सत्यमेव जयते

Guidelines for Delivery Channels for Provision of Public Services through Mobile Devices

Version 1.0

August 2014

Government of India

Ministry of Communications & Information Technology

Department of Electronics and Information Technology

Metadata of Document

S. No.	Data elements	Values
1.	**Title**	Guidelines for Delivery Channels for Provision of Public Services through Mobile Devices
2.	**Title Alternative**	
3.	**Document Identifier** *(To be allocated at the time of release of final document)*	
4.	**Document Version, month, year of release** *(To be allocated at the time of release of final document)*	V1.0, August 2014
5.	**Present Status**	
6.	**Publisher**	Ministry of Communication and Information Technology, Department of Electronics and Information Technology
7.	**Date of Publishing**	
8.	**Type of Standard Document** *(Policy / Technical Specification/ Best Practice /Guideline/ Process)*	Best practices.
9.	**Enforcement Category** *(Mandatory/ Recommended)*	Recommended
10.	**Creator** *(An entity primarily responsible for making the resource)*	Ministry of Communication and Information Technology, Department of Electronics and Information Technology
11.	**Contributor** *(An entity responsible for making contributions to the resource)*	Deity, NIC, NeGD
12.	**Brief Description**	**Objective of the document is to provide:** • Guidelines to **deliver public services round-the-clock** to the users using m-Governance • Guidelines to develop **standard** based

		mobile solutions • Guidelines to **integrate the mobile applications** with the common e-Governance infrastructure.
13.	**Target Audience** *(Who would be referring / using the document)*	This document is intended for: Policy makers, Software Designers / Engineers, Testing and QA Engineers
14.	**Owner of approved standard**	Ministry of Communication and Information Technology, Department of Electronics and Information Technology
15.	**Subject** *(Major Area of Standardization)*	m-governance
16.	**Subject. Category** *(Sub Area within major area)*	e-Governance
17.	**Coverage. Spatial**	All stakeholders involved
18.	**Format**	PDF
19.	**Language** *(To be translated in other Indian languages later)*	English (To be translated in other Indian languages later)
20.	**Copyrights**	Ministry of Communication and Information Technology, Department of Electronics and Information Technology
21.	**Source** ***(**Reference to the resource from which present resource is derived)*	
22.	**Relation** *(Relation with other e-Governance standards notified by DeitY)*	

Point of Contact

JS (e-Gov)

Department of Electronics and Information Technology,

jsegov@deity.gov.in

Executive Summary

The National e-Governance Plan (NeGP) of the Government of India takes a holistic view of e-Governance initiatives across the country, integrating them into a collective vision. Around this idea, a massive countrywide infrastructure reaching down to the remotest of villages is being developed, and large-scale digitization of records is taking place to enable easy and reliable access over the internet. Public Service is *“any service or part thereof being provided to any person by the Central Government and the State Government or public authority either directly or through any service provider and includes the receipt of forms and applications, issue or grant of any license, permit, or certificate, sanction or approval and the receipt or payment of money by whatever name called in a particular manner”.* The ultimate objective is to bring such public services closer to home; as articulated in the Vision Statement of NeGP: *"Make all Government services accessible to the common man in his locality, through common service delivery outlets, and ensure efficiency, transparency, and reliability of such services at affordable costs to realize the basic needs of the common man"*. As an extension of this vision, and in cognizance of the vast mobile phone subscriber base of over 870 million in the country as of October 2013, the Government has decided to also provision for access of public services through mobile devices, thereby establishing mobile Governance (m-Governance) as a compelling new paradigm within the ethos of e-Governance. As a part of this initiative, DeitY has also prepared an m-Governance policy framework of Government of India which aims to utilize the massive reach of mobile phones and harness the potential of mobile applications to enable easy and round-the-clock access to public services, especially in the rural areas.

Disclaimer

The National e-Governance Plan (NeGP) of the Government of India strongly recommends adherence to Open Standards while taking decisions on the use of tools, technologies and database formats for all software applications being currently planned and developed for delivering e-Governance services and solutions.

However, many legacy and existing e-Governance applications are based on proprietary tools, technologies and database formats. Quite a few of these also form part of some of the Mission Mode Projects envisaged under the NeGP.

In this document, although detailed guidelines for delivery channels for mobile has been primarily based on the open standards, specific sections on proprietary software are also added to address requirements of such applications for a holistic perspective for the developers and solution providers.

Contents

1. Introduction

The National e-Governance Plan (NeGP) of the Government of India takes a holistic view of e-Governance initiatives across the country, integrating them into a collective vision. Around this idea, a massive countrywide infrastructure reaching down to the remotest of villages is being developed, and large-scale digitization of records is taking place to enable easy and reliable access over the internet. Public Service is *"any service or part thereof being provided to any person by the Central Government and the State Government or public authority either directly or through any service provider and includes the receipt of forms and applications, issue or grant of any license, permit, or certificate, sanction or approval and the receipt or payment of money by whatever name called in a particular manner".* The ultimate objective is to bring such public services closer to home; as articulated in the Vision Statement of NeGP: *"Make all Government services accessible to the common man in his locality, through common service delivery outlets, and ensure efficiency, transparency, and reliability of such services at affordable costs to realize the basic needs of the common man"*. As an extension of this vision, and in cognizance of the vast mobile phone subscriber base of over 870 million in the country as of October 2013, the Government has decided to also provision for access of public services through mobile devices, thereby establishing mobile Governance (m-Governance) as a compelling new paradigm within the ethos of e-Governance. As a part of this initiative, DeitY has also prepared an m-Governance policy framework of Government of India which aims to utilize the massive reach of mobile phones and harness the potential of mobile applications to enable easy and round-the-clock access to public services, especially in the rural areas.

As part of the initiative a shared technical infrastructure Mobile Services Delivery Gateway (MOBILE SEVA) has been created to enable integration of mobile applications with the common e-Governance infrastructure and delivery of public services to the users. The objective of creating the MOBILE SEVA is to put in place government-wide shared infrastructure and services to enable rapid development, mainstreaming and deployment of m-Governance services. It will enhance interoperability across various public services as well as reduce the total cost of operation of m-Governance services by providing a common pool of resources aggregating the demand for communication and e-Governance services, and act as a platform for various Government Departments and Agencies to test, rapidly deploy, and easily maintain m-Governance services across the country.

