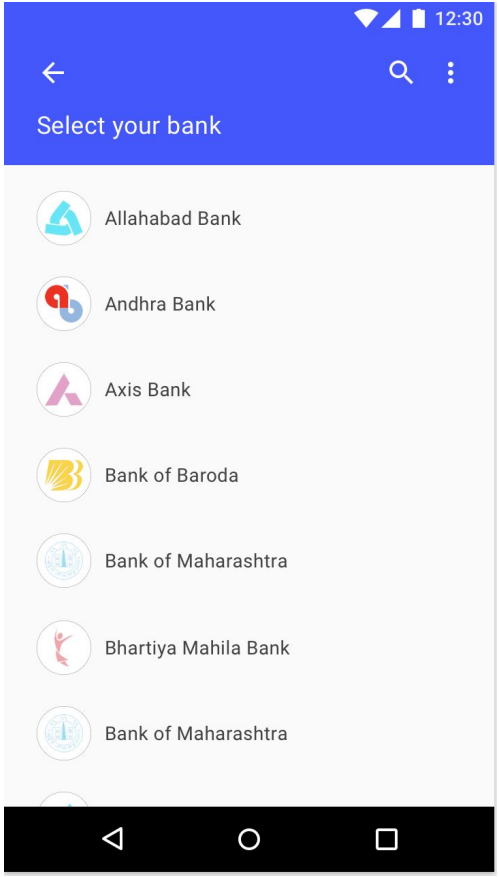
- Predefined standard
  - Mandating that all banks must comply
  - Lowers the friction, but Third Parties need to integrate with each bank
  - Example: UK with Open Banking

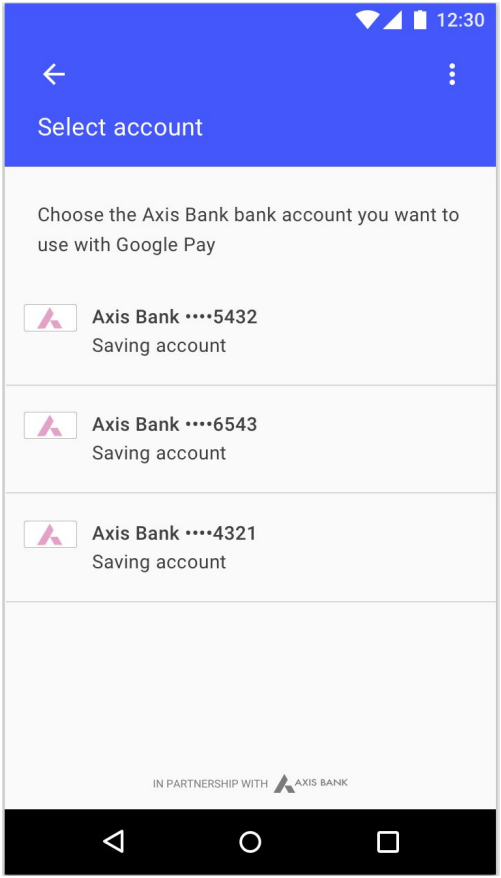


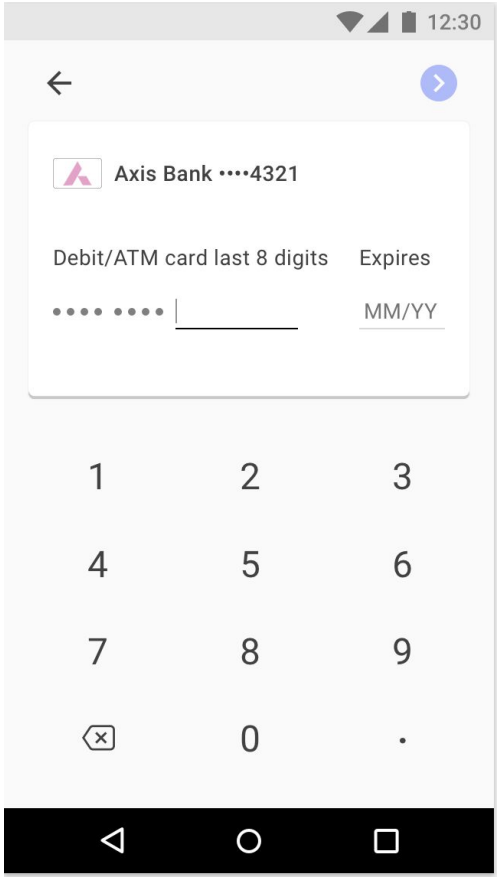
Third Party Support, Approach #2 (preferred)

