This document describes the process of connecting and validating users in proposed p2p e-cash transfer.

The scenario has two users with devices – device A which will send the money (will be called as consumer hereafter) and device B which is a merchant and will receive the money.

The app will require any user to sign up first using the government issued ID card such as aadhaar card. Once the sign up is done, app will connect to RBI server and download a key pair on the phone.

1. Merchant will start the app and enter the amount it wants to receive.
2. Once the amount and details are entered the app will create a barcode of the same. At the same time, app will start a hotspot.
3. The consumer will start the app and scan the barcode using the send button.
4. The barcode shall contain basic information such as some validation message, network name (hotspot) and network key.
5. Using the scanned information, the consumer’s app will connect directly to the hotspot started by merchants app. All the basic network validation will be done internally.
6. Once the two devices are connected, the main process of validation will start.
7. Both devices will exchange public key of each other.
8. Once done, both the devices will exchange basic data in form of encrypted packet. The packet shall contain data such as user info and some other validations related data if and as necessary. The packet will be encrypted with the respective users’ public key. For example, consumer will encrypt packet using merchants’ public key.
9. The merchant’s device will decrypt package received from consumer’s device using its private key and verify the data.
10. Once verification is done, the consumer shall send the money requested by merchant and will deduct it from app’s database pending upload to RBI server.
11. Once the transfer is done successfully, the hotspot will be shut down by app.