MSDP (Mobile e-governance Services Delivery Platform) provides an integrated platform for delivery of government services to citizen over mobile devices using Mobile Service Delivery Gateway (MSDG), SMS Gateway, m-App Store, m-Payment Services, Location Based Services (LBS), Unstructured Supplementary Services Data (USSD), Unstructured Supplementary Service Notify (USSN), Unstructured Supplementary Service Request (USSR), MMS, Cell Broadcasting Service (CBS), SIM Toolkit (STK), IVRS etc.

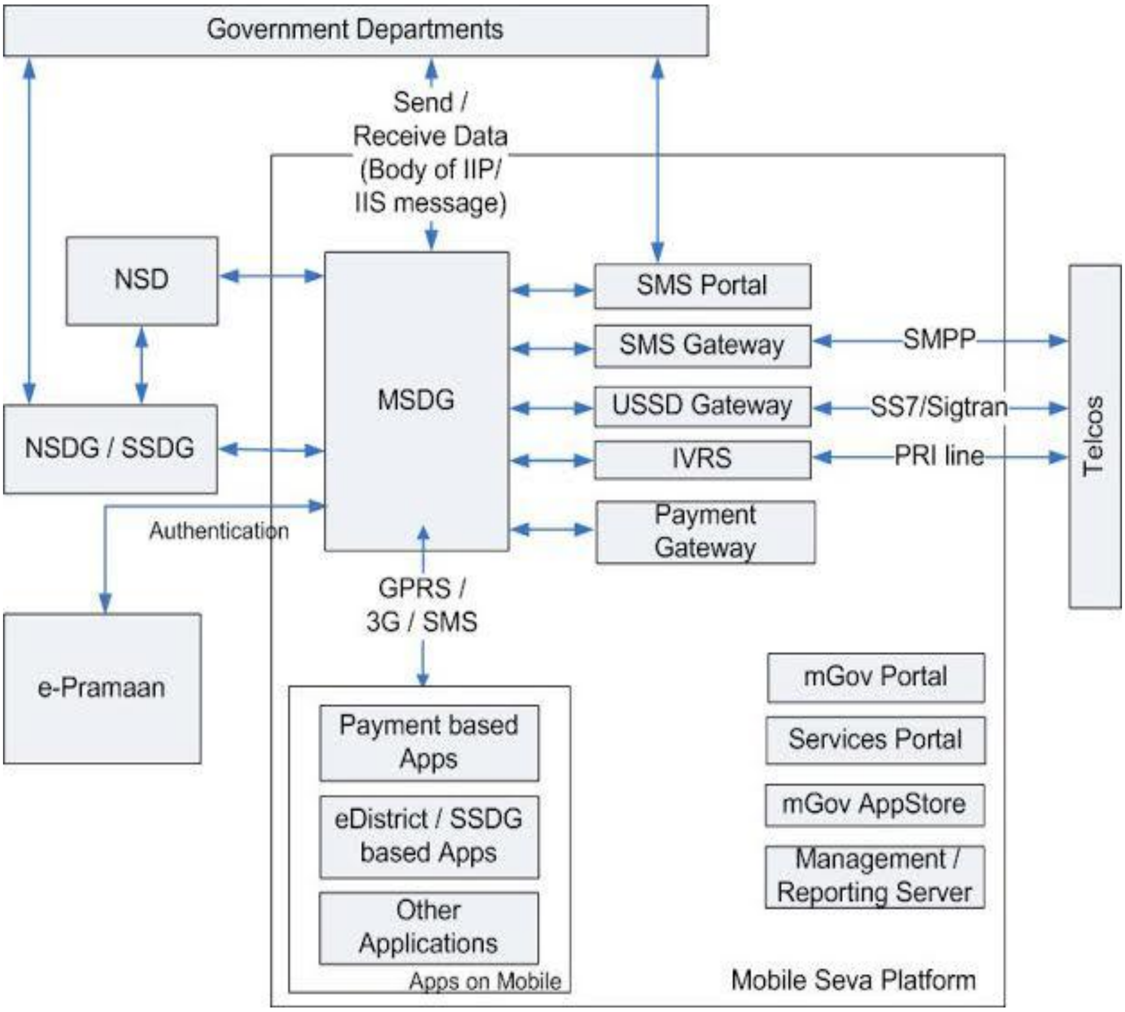


Figure 1: Mobile e-governance Services Delivery Platform (MSDP)

MSDG is a messaging middleware to facilitate e-Governance services delivery based on e-Governance Standard protocols which are IIP (Interoperability Interface Protocol), IIS (Interoperability Interface Specifications), IGIS (Inter-Gateway Interconnect Specifications) and Gateway Common Services Specifications (GCSS) in Annexure III.

Objectives:

- Guidelines to **deliver public services round-the-clock** to the users using m-Governance
- Guidelines to develop **standard** based mobile solutions
- Guidelines to **integrate the mobile applications** with the common e-Governance infrastructure.

2. Target Audience

This document is intended for:

- **Policy makers:** IT and other State department Secretary.
- **Software Designers / Engineers:** To understand and evaluate various Delivery channels for enable integration of mobile applications with the common e-Governance infrastructure and delivery of public services to users.
- **Testing and QA Engineers:** To define test plans and test cases based on the various delivery channels.

3. Type of Standard Document & enforcement Category

This document, as the name suggests, provides norms and recommendations termed as Best Practices for delivery channels for m-governance.

4. Definition and Acronyms

For definitions and acronyms please refer ANNEXURE IV.

5. Types of Mobile Devices and Mobile Platforms

Each year brings to life a new top of the line phone, while the previous year leaders can easily and quickly lose their positions. A mobile device, or handheld, is an electronic device that enables some kind of computing, and which is small enough to be easily carried around. Mobile devices enable people to take advantage of computing power without being shackled to a specific time or place. These devices are quite pervasive nowadays. Commonly used mobile devices include cell phones, and multi-media players. Most hand held devices are equipped with Next Generation Web Standards HTML5.0 Browsers, WI-FI, Bluetooth and GPS capabilities that can allow connections to the Internet and other Bluetooth capable devices.

5.1 Mobile Handset Manufacturers

A mobile phone (also known as a cellular phone/cell phone/hand phone) is a device that can make and receive telephone calls over a radio link whilst moving around a wide geographic area. It does so by connecting to a cellular network provided by a mobile phone operator, allowing access to the public telephone network. In addition to telephony, modern mobile phones also support a wide variety of other services such as text messaging(SMS), MMS, email, Internet access, short-range wireless communications (infrared, Bluetooth), business applications, gaming and photography.