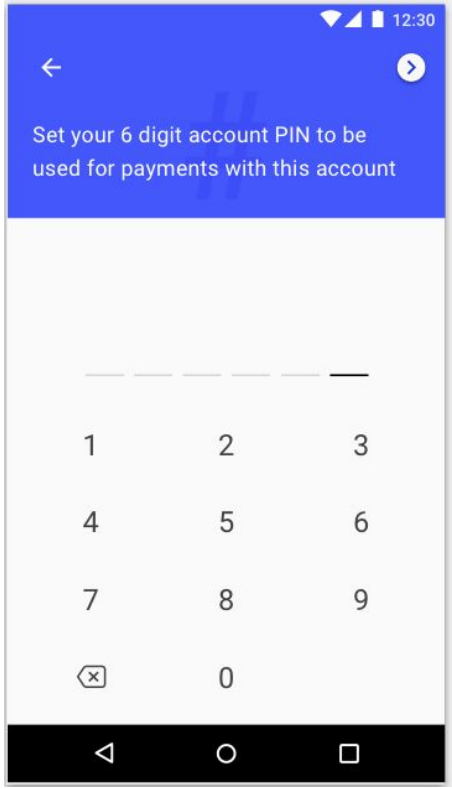
- Central API for Secure Client Authentication
  - Exposed directly from the RTP system (or via its partner service)
  - One integration point for all 3Ps, works with all financial institutions
  - Example: UPI in India

