

December 08, 2010

The Chairman,
Telecom Regulatory Authority of India,
Mahanagar Doorsanchar Bhawan,
Jawahar Lal Nehru Marg,
New Delhi 110002

Sub: Consultation Paper on “Quality of Service requirements for delivery of basic financial services using mobile phones” (CP 13/ 2010)

Dear Sir,

We are pleased to present our views on the captioned Consultation Paper.

We hope our enclosed views would help in these efforts. We would be glad to share and explain our suggestions in person as well.

Thanking you,

Yours faithfully,

KAPIL DEV KUMAR
Authorised Signatory

INFOTEL BROADBAND SERVICES PVT LTD'S VIEWS ON CONSULTATION PAPER ON QUALITY OF SERVICE REQUIREMENTS FOR DELIVERY OF BASIC FINANCIAL SERVICES USING MOBILE PHONES (CP 13/ 2010)

Introduction:

The Government is continuously striving to achieve vision of empowering the poor and financial inclusion is one of the powerful tools to ensure such empowerment and will always be an integral part of agenda of inclusive growth and sustainable development. However it is equally important to ensure that such model should be replicable and viable across the country.

In recent times, the phenomenal growth of telecom penetration in urban as well as rural parts of the country has opened up great opportunity in bringing connectivity driven banking models to those people who have as yet no access to even basic financial services. Besides delivery of basic financial services to unbanked population, the telecom driven new delivery models will cut delay and reduce the direct and indirect costs and hardships incurred by the beneficiaries while ensuring authentication and traceability of such transactions.

In order to make this initiative successful and achieve wider customer acceptance, it is necessary that the service will be easy to use, secured, ubiquitous and cost efficient and should have following attributes

- a. **Security:** Network security protocols and interface standards should be as per prevalent industry standards so as to ensure security and integrity of transactions
- b. **Speed:** The transaction should be completed preferably instantaneous or within reasonable time period
- c. **Reliability:** There should be minimum instances of transaction failures
- d. **Traceability:** sound audit trails should be available for all transactions
- e. **Consumer Protection:** There should be a safeguarded consumer information, minimum instances of fraud and efficient consumer grievances redressal mechanism

In addition, for faster growth and reach of these services, the policy makers also need to address following policy issues

- a. With the advanced technologies like 3G and BWA expected to come soon, there will be a larger window to innovate service delivery with better performance parameters. Taking these technological advances into consideration, the model or framework that is being proposed for implementation should be flexible enough to accommodate other means of access as and when requisite technologies evolve.
- b. The model that is being proposed is bank centric model wherein telecom operators have a role of simple carrier. While this can be a first step towards an important goal of financial inclusion, the policy makers should also be open to explore alternate non bank model or operator centric model. The success of the M-PESA model adopted by Kenya can be a good example in this regard. Such success stories emphasize the fact that with appropriate regulatory mechanism in place, operator centric model can not only be as safe as bank centric model but also enable greater proliferation of banking services into under-banked and non-banked areas and can have greater contribution towards the financial inclusion process.
- c. In order to establish certainty in the market and achieve quicker rollout of services, there can be a guiding framework for entering into partnership across the value chain. For example, there can be a reference agreement for arrangement between banks and Telecom service provider recommending provisions for technical and commercial collaboration. It should be noted that a fair revenue share model for all stakeholders shall make this initiative sustainable and attractive for all players.

- d. Considering focus on the currently unbanked population, it is important to make available content in vernacular/local languages as well which will surely attract non-English speaking users thus increasing the number of m-Commerce users.
- e. It should be ensured that other ongoing initiatives in this direction also get integrated with the planned measures towards financial inclusion framework so as to have standardized processes and protocols with inter-operability features. For example Union Bank of India's proposed mobile payment service in partnership with Obopay, Interbank Mobile Payment Service (IMPS) launched by National Payment Corporation of India, provision of Broadband Enabled Rural Public Service Terminals (RPST) under USO fund for providing Banking Services etc.

All of above measures will help to build trust and wider acceptance amongst customers – an important factor for overall success of the scheme.

Issues for consultation

2.1 What method(s) of communication on mobile network (GSM and CDMA) would be suitable for enabling financial transactions using mobile phones? Please explain your answer

Response:

A network operator will need to implement 4 key requirements to offer a secure, reliable, payments transaction platform:

- Ensure **sophisticated data coverage** as financial transactions need extremely low latency requirements
- Provide **adequate security measures** (PIN based, etc)
- Provide **adequate bandwidth** (however given the micro payment nature of such transactions, it may not be a major challenge)
- **Meet interoperability standards** (e.g., open wallet transmission between two different network providers linked to two different banks)

As for networks, the solution should be network agnostic as GSM, CDMA and BWA technologies can support secure data transmission.