All mobile phones have a number of features in common, but manufacturers also try to differentiate their own products by implementing additional functions to make them more attractive to users. Low-end mobile phones are often referred to as feature phones, and offer basic telephony. Handsets with more advanced computing ability through the use of native software applications became known as smart phones. The different Handset manufactured by various manufacturers has different mobile OS enabling various specific features and functionality. The support for the native apps and other special features are unique and hence catering to the large number of user poses a great deal of challenge. Hence prior to offering public services over mobile phones, it is recommended to know the target users to begin with and gradually making the services available for all. The service going to be offered must be designed to cater the large population using various mobile handset manufactured by different vendors.

5.2 Mobile Operating System

A mobile/handheld device has an operating system called a mobile OS, is an operating system that is specifically designed to run on mobile devices such as mobile phones, smart phones, tablet computers and other handheld devices. The mobile operating system is the software platform on top of which other programs, called application programs known as apps, can run on mobile devices.

The manufacturer chooses the operating system for that specific device. The operating system is responsible for determining the functions and features available of the device, such as thumbwheel, keyboards, WAP, synchronization with applications, e-mail, text messaging and more. The mobile operating system will also determine which third-party applications can be used on your device. The mobile market is fragmented Because of different OS software platforms, some of the common and well known mobile OS includes: J2ME, Windows Mobile, Palm OS (and newer webOS), BlackBerry, Symbian, Tizen, Android, and iPhone OS etc.. All of these have their own unique features as well as areas where user's demand has forced third-party solutions. A mobile OS determines the choice of apps and phone functionality. While most of basic public services can be delivered using delivery channels like SMS, USSD, IVRS and other such elementary channels which are uniform over all mobile devices having different OS. The choice of apps and OS to deliver a particular service requires advance knowledge of various mobile OS available in the market and their market share to cater the target users in order to build different version of applications. The present Indian Mobile market share is given in the following figure.

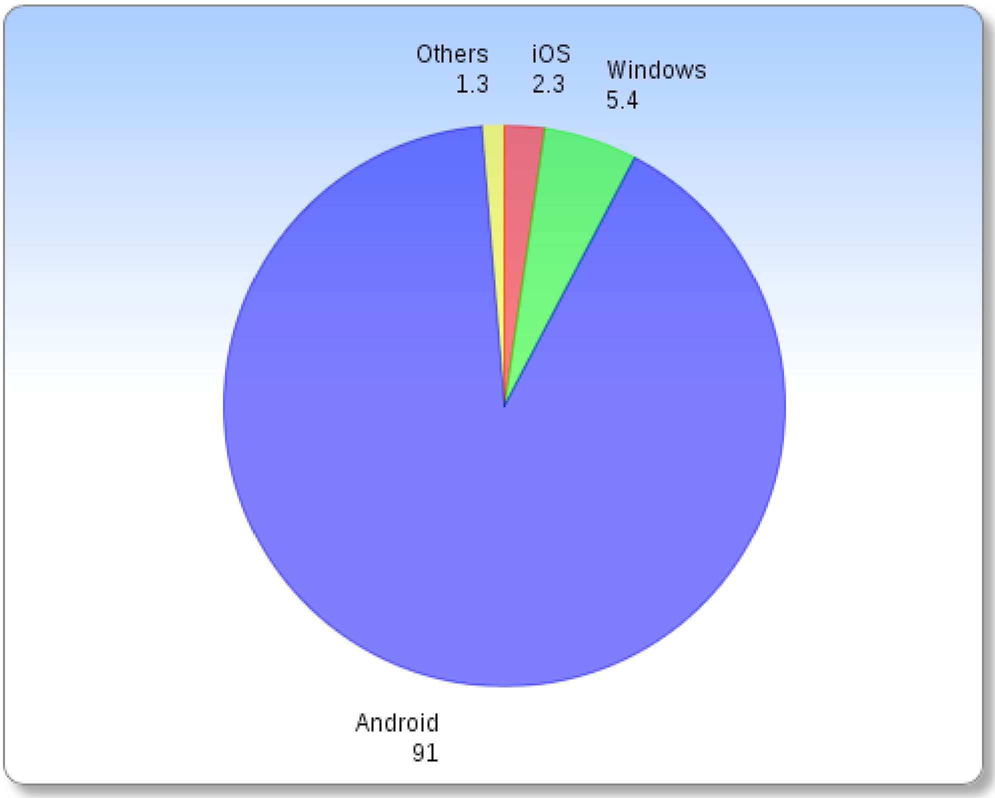


Figure 2: Mobile Platform Market share in India

6. Delivery Channels

6.1 Short Messaging Service (SMS)

Short Messaging Service (SMS) is a text messaging service component of phone, web, or mobile communication systems, using standardized communications protocols that allow the exchange of short text messages between mobile devices.

It needs little bandwidth, works well in poor signal areas, is easy and inexpensive to implement. Users need only a mobile phone. Localization can also be easily accomplished on SMS.

SMS based mobile applications can be effectively deployed by government departments and agencies for providing a range of services in different areas. These include submission of forms, alerts and notifications etc. for services at district and sub-district levels, such as certificates, pensions, land records, etc. They can also be effectively used for a variety of services in health, education, weather alerts, market prices, disaster management, etc.

The text limit of current SMS for English text is 160 characters. For Indian languages the text limit is 70 chars and would not be enough. There are some established standards like 3GPP in which compression algorithms could be used to fit Indian language text into the character limit.

6.1.1. Types of SMS Based Services

There are three kinds of services usually deployed:

- **Informational Services:** These are pure information based services aimed at providing generic or specific information to the users about various activities. For example, at a tourist location, the Tourism Department might provide relevant information about the place to the tourists arriving there. Similarly, Health Department might provide information about an immunization drive in a particular area.

- **Interactional Services:** These services are aimed at user requests for the status of a particular transaction or activity. For example, a user may request for the status of her application for a new ration card. For a mobile based interactional service, the user is required to send an SMS with specified key words to a pre-designated short or a long code for obtaining the information.

- **Transactional Services:** These are services that ultimately result in a transaction based on the request from the user with or without payment of a fee. For example, a user may submit a new request for a ration card through her mobile device. After the request is received, the concerned department processes the same and delivers the card to the user.