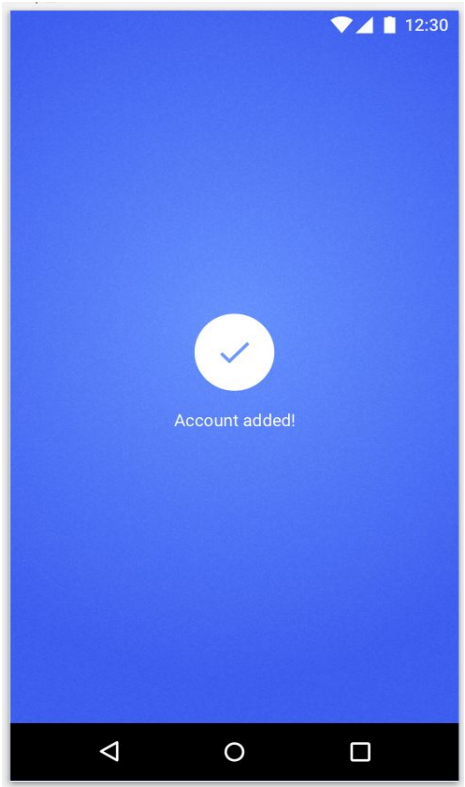




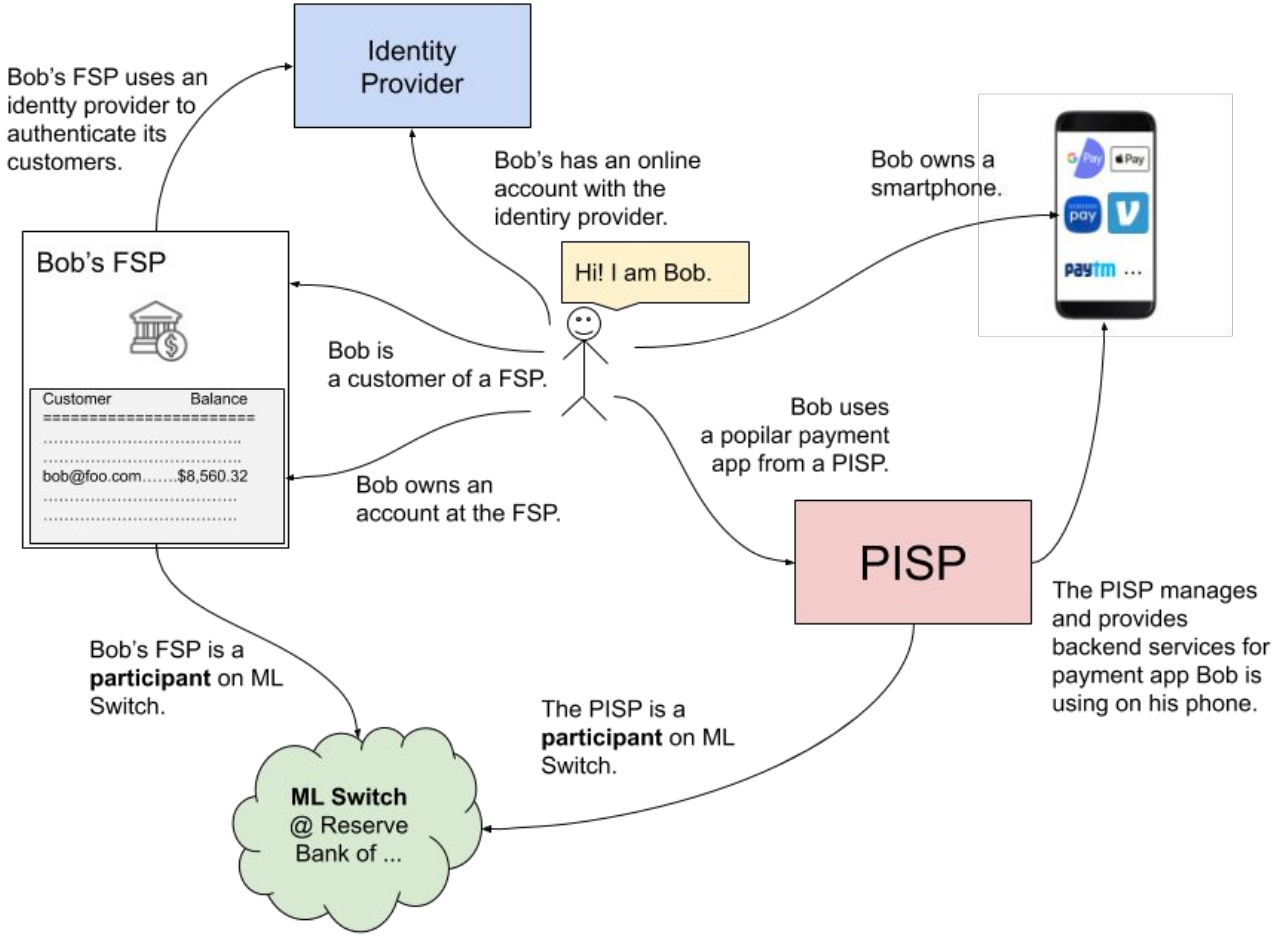




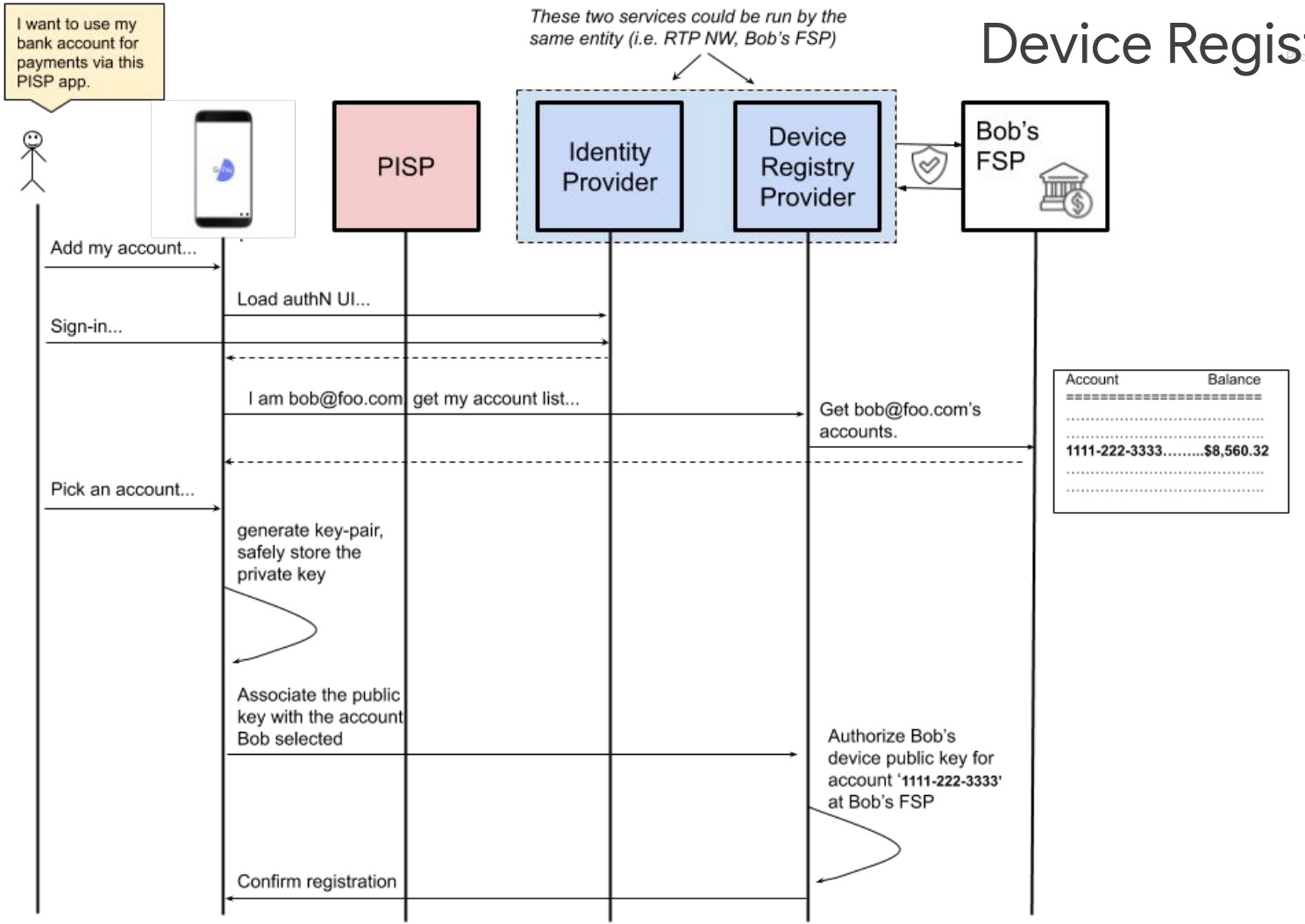




Mojaloop & Other Entities



Device Registration