We propose use of following protocols for transaction support:

- a. **IVR:** IVR can be used for a basic 'identity authentication' by the entering of a 'PIN' (effectively, the combination of the phone from which you call, and the 'PIN' that you 'know' establishes reasonable identity) – and therefore, could be used in some scenarios where identity is essential
- b. **SMS:** SMS may be the least preferred technology due to security issues on payments transaction data exchange. As SMSs are prone to spoofing, it is recommended that SMS should not be used for the purpose of identity authentication unless it is supported with an additional mechanism which guarantees that only device has been used for sending the SMS (and not a machine). The SMSC receives SMS from both a mobile device as well as other servers – some of whom can spoof the sender's mobile number. It is imperative that, when the SMSC connects a message to the SMS Gateway, it clearly identifies which SMS came from a 'device' and which came from 'non-device' sources. If this can be achieved encryption of message might not be necessary.
- c. **IP / HTTP:** will be available only on higher end phones, or data devices. Any bio-metric data transfer, whenever implemented, should happen only using IP/HTTP, and using the standard Aadhaar encryption protocol.

d. **SIM Toolkit application:** As the user interface / menu is resident in the SIM, this will be faster and easier to transact providing end-to-end security.

Using security, cost and user friendliness as core parameters and experience in several emerging markets, STK appears to be the most feasible technology. However, the solution should be flexible enough to run on multiple technologies given the 2G/3G/4G trends.

It is also submitted that the above only specifies the ‘communication protocol’, and does not define/limit the ‘user experience’. For example, one could create a User Interface to interact with the customer on the phone, and finally send an SMS to actually do the transaction. Thus the Authority should only specify the communication protocol but not the User Interface norms.

2.2 What in your view would be appropriate time frames for delivery of messages and responses with respect to the method(s) suggested by you? What parameters need to be defined to ensure timely delivery of information to support financial transactions using mobile?

Response:

Telecom Operators’ operating mobile banking/payments ecosystems in emerging markets are able to process transactions in ~10 seconds (close to average time required for a credit card transaction). The aim would be to match the current transmission standards for a credit card transaction. Telcos, however, will need to ensure to provide low latency networks to provide a frictionless experience

2.3 In the method suggested by you would it be possible to prioritize the transaction messages over other messages on the network? If yes what would be the cost implications? Please also reply this with reference to SMS as means for financial transactions.

Response:

In order to establish some form of guaranteed QoS, the various options can be:

- Allocate different channels (BTS) for mobile payment transactions. However, this method is expensive and will require upfront investments.
- Set up virtual priority based data traffic systems which are able to distinguish between a normal and mobile payment transaction. This method will require limited investments into programming, etc and is likely to be the more feasible option.
- In case of SMS, the Authority can provision for a dedicated national short-code, which the MSC can then route to a specific SMSC. Under this scheme, a dedicated SMSC for financial transactions can be explored, which will not suffer from any queuing problem and therefore can give an almost instantaneous QoS.

In the event, the cost for most optimal solution implementation is envisaged on the higher side, the Government can also explore USO fund support for the upfront investment and associated operating costs.

2.4 What do you think would be the security requirement using the method proposed by you for the five basic transactions i.e. no-frills account opening, cash in, cash out, checking balance, and money transfer?

Response:

For undertaking basic financial transactions, normal standard security systems (PIN based encryption) appear to be the most feasible option. All routing of messages to the scheme providers' servers must be with the highest level of security with dedicated connectivity like leased lines (E1links) / VPNs.

Following illustrative steps can ensure end-to-end security:

- Mobile Financial Services can be hosted and installed on SIM card, which can make fraud impossible without SIM card
- PIN number will always be required before m-payment
- PIN does not travel in plain text during the transaction
- Telecom Service provider can also provide OTP (One Time Passwords) to be used as the second factor authentication
- Immediate fraud detection embedded in m-transactions thanks to notification SMS to initiator and to destination

In addition, buying some standard software which could provide anti-fraud systems embedded in the mobile banking application could be evaluated.

It is worthwhile to note that mobile based financial transactions can have better transaction security than card based e-commerce transactions for following reasons

- Unlike e-commerce transactions which are device independent (without check of physical possession of card), Mobile financial services will always be device / SIM dependent
- PIN number is always required before m-payment as compared to signature in case of card transactions which is easily forgeable
- With respect to transaction notification, immediate fraud detection embedded in m-transactions on account of notification SMS to initiator and to destination as against in card payment the fraudulent card usage often gets undetected unless transaction notification service via is activated.

Thus m-transactions offer enhanced security proposition on account of combined physical and virtual authentication, comparable transmission security as for credit cards and embedded anti-fraud alert system.

2.5 What would be measurable QoS parameters for such networks? Please specify both network and customer centric parameters.

Response:

Following QoS parameters may be measured for such networks:

- Call set up success rate should be 98-99% i.e. providing business continuity and disaster recovery plans to ensure services are always available at all times
- Set up a long term goal to achieve 99.99% system/network availability and ensure all signed on participating institutions follow the same rule
- Ensure low congestions (identify peak time cycles and fully utilised base stations)
- Maintain details of transaction records consummated within mobile payment system for a duration as mandated by banking regulations

2.6 Please list any other issue that you think is important and your comment thereon to finalise QoS parameters for facilitating financial transactions on mobile network?

Response:

As stated earlier, the proposed solution should be flexible enough to run on multiple technologies given the 2G/3G/4G trends. Data driven devices (hand-held devices, computers accessing bandwidth) should also be included in addition to mobile phones to provide basic mobile banking services as proposed.

It could be worth considering to allowing closed ecosystems to operate initially to ensure the service reach critical mass of merchant and customer adoption.

Before finalising requirements and blueprinting, the industry could invest resources (potentially with help from government and regulators) to prototype in select geographies and implement learnings from such pilot phase into the nationwide roll-out.