6.1.2. Deploying SMS Based Services

- A cost-effective, high performance and scalable solution is required to deploy SMS services.
- The solution should provide a wide range of features to suit the needs of users.
- The range of protocols supported should allow the solution to be deployed on digital wireless networks based on GSM, IS-41 (D-AMPS, CDMA) and TDMA standards. There are next generation wireless systems like LTE and LTE Advanced.
- The solution should be able to work efficiently with long queues of messages.
- There should be provisions to send/receive text and Mobile Originated/Mobile Terminal SMS messages.
- The message originator should have the ability to activate delivery notifications.
- Using SMS Gateway, there should be provision for interchange messages with other systems such as Internet email (Capable of supporting POP3, IMAP4, SMTP (with or without SSL)), the web etc.
- A dynamic system configuration is preferred so as to provide adaptability to new technology.
- **Sending-Receiving SMS:** 3GPP standards such as **TS 23.038** and its previous versions are meant for sending - receiving SMS's and is primarily made for European scripts. The latest 3GPP TS23.042 standard is about the compression of messages using Huffman encoding; this requires the language knowledge for building the Huffman tables. At present these standards do not have the Indian Language perspective and will require some Indian language specific inclusions. The vendors, developers can participate, propose the amendments, and create new standards using the 3GPP guidelines.

6.1.3. Multi-Channel Service Delivery Platform for Mobile Cloud Apps

As the mobile client computing is penetrating to rural areas and e-governance services available from the GI-Cloud are required to reach the every citizen, mostly resides in rural areas. It is also essential to provide reliable & secure connectivity for these cloud based application and data to these mobile rural users. The intermittent nature of present GPRS networks is hard to make it possible to provide reliable and unified solution. The SMS based approach with secure measures makes the optimal integration of existing services to provide seamless connectivity to rural areas, by considering the factors like on-the-fly integration of existing channels (say GPRS and SMS together). That is, a specially designed client application shall use GPRS to access Cloud Services and switch to SMS channel if GPRS is not available with the help of a proxy application & SMS gateway running for the mobile cloud apps.

6.2 Multimedia Messaging Service (MMS)

Multimedia Messaging Service, or **MMS**, refers to a way of sending messages that include multimedia content to and from mobile phones. It is supported by GPRS enabled and newer devices. MMS is implemented using a combination of WAP and SMS technologies. MMS enables multimedia messages containing content such as pictures, graphics, music, images, and ringtones. The MMS standard, based on 3GPP & WAP Forum standards, includes an MMS mail client on the device, a WAP - gateway for sending & receiving messages & a multimedia messaging service center (MMSC) for storing, trans-coding and relaying messages.

6.2.1. Deploying MMS Based Services

- The solution should provide a wide range of features to suit both new and existing mobile operators and content providers.
- The solution should be compliant with the standards and specification maintained by:
  - For Network Protocols carrying MMS Message
    - 3GPP at www.3gpp.org
    - 3GPP2 at www.3gpp2.org
    - Open mobile Alliance at www.openmobilealliance.org
    - Internet Engineering Task Force at www.ietf.org
  - For Encoding of Multimedia Message
    - Internet Engineering Task Force (RFC) at www.ietf.org
    - International Telecommunication Union at www.itu.int
    - International Organization for Standardization (ISO) at www.iso.org
    - International Electrotechnical Commission (IEC) at www.iec.ch
    - Synchronized Multimedia Integration Language(SMIL) at www.w3.org
- The 3rd Generation Partnership Project (3GPP) is collaboration between groups of telecommunications associations, known as the Organizational Partners. The term "3GPP specification" covers all GSM (including GPRS and EDGE), W-CDMA and LTE (including LTE-Advanced) specifications. The following terms are also used to describe networks using the 3G specifications: UTRAN, UMTS (in Europe) and FOMA (in Japan). 3GPP supports Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface. For details please refer: http://www.3gpp.org/
- There should be a solution to flexible postponed delivery scenarios: To allow the operator to define message delivery scenarios on the base of Alert messages, or schedules on the base of the error code from a previous delivery attempt.
- The message originator should have the ability to activate delivery notifications and read-reply reports.
- Although the MMS standards do not specify a maximum size for a message, to develop mechanism to support more than 300 kB size, which is the currently recommended by networks due to limitations at the WAP gateway end.
- A dynamic system configuration is preferred so as to provide adaptability to new technology.
- The infrastructure should be scalable to match network growth.
- The two key components to ensure effective MMS processing are:

  - MMS Control Centre to efficiently manage and control the flow of messages through the platform, deciding on the most efficient route bearing in mind current server load and availability.
  - MMS Store to temporarily store the multimedia files while the transaction is processed.
- There should be efficient management of the sending of messages to supplier networks by looking at availability and current loads.
- The standard formats which may be used for MMS are:
  - WML (Wireless Markup Language) provides navigational support, data input, hyperlinks, text and image presentation.
  - XML (Extensible Markup Language) to encode documents in machine-readable form.
  - SMIL (Synchronised Multimedia Integration Language) allows for time dependent display of information. For MMS based service through Web Interface the most important standard in W3C is SMIL2.0

6.2.2. Challenges - Offering Services via MMS

Handset configuration can cause problems sending and receiving MMS messages. There are some interesting challenges with MMS that do not exist with SMS and may be preferably addressed:

- Multimedia content developed by a particular phone should be compatible to be delivered to other phones.
- Mechanism should be developed to include distribution lists or to address large numbers of recipients by *Value-Added Service Providers* (VASPs) in 3GPP.
- To optimize and reduce the transactional overhead in case of bulk-messaging.
- To develop alternate mechanism apart from the database maintained by operator to determine whether a handset is MMS capable or not, which may be standardized.

6.3 Unstructured Supplementary Service Data (USSD)

Unstructured Supplementary Service Data is a technology unique to GSM. It is a protocol used by GSM cellular telephones to communicate with the service provider's computers. USSD provides session-based communication, enabling a variety of applications. It can be used for WAP browsing, prepaid callback service, mobile-money services, location-based content services, menu-based information services, and as part of configuring the phone on the network. USSD messages are up to 182 alphanumeric characters in length.

USSD provides a cost-effective and flexible mechanism for offering various interactive and non-interactive mobile services to a wide subscriber base. USSD supports menu-based applications facilitating more user interactions. It is neither a phone-based nor a SIM-based feature. It works on almost all GSM mobile phones (from old handsets to new smart phones). USSD allows faster communication between users and network applications (almost seven times faster than SMS) because messages are sent directly to the receiver allowing an instant response. The USSD gateway supports an open HTTP interface. USSD is supported by WAP, SIM Application Toolkit and CAMEL enabling scope for many applications.