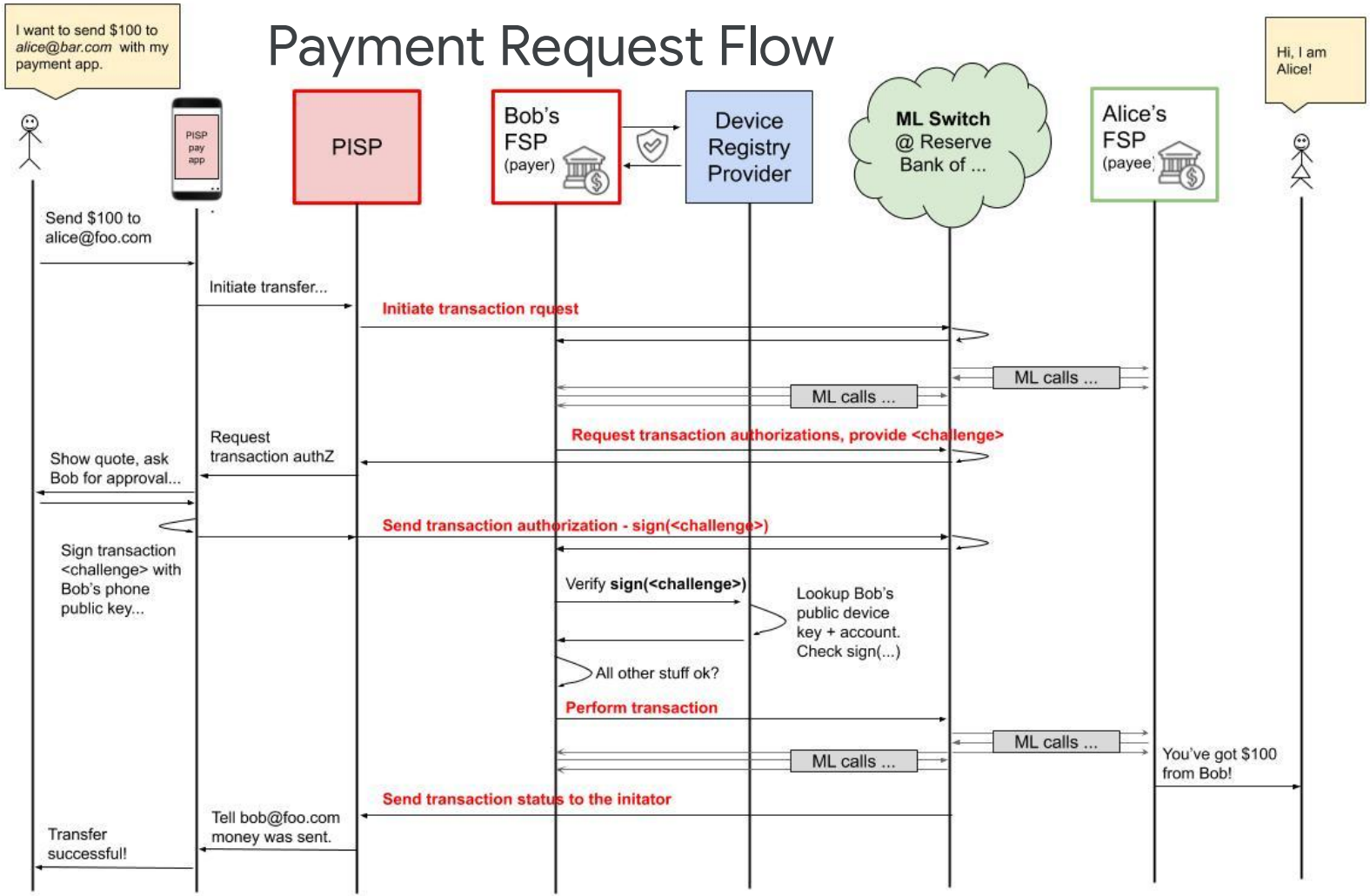
Device Registry Provider

- Stores **end-user device registration records**, which contain
  - Public key part of the **account/device binding** key-pair,
