

Response to Consultation Paper On Quality of Service requirements for delivery of basic financial services using mobile phones released by the Telecom Regulatory Authority of India (TRAI) dated 28th October 2010.

ISSUES FOR CONSULTATION

Preamble

Communications networks fundamentally provide on-line, real-time access to financial (and other) systems. It is our considered view that the purpose of this consultation paper exercise must not be to determine whether any one bearer technology is superior and mandate it for use by all financial institutions or solution providers using mobile communications access networks as technology enablers for financial transactions.

Solutions for enabling financial transactions ought to ideally be evolved as shown below:

Problem statement	Response
Consumers desire the ability to carry out financial transactions outside of bank branches and independent of timings	Provide access to banking systems from external sources using appropriately convenient means
Different financial transactions need varying levels of security based on the perceived RISK for that transaction both by the financial institution as well as the Consumer	Provide a means of securing the transaction such that the RISK is eliminated or minimized to an extent acceptable to the financial institution as well as the Consumer
Consumers need the ability to exercise their choice with respect to financial institutions, communications networks, communications devices as well as MODE of communication – such as voice, messaging, data.	Provide a multitude of solutions that allow Consumers the ability to conduct the transaction on the basis of their preferences

The intent must be to forge a sustainable and vibrant ecosystem that allows for innovation and encourages ideas and solutions from the widest number of participants by lowering the entry barrier.

It is desired that the Telecom Regulatory Authority enables the creation of open, fair transparent and democratized access to telecommunications infrastructure. At the same time, it is also important that the solution providers come up with appropriate solutions creatively, without imposing unreasonable demands for quality of service or encryption of financial transactions upon telecom operators. This will only serve to escalate costs for telecommunications providers, which they will logically have to pass on,

creating an upward spiral of costs. A good example to consider is the case of customers using internet banking using internet service providers. When users access the internet to conduct financial transactions, their ISPs are not held responsible for guaranteeing bandwidth or encryption techniques used. The onus of ensuring that a financial transaction is secure or dealing with the failure of access connectivity in the course of a given transaction rests with the institution providing services and the customer availing them. This principle must be extended to financial transactions using mobile telecommunications networks and devices.

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.

As detailed in Chapter II of the consultation paper, a number of different and valid choices are available as well as suited to enable financial transactions using mobile phones. These include

- a. voice
- b. messaging (SMS / USSD) and
- c. data (WAP / IP)

It is possible to implement secure and viable means of financial transactions using each technology (or a combination) of bearer options such that transactions are adequately secure as well as electronic confirmations or physical receipts are delivered. It is critical to note that each of these options is purely a "**BEARER**" technology to enable financial transactions. The solutions at the end points i.e. transaction origination and processing can have the entire intelligence to secure, authenticate, authorize, and confirm transaction status. The requirement to mandate that the access medium must provide the encryption for every message exchanged across the entire ecosystem will only create a burden on the telecommunications provider that may be wholly unnecessary.

There are several existing voice based solutions that allow users to carry out financial transactions by providing credit card details to an IVR system that captures the information using DTMF digits (e.g. selection of an add-on package for an existing DTH subscriber). The user can be connected to such an IVR system after having called a Toll-free call center and the agent handholds the customer through the transaction. The provider then confirms the transaction through various options such as a voice confirmation from an agent, the next bill for that customer, an SMS confirmation and so on.

Similarly, there are solutions that use SMS / STK and USSD. At Eko India, we process in excess of 8,000 financial transactions every day varying between as little as Rs 100/- and as much as Rs 10,000/- using USSD technology for carrying transaction information, a patented security mechanism and USSD responses as well as SMS messages for transaction confirmation. Contrary to what is mentioned in the consultation paper, notwithstanding limitations, USSD response messages can be presented in a desired format which when designed properly, are necessary and sufficient as notifications for financial transactions.

The larger challenge for solution providers today is that there is no simple or central mechanism to obtain uniform connectivity or access across all telecom operators to enable the seamless use of end-user applications.

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?

Ideally transaction status must be communicated instantly or as near instantly as possible (less than 30 seconds). Anecdotal / empirical data suggests that users are willing to wait as long as 5 minutes in some cases before attempting to approach an alternative source for transaction confirmation. Even so, the onus of providing such alternatives rests with the financial service provider (e.g. a telephonic customer care center). It is important to understand that a one-size-fits-all approach may not be the best solution in this instance.