It is used to send short commands to and from the Mobiles and GSM network. USSD text messages can be up to 182 bytes in length. Messages received on the mobile phone are not stored.

3GPP GSM 02.90 (Stage - 1) 3GPP GSM 03.90 (Stage - 2)

At presents these standards for USSD do not consider Indian Language text and vendors, developers are encouraged to participate in enhancing these standards for Indian languages.

6.3.1. Deploying USSD Based Services

- The access policies and bandwidth allowances should be managed separately for each application.
- There should be provisions to send/receive MO/MT USSD messages between mobile subscriber and application/service provider.
- The solution should support USSD1, and preferably USSD2, suiting to the service offered via the channel.
- The solution should support GSM MAP phase I, II, III for GSM phones and IS41 for CDMA phones.
- An optimum security solution to provide secure USSD-based transactional services is desired.

  The top 5 security threats for USSD-based apps are:
  - USSD Commands Request/Response Tampering
  - USSD Request/Response Message Replay Attacks (in case the phone is lost)
  - USSD Application Prepaid Roaming Access Test
  - Verify Strong Cryptographic Implementation
  - Improper Data Validation (USSD IP Mode Applications)
- The infrastructure should be scalable to match network growth.
- A dynamic system configuration is preferred so as to provide adaptability to new technology.

6.4 Interactive Voice Response (IVR) System

Interactive Voice Response is a technology that allows a computer to interact with humans through the use of voice and DTMF (dual-tone multi frequency signalling) keypad inputs. IVR enables users to interact with a database via a telephone keypad or by speech recognition and also service their own inquiries by following the IVR dialogue.

IVR systems are an example of computer-telephone integration (CTI). They can respond with pre-recorded or dynamically-generated audio to further direct users on how to proceed. IVR applications can be used to control almost any function where the interface can be broken down into a series of simple interactions. IVR systems deployed in the network are sized to handle large call volumes.

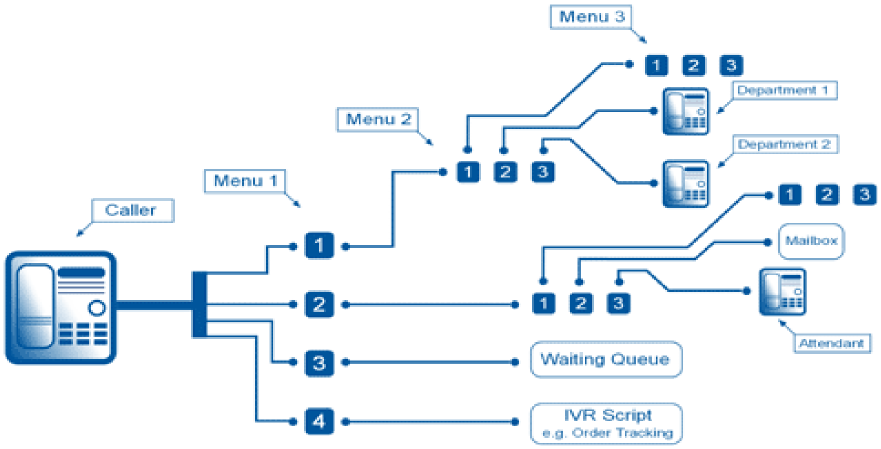


Figure 5: IVR Call Flow Process

Each number key on a telephone emits two simultaneous tones (DTMF): one low-frequency and the other, high-frequency. The number ONE, for example, produces both 697-Hz and 1209-Hz tones that are together universally interpreted by the public switched telephone network as a "1". A computer needs special hardware called a **telephony board** or **telephony card** to understand the DTMF signals produced by a phone. A simple IVR system only requires a computer hooked up to a phone line through a telephony board and some inexpensive IVR software. IVR equipment includes a computer phone system that houses and controls telecommunications resources (computer telephony cards) and hosts the IVR management and control software.

6.4.1. Deploying IVRs Based Services

- An IVR can be deployed in several different ways:
    - Equipment installed on the customer premises
    - Equipment installed in the PSTN (Public Switched Telephone Network)
    - Application Service Provider (ASP) / Hosted IVR
- The solution should conform to W3C's standard XML format for specifying interactive voice dialogues between a human and a computer.
- Menu Options:
    - Messages need to be kept short, and should include some prominent key words
    - The function need to be announced followed by the key required to activate it
    - Provision to the customers for two or three chances to select an option
    - The system should transfer a caller to an operator if no option is chosen

  - Provision for repeat facility, keeping the best practice for the repeat to occur automatically rather than relying on the customer selecting to hear the options again
- Queuing: The customer should be indicated for being in the queue and the approximate time before the call will be answered – update the customer at reasonable intervals
- User Responses:
  - Provision to allow users who need extra time to respond to prompts
  - Non requirement for the same information to be entered more than once
- Help facilities
  - Provision for option in the menu to access a human operator
  - Provision of context-sensitive help

6.5 Mobile Application (m-Apps)

Mobile application software is applications software developed for handheld devices, such as mobile phones, tablets etc. These applications can be pre-installed on phones during manufacture or downloaded by users from various mobile software distribution platforms, or delivered as web applications using server-side or client-side processing (e.g. JavaScript) to provide an "application-like" experience within a Web browser.

6.5.1. Mobile Application Dependency on Handset and O/S

Mobile Application software developers also have to consider a lengthy array of screen sizes, hardware specifications and configurations because of intense competition in mobile software and changes within each of the platforms.

There are numerous types of mobile systems and mobile devices available at present and more advanced ones are also evolving. Though the advanced technology available today helps developers a great deal, but it still takes a lot of time, thought and effort to create apps for different mobile systems.

Different mobile applications need to be developed for various mobile platforms available, such as Apple, Android and BlackBerry etc and also mobile application needs to be developed based on the handset capability of the target users for delivery of public services. The different version of m-apps is to be maintained depending on mobile platforms and mobile devices. Proper provision for update and release of m-apps should be ensured to provide up to date features and functionality.