  - **Identifier of financial account** held at an FSP,
  - **Conveyable (maybe even human-readable) party+account identifiers** (i.e. *alice.smith@gpay*),

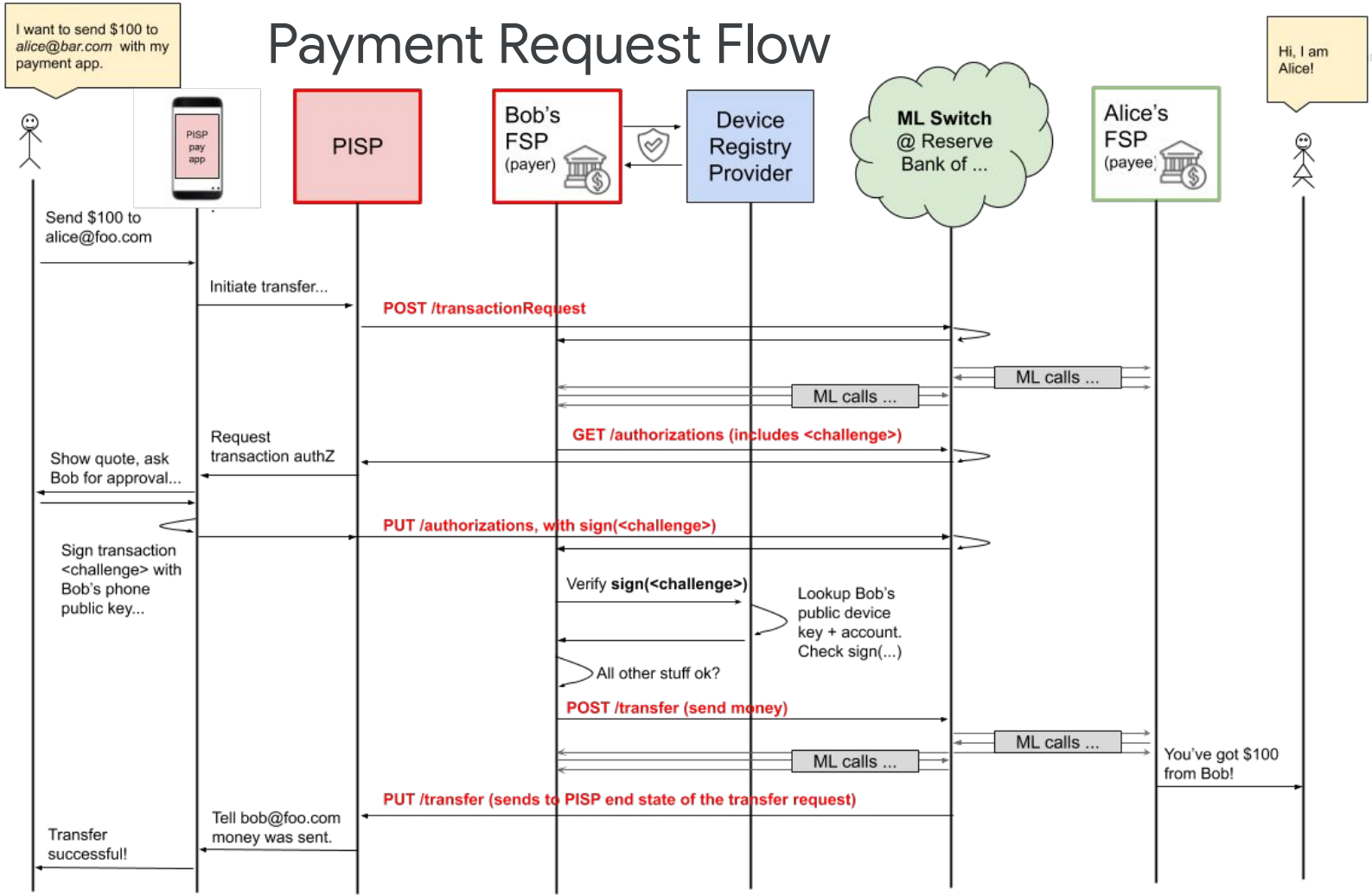
- Provides following services to the RTP network:
  - Assists ALS in **party/account resolution**,
  - Allows FSP to **verify transaction authorizations**.