For example, it will always be possible for a solution based on IVR to provide instant voice confirmation. Similarly USSD solutions always return an instant transaction status. The statement in section 2.18 of the consultation paper, “The messages sent over USSD are not defined by any standardization body, so each network operator can implement whatever it finds suitable for its customers” is misleading. (Section 2.19 goes on to provide references to GSM specifications for USSD). What is being referred to here is that the ***syntax*** has been left open. This is a wonderful thing for it allows application providers to program the back-end such that users may do all sorts of things from checking their prepaid account balance (nearly all operators), to ordering subscription services (e.g. Jokes from Vodafone or Missed Call Alerts from Airtel and so on – using a different “syntax” in each case), to debiting their no-frills bank account in the case of SBI / ICICI Bank no-frills account holders acquired by Eko. This is true even in the case of SMS which allows application providers to create varying syntax for all kinds of things from voting on reality shows to securing financial transactions.

With the advent of 3G, customers will be able to access full-fledged internet services for carrying out financial transactions from their phones. In this case, as in the case of WAP, the transaction confirmation is dependent more on the end point applications and near instant.

From a layman’s point of view, at this juncture, even the Quality of Service for voice calls or P2P SMS which is the predominant source of business for all telecommunications providers in India, is often less than satisfactory. As such imposing stringent QoS norms for specific types of transactions on various bearers may be an expedient demand. A benchmark of message delivery SLAs for SMS which is the only store and forward mechanism and therefore subject to delays could be set as follows:

Benchmark	Parameter / SLA
95% of SMS messages to be delivered*	in less than 30 seconds
99% of SMS messages to be delivered	in less than 2 minutes
99.9% of SMS messages to be delivered	in less than 5 minutes

*subject to the condition that user is in an area with GSM network coverage and has the phone switched on

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.

As mentioned in the response to the previous questions, the larger focus must be in ensuring open, fair and transparent access of telecommunications networks to solution service providers rather than mandating changes to bearer specifications of mobile network operators - which may be possible, but come at costs that would make the entire ecosystem untenable.

It is possible to allocate message throughput for specific applications at the SMSC. However, it may be overly onerous to determine which transactions are financial transactions and engineer applications, SMS gateways and SMSCs to prioritize them. Person to person messaging is by default accorded priority over person to application messaging. Thus, application providers often use a normal 10-digit mobile number to receive requests. However since a 10-digit number is tied to a particular licensed operator in a specific circle, all messages sent from outside that circle are treated as STD SMS and charged as such. Also, obtaining and operating a 5 digit SMS code across telecom operators is still a very complex, time consuming and expensive task. Currently telecom operators do provide (to their own customers)

- Toll free SMS short-codes
- Toll free 10-digit numbers
- Special rate 10-digit numbers

An analogy here is the 1800 / 1862 numbering system that allows for toll-free or special rated calling, but one that accommodates universal pricing across subscribers independent of their originating telecom circle.

For example, every telecom operator provides their subscribers various toll-free numbers – for customer care, for self-provisioning of services and so on. However, what will be required here is the ability to provide a toll-free or variably rated short-code or long code that remains the same across telecom operators and across circles such that a uniform pricing (of the message) may be advised by the financial service provider to their customers.

We would like to re-iterate that the telecommunications infrastructure must enable multiple options for end-users, end-devices and technologies to access applications that enable financial transactions. The mechanism of securing the transaction, the particular user interfaces, as well as transaction syntax or application protocols must be left to the solution providers to implement at the end-points.

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

The security requirements for financial transactions must respond to the RISK perception of the transaction by the transacting institution as well as the customer rather than to the medium of message exchange used.