6.5.2. Data Collection: m-forms

Mobile Application can also make use of the various forms for data collection. Many data collection systems are built from existing commercial or open source components, or even come packaged as an end-to-end solution. The components of data collection relate to each other as shown below:

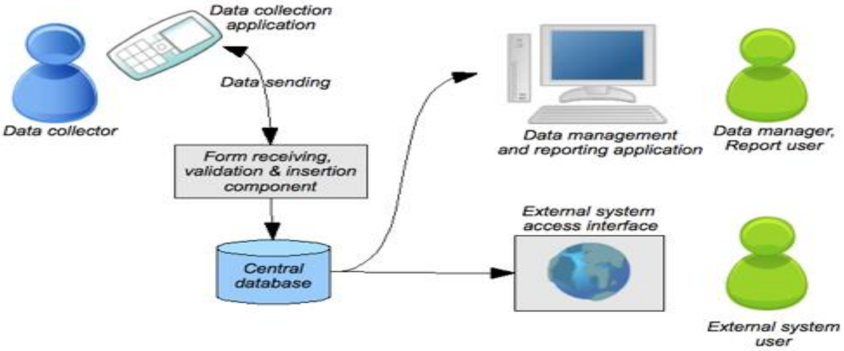

Data collection application
Data collector
Data sending
Form receiving, validation & insertion component
Central database
Data management and reporting application
Data manager, Report user
External system access interface
External system user

Figure 7: Data Collection using Forms

The data collection may be done by various methods. Following are the most common types of data collection client applications which may be used:

1. **Fixed format SMS based Forms:** The 'client application' in this case is the phone's built-in SMS functionality. The user writes and sends SMS in a predefined format, representing answers to successive questions.
2. **Java Micro Edition Platform (J2ME) Application based Forms:** A J2ME application is written in the Java programming language, and loaded onto the phone over Bluetooth or by downloading the application from the Internet. To use the client application, the data collector navigates through questions in an application on the phone, which collects the answers and submits the completed form to a server.
3. **Mobile Operating System based Forms:** Mobile Operating Systems such as Android, Windows Mobile can also be used for developing native platform-dependent applications which can have various forms for data collection.
4. **Web-based Forms:** The 'client application' for web-based forms is the phone's web browser. The user browses to a website, where the form is published in an optimized format for mobile browsers.
5. **Voice-based based Forms:** The user dials a number and then chooses from options on a menu, useful when there are low levels of literacy among data collectors, or when a system is needed that caters for both landline and mobile phones.
6. **Wireless Internet Gateway (WIG) based Forms:** WIG uses a programming language (Wireless Markup Language, or WML) that is internal to almost all SIM cards. The menu definition is easy to write, but the size limit is 1MB, making it difficult to support long menus or multiple languages.
7. **Unstructured Supplementary Service Data (USSD) based Forms:** This is a real-time question-response service, where the user initiates a session and is then able to interact with the remote server by selecting numeric menu options. The phone needs to be continuously connected during the session, which needs a good, consistent signal.

Once data has been captured on the phone, the completed form generally needs to be submitted to a central back-end server.

6.5.3. Deploying Forms Based Services

- The mobile data collection system should have the required components that communicate for data collection, transmission, storage and retrieval, namely:
  - The data collection client interface, which the user interacts with to accomplish data collection and transmission
  - The data transfer method, which dictates how the information input on the phone is transmitted to a central server for storage and retrieval.
  - Server-side components to receive and store the data, and allow users to display and manage the database.
- The solution should fulfill the necessary technical requirements of the chosen data collection application.
- The limitations of mobile devices require developers and designers to come up with alternate ways to allow users to input data faster and more easily.
  - Mobile forms developed should significantly remove the constraints like smaller screens, slower connections, easier text entry etc.
  - To use radio buttons, checkboxes, select menus and lists which tend to work much better than open text fields for seeking inputs from users on mobile devices.
  - To use “field zoom” feature when a user selects a form’s input field, to expand it to fill the screen’s viewable area. Field zoom is another great reason to top-align input field labels in forms.
  - To recognize specific input types by some mobile Web browsers (although part of the developing HTML5 standard) and adjust their input modes accordingly.
  - For drop-down select menus on Web forms, a pop-up menu control may be provided, which control display of the options in the menu in a contained list that can be scrolled at various speeds though drag, nudge and flick gestures. The large touch targets would make it easy to select the right value.
  - In addition to having compound menu controls developers may explore custom input controls provided by mobile operating systems like sliders, split buttons, rating widgets, scrubbers in place of standard form controls to make inputting easier for users.

6.5.4. m-Gov service support center

It must operate with common infrastructure to provide following functions:

- White list management for the reliability and authenticity of m-App
- m-App modification prevention
- To prevent the duplicative development of m-Services
- Mechanism for the verification of m-App integrity

7. Other Technologies

7.1 Location Based Services (LBS)

Location-based services (LBS) denote services offered to mobile users according to their geographic location. LBS give the possibility of a two way communication and interaction. Therefore the user tells the service provider his actual context like the kind of information he needs, his preferences and his position. This helps the provider of such location services to deliver information tailored to the user needs. LBS enables to retrieve and share information related to their current position. Examples are Google Latitude or Panoramio.

It works as an intersection of the following features in a system:

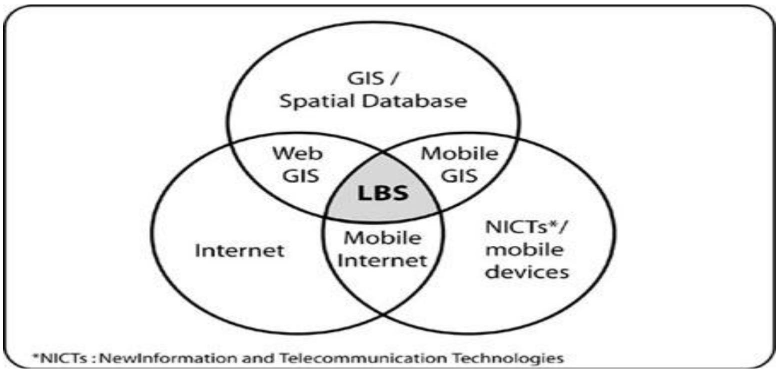


Figure 8: Location Based Service (LBS)

Geographical Information System (GIS) is a hardware, software and procedures designed to support the capture, management, manipulation, analysis, modeling and display of spatially referenced data for solving complex planning and management problems.

Internet is used to utilize the database dynamically so as to provide the appropriate service.

Mobile Devices as an end- device to execute the service.