- Who operates such service?
  - Ideally, the operator of the ML Switch runs DRP (there could be “decentralized” design where each FSP runs its own).

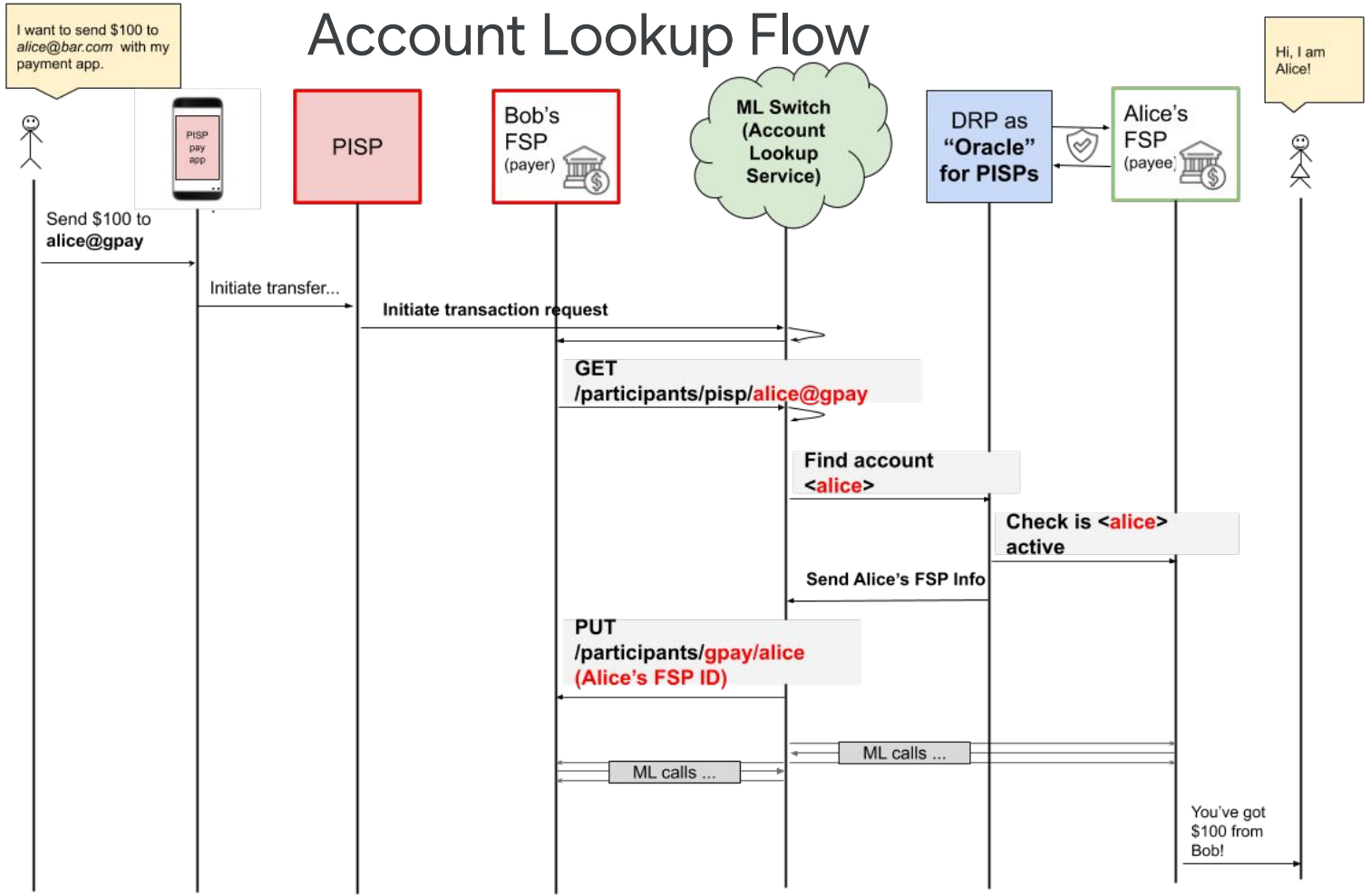
Payment Request Flow



Payment Request Flow



Account Lookup Flow



Multifactor Transaction Authorization

- This PISP model supports various authentication factors:
  - **Possession**: The private key part of the device<->account binding key-pair which is securely stored on the phone.
    - Fallback: if the phone's key store is not HW-backed, (in FIDO, U2F authenticator attestation key is missing), then require additional OTP over SMS.
  - **Inherent**: FIDO mandated biometrics (face unlock, fingerprint).
    - Fallback: on cheaper phones without biometric HW capabilities, Android falls back to lock screen (PIN/swipe - basically a **knowledge** factor).
- FIDO in Android and AndroidGo phones from N+

Transaction Authorization, with even more factors...

- On top of U2F, authorization could be augmented to include additional factors such as:
  - **Knowledge**: If amount > X, additionally require user to provide their **PIN** (which will be added to
  - Geo **Location**: Include long+lat in authorization reply.
    - Require FSPs to trust the PISP to verify non-rooted state of the user device (Android has a remote attestation service which FSP could use for that).