The key parameters that determine transaction risk are:

- Type (financial, non-financial e.g. registration, PIN change)
- Value (or size)
- Audit trail (originator / recipient KYC)
- Repeatability (e.g. ECS payments)
- Frequency (unusually frequent transactions may be indicative of fraud)
- Repudiation (provider must be able to prove transaction authorization)

All solution providers must address these concerns. The concerns may be addressed using authentication / authorization data in various ways. Taking the example of a voice based transaction using a credit card: usually a provider will first authenticate the customer using data linking the customer to the service. Then for a financial transaction the customer is asked to provide (DTMF) information linked to the financial instrument which is further authenticated using data on the instrument. Finally the customer is asked to authorize the transaction using an input that signals confirmation. Some of these steps may be skipped in some cases – e.g. if the user uses a particular instrument regularly, there may be an option provided by the application to register that instrument and simply choose it rather than input all of the information repeatedly. However, all financial transactions require express authorization.

Similarly, in the case of STK / Mobile devices / WAP / Internet based transactions also, there is always an authentication step followed by authorization.

The tokens, references, methods or encryption that is used depends on the choice of medium, transaction risk and user convenience. This must remain as it is even for transactions using mobile phones and telecommunications infrastructure as a means.

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

Current QoS parameters used and monitored by the TRAI for normal use of the bearers such as Voice, SMS, USSD, WAP, GPRS should be valid for financial transactions too. The authority could consider allocation of a portion of the USO fund towards ensuring universal telecom access for providing a reliable transport mechanism for everything ranging from basic voice calls to financial services.

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?

Telecommunications networks have reached massive scale in India. Despite the fact that voice calling rates are the lowest in the world, there are several telecommunications providers who are able to sustain healthy levels of profitability.

However, when it comes to creating applications using other bearer channels – be it SMS, USSD, WAP or Internet – typically defined as Value Added Services, it is extremely difficult to create a service paradigm that is uniform for the customers of an independent service provider. There is little transparency,

process similarity or pricing. Everything depends on the specific situation at each telecom operator. This makes the task rather difficult and times even unpleasant.

Financial services delivery and financial inclusion is a national priority. Treating it as a “value added service” meant to increase either loyalty or ARPU for a telecommunications provider will defeat the larger goal of inclusion. Telecommunications providers must rightfully charge for the use of the infrastructure they have created – viz., the access network – but on comparable and reasonable terms. Ensuring access will create the environment where innovative service providers and application developers can freely participate in providing financial transaction services that conform to the norms set by the financial service providers based on the yardstick of transaction risk.

Creating a burden of Quality of Service or blanket technical standards of encryption, or specifying bearer choice will create deterrents to the widespread proliferation of financial services.

Epilogue

Equitable access to national communications infrastructure for accelerating delivery of essential services

Mobile subscribers in the country have grown spectacularly: over 350 times from around 2 Mn in April 2000 to over 700 Mn by end of October 2010. The telecom revolution that is sweeping across the country offers a splendid opportunity to ensure a meaningful implementation of essential services like health care, education and financial services/inclusion.

In order to do so, it is imperative that a universally accessible, simple and common addressing system is evolved. The internet uses domain name registration and universal resource locaters (URL) as the common addressing system allowing a service provider to offer single window access globally. Unlike internet where the bearer is always IP, Telephony provides a bounty of bearer choices ranging from voice, SMS, USSD and Data.

Type of bearer	Addressing	Access to	Control status	Remarks
Voice	10-digit or 11-digit (toll free) Phone number	Individuals and institutions	Open access	Publicly published tariffs by service providers
SMS	SMS Short code number	Institutions	Restricted access	Controlled by individual telecom service providers
USSD	USSD short code	Institutions	Highly restricted access	Controlled by individual telecom service providers
Data	WAP or Internet site URL	Individuals and institutions	Open access	Publicly published tariffs by service providers

A Policy Framework must be evolved to:

- a) Mandate access to all bearers and centralize allotment and management of the addressing mechanisms by a neutral independent entity (like the domain name registrar)
- b) Mandate that services must be available on the basis of transparently available and published commercial rates based on the cost of the infrastructure and then allowed to evolve basis free market forces. However, pricing may need to be kept reasonable, given that essential services, for e.g. financial inclusion, will need small ticket transactions to be viable.

The suggestions are on the lines of the existing Number Portability directive that aims to transfer control of the personal identity (mobile number) from service provider to end-user; similarly the above mandate will permit the transfer of control of a corporate or social identity by using telephony (short or long codes across bearers) as a universal addressing mechanism.