7.1.1. Key Factors to LBS Success

- The application developed should be compelling providing valuable to consumers or businesses which is easy and intuitive to use.
- The key consideration while designing the LBS application is handset availability. There is wide range of LBS-capable handsets available in market and with users.
- LBS application designed needs to be Internet-friendly, IP-based user plane standards.
- Awareness and promotion of the designed LBS application is the another key success factor. The security and privacy concerns of user must be ensured.

7.1.2. LBS Components

For user to start using a LBS different infrastructure element are necessary. The five basic components are:

- **Mobile Devices:** A tool for the user to request the needed information. The results can be given by speech, using pictures, text and so on.
- **Communication Network:** The mobile network which transfers the user data and service request from the mobile terminal to the service provider and then the requested information back to the user.
- **Positioning Component:** For the processing of a service usually the user position has to be determined. The user position can be obtained either by using the mobile communication network or by using the Global Positioning System (GPS). Further possibilities to determine the position are WLAN stations, active badges or radio beacons. The latter positioning methods can especially used for indoor navigation like in a museum. If the position is not determined automatically it can be also specified manually by the user.
- **Service and Application Provider:** The service provider offers a number of different services to the user and is responsible for the service request processing. Such services offer the calculation of the position, finding a route, searching yellow pages with respect to position or searching specific information on objects of user interest (e.g. a bird in wild life park) and so forth.
- **Data and Content Provider:** Service providers will usually not store and maintain all the information which can be requested by users. Therefore geographic base data and location information data will be usually requested from the maintaining authority (e.g. mapping agencies) or business and industry partners (e.g. yellow pages, traffic companies).

7.1.3. Application Examples

- **Emergency Services:** Ability to locate an individual’s exact location or when one is not able to reveal it because of an emergency situation (injury, criminal attack etc.).
- **Navigation Services:** Navigation services based on mobile users’ need for directions within their current geographical location. The ability of a mobile network to locate the exact position of a mobile user can be manifested in a series of navigation-based services.
- **Information Services:** Finding the nearest service, accessing traffic news, getting help with navigating in an unfamiliar city, obtaining a local street map – these are just a few of the many Information services offered via LBS. Location-sensitive information services mostly refer to the digital distribution of information based on device location, time specificity and user behavior.
- **Tracking and Management Services:** Tracking services can be equally applicable both to the consumer and the corporate markets. One popular example refers to tracking postal packages so that companies know where their goods are at any time. Vehicle tracking can also be applied to locating and dispatching an ambulance that is nearest to a given call.

- **Billing Services:** Location sensitive billing refers to the ability of a mobile location service provider to dynamically charge users of a particular service depending on their location when using or accessing the service.

7.2 Cell Broadcast Centre

Cell Broadcast is a mobile technology which allows text messages to be broadcasted to all mobile handsets and similar devices within a designated geographical area. It is a one-to-many geographically focused service, in contrast to SMS which is a one-to-one or one-to-few service. It is usually used for providing location-based services, especially emergency services, as it utilizes minimum network resources for message broadcast and provides instantaneous delivery to all subscribers in a geographic area. A Cell Broadcast message is an unconfirmed push service, meaning that the originator of the message does not know who has received the message, allowing for services based on anonymity. Mobile telephone user manuals describe how the user can switch the receiving of Cell Broadcast messages on or off.

Also known as Short message service-Cell Broadcast (SMS-CB), CB messaging is a mobile technology feature defined by the ETSI's GSM committee and is part of the GSM standard. It is also supported by UMTS, as defined by 3GPP.

7.2.1. Deploying Cell Broadcast Centre

Service Area Broadcast Protocol (SABP) 3GPP TS 25.419

It defines the protocol between the Cell Broadcast Centre (CBC) and the Radio Network Controller (RNC). Support for Indian languages in this protocol will allow emergency disaster alerts and other e-governance alerts to be sent/broadcasted to handsets in local languages.

- Above standards and many more other such standards describes SMS protocols, trigger alerts, news broadcast etc. At present these standardizations do not cover Indian languages and vendors, developers are encouraged to participate in enhancing these standards for Indian languages.
- The system architecture should be highly efficient, available and scalable.
- CBC should support multiple users.
- The system should be designed to be deployed in GSM, CDMA and 3G UMTS networks.
- It should be able to integrate with the network elements over various interfaces like TCP, MMI, SS7, SIGTRAN etc.
- The GSM solution should integrate with any vendor Base Station Controller (BSC), Radio Network Controller (RNC) and Operations and Maintenance Centre – Radio system (OMC-R), all compliant with the respective 3GPP standards.
- The CDMA solution should integrate with any vendor MSC IS41 interface (to integrate with CDMA network elements).

- CBC should integrate with Cell Broadcast Entities (CBE) on a standardized interface over TCP/IP.
- The solution should be equipped with a set of APIs for connecting to any source or cell broadcast entity (CBE), as well as an intuitive, user-friendly graphical user interface (GUI).

7.3 Localization

Given that only a miniscule segment population in India can read and write English, it is important to deploy local/ regional languages to ensure all-round success of m-Governance initiatives. For detailed guidelines please refer to the **Mobile Localization Guidelines**.

7.3.1. Indian Language SMS

Currently, Indian language SMS services are offered by some operators but unlike the English SMS service, the language service is not necessarily interoperable across networks and cannot be availed on all types of handsets. The lack of a standard for Indian SMS comes in the way of providing scalable, interoperable and affordable SMS services in Indian languages.

To realise the goal of interoperable and affordable Indian language SMS, the following are the priority areas:

- Text entry standards (i.e. keypad)
- Encoding standards to support all the major Indian languages
- Font support standardization for handsets to send and receive Indian language SMS

7.3.1.1. Text entry methods

The two methods in vogue are:

- Mapping the Indian language characters on the handset keypad
- Screen-assisted text inputting mechanisms available from a few OEMs and vendors

The keypad for the English language has been standardized by ITU. Although efforts on supporting the Indian languages on handheld devices are on, acceptable standards are yet to be evolved. In the absence of any national standards specifying mapping of the Hindi (and other Indian Languages) alphabets to the 12-key mobile devices, the handset vendors keen on penetrating the large Indian market are using their own mappings (which can differ across vendors).