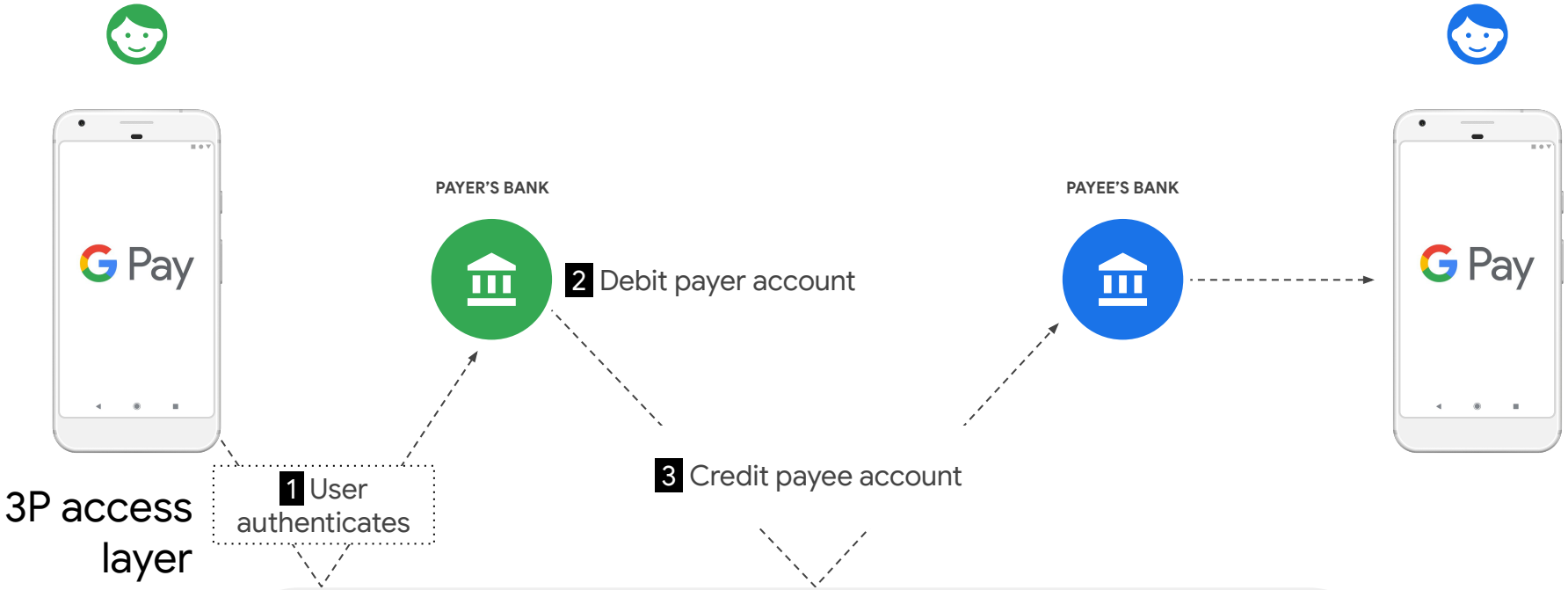
Quick Summary of Mojaloop Changes

1) Device<->account binding process is driven by a new type of service - Device Registry Provider (DRP),
2) DRP provides account resolution services to ALS, maps registered device<->account identifiers to the actual FSP accounts,
3) There is a new type of *participants* - PISPs,
4) PISPs can initiate a transaction requests, which is verified by
5) New multi-factor transaction authorization ideally based on U2F (FIDO),
6) The FSPs rely on the DRP for authorization verification.

3PPI proposal can be found at:

http://bit.ly/mojaloop-pisp


Tez accepted
Spend ₹100 here using Tez and get a scratch card worth up to ₹100! *



Coming soon: Mexico

Mexico followed the Southeast Asia model

CODI QR system

What's next for Mexico?

Google is deeply engaged with the Central Bank of Mexico

Google has been collaborating on

- Securely opening instant payments system to third party apps
- How end users can securely authenticate on a third party app
- How third parties can securely send instructions to the payment system
- How to design the best user experience

Banxico is designing something like India's UPI, but with added security, including recommendations provided by Google.

Google's Technical Recommendations

- Allow refunds: Refunds important alongside user-to-merchant purchases, in accordance with individual merchants' policies and without user interaction; require unique identifier linked to original transaction
- Clear & traceable merchant settlement: Transfer information related to taxes, fees & transaction identifiers
- Conveyance mechanisms: Build ecosystem for multiple ways of transacting, including QR Codes & NFC
- Tiered KYC: Build tiered levels of KYC/ AML for consumers and smaller merchants; upgrade KYC with scale
- Deterministic status of transactions: Ensure each transaction reaches terminal state (Success or Failure in real time.)
- Idempotency: Incorporate idempotency ID for each transaction so same transaction is not executed twice when networks are unstable and unreliable.

Google's Technical Recommendations

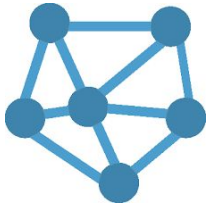
- National addressing database: Identifiers that are (i) Easy to remember, (ii) Easy to share without risk, (iii) Interoperable (e.g., email addresses, phone numbers)
- Authentication and adequate trust delegation important to find balance between safety and convenience
- Third party access: Standardized APIs the best way to provide access to both FIs and third parties
- Transactions: Start with real time Push with a plan to introduce pull (or request)
- Enable Mandates: Allow users to delegate permission to the merchant to pull money directly from their accounts. with restrictions (overall money exposure, time frequency, revocation)

User

Payment app

Auth app

Payment app server



Payments Network

Financial institution

- User uses the payment app to register themself, link their bank account and initiate payments
- Payment app invokes the auth app for capturing sensitive user credentials
- Auth app encrypts captured credentials & sends a signed encrypted request to the payment app
- Payment app propagates with a request to the network & financial institution

User Journeys

User Registration

- Network creates a profileID which associates device to phone number
- Trust established between auth app and network through exchange of device specific public key

Financial Institution (FI) Account registration

- Establish a binding between the device, the network profileID and FI account(s)

Payment Initiation

- Sends signed, encrypted payment request to FI
- FI can optionally challenge the user for yellow path