7.3.1.2. Encoding standard

The Unicode standard supports the 22 major Indian languages but uses more bandwidth (2 octets for each character) and hence the maximum size of SMS that can be sent using Unicode (70 characters) would be less than half of that of an English language SMS (170 characters). In

September 2009, the 3rd Generation Partnership Project (3GPP), which unites telecommunications standards bodies, included language tables that enable SMS in the 22 major Indian languages, with nearly the same message size as in English, and with bilingual capability in English and any Indian language enabled by a proposal from CEWiT with support from various other industry partners in India.

7.3.1.3. Font support

Solutions for aesthetic display of Indian language scripts on small handset screens are being worked out. Similarly, solutions are tried out for handsets already in use so that they can receive and display messages in Indian languages, even if they cannot be used to send such messages.

7.4 M-Payment

Mobile payment is an alternative payment method. Instead of paying with cash, check, or credit cards, a consumer can use a mobile phone to pay for a wide range of services; after having authenticated the user using AADHAR or any other means. The basic aim of mobile payments is to enable micropayments on low-end mobile devices which support only voice and text, in addition to higher end phones which could support web-browsing or Java application capabilities. RBI operative guidelines for banks for m-payment in India is given at Annexure II.

7.4.1. Mobile banking (M-Banking OR mbanking)

M-Banking is a term used for performing balance checks, account transactions, payments, credit applications and other banking transactions through a mobile device. The earlier mobile banking services were offered over SMS, a service known as SMS banking. With the introduction of smart phones with WAP support the mobile web is also being used for M-Banking. Latter with the advancements of web technologies such as HTML5, CSS3 and JavaScript it became feasible to launch mobile web based services to compliment native applications.

7.4.1.1. Deploying M-Banking

- **Mobile Banking Service over Application/ Wireless Application Protocol (WAP):** Mobile phones with or without GPRS connection can do M-Banking by downloading the application on to the mobile handset or via WAP on all phones with GPRS connection. The functionalities offered include Funds can be transferred within and outside the bank, Immediate Mobile Payment Services (IMPS) etc. The charge for SMS/GPRS is to be borne by the user.

- **Mobile Banking Service over SMS:** Mobile phones with or without GPRS connection can do M-Banking. There is no need to download the application. Ordinary SMS charges are applicable. The functionalities offered include Immediate Mobile Payment Services (IMPS-Mobile to Mobile Transfer). The charge for SMS is to be borne by the user.

- **Mobile Banking Service over Unstructured Supplementary Service Data (USSD):** Mobile phones with or without GPRS connection can do M-Banking. There is no need to download the application. The functionalities offered include Fund Transfer within bank. The charge for USSD is to be borne by the user.

7.4.2. Immediate Mobile Payment Services (IMPS)

The Immediate Mobile Payment System (IMPS) has been developed by the National Payments Corporation of India (NPCI) to expand the scope of mobile payments to all sectors of the population. IMPS offer an instant, 24X7, interbank electronic fund transfer service through mobile phones. An IMP provides an inter-operable infrastructure to the banks for enabling interbank real time funds transfer transactions. IMPS rides on the existing NFS Interbank ATM transaction switch infrastructure and message format making it easy for banks to adopt.

To enable the transfer of money, both the sender and the receiver of payment have to link their bank accounts with their phone numbers through their respective banks. The sender has to register for mobile banking service with her/his bank. Upon registration, the bank will provide a link to the mobile banking software which needs to be installed in the mobile phone to enable payments. Both the sender and the receiver will receive a Mobile Money Identifier (MMID) while the sender will also receive a Mobile PIN (MPIN) for authentication of transactions. While transacting, the sender has to input the MPIN, receiver’s mobile number and MMID, and the amount of funds to transfer. IMPS will authenticate the sender, check the receiver’s mobile number and MMID, and transfer the funds to the receiver’s account in real-time. Both the sender and the receiver receive messages notifying them about the success or failure of the transaction.

7.4.3. Contactless cards and Mobile Phones

These cards are based upon a technology known as NFC (Near Field Communication) that allows NFC enabled cards to be ready by taping them on or by passing them by, a card reader than swiping them through or inserting into, the POS terminal. They are now being integrated into mobile phone handset for m-Payments. NFC enabled phones are expected to become more widely available. The NFC chip inside the phone will be connected to the secure element within the SIM card, allowing information stored in an m-wallet to be accessed by the NFC card reader. Authorization for payments involves entering a PIN.

7.4.4. Airtime balance for payment

Airtime as balance for payment was realized because of the need for the unbanked majority to easily and cheaply transfer funds around the country. The facility required is the most basic of mobile phones, an account, which can be opened at any one of vendors to start transferring and receiving money. Since the system uses either SIM toolkit or USSD technology depending on the country, the network charges are minimal to nonexistent. It has lowest entry barriers, since it works on more than 95 percent of handsets and has low transaction costs and no bank account or credit card required.

In addition to money transfers, in some countries, airtime is beginning to be used to pay for goods and services, essentially transforming the mobile device into an airtime wallet. A user may fund the mobile transaction either by prepaying for airtime, thereby "topping up" the account and then using the value as a medium of exchange, or by establishing a stored-value account maintained by the carrier for the mobile phone holder, which can then be used for transactions. A mobile top-up request can be executed through the mobile operator's network to debit the account of the payment initiator and credit the account of the recipient. Some networks permit roaming prepaid users to top up their accounts using vouchers purchased from other network operators, which may be impacted by foreign currency conversion charges.

In this practice, the telecommunications firm authorizes its retailers to market and sell mobile phone airtime credits in return for a small fee, which permits consumers to sell surplus credits for unused minutes to a third party. This commoditization of airtime permits the operator to efficiently expand its agent network to remote and rural geographies typically underserved by mainstream financial services providers.

7.4.5. Mobile Wallet

A Mobile Wallet is functionality on a mobile device that can securely interact with digitized valuables thereby making payments using the mobile phone. Mobile wallet may reside on a phone or on a remote network / secure servers. It is controlled by the user of the wallet.

7.4.5.1. How Payment Works:

Following technologies help the Mobile Wallet for m-Payment:

- **Near Field Communication (NFC) controller and antenna:** Enable mobile devices to send account information securely to contactless payment readers at customer check-outs and other points-of-sale, and read contactless enabled tags placed in advertising collateral and consumer products.
- **Secure element:** A secure smart card chip inside the phone used for storing and accessing account information. It is separate from the memory where photos, apps, and contacts are stored. Access to personal information in the secure element is protected by additional security layers.
- **Electronic wallet application:** The application or user interface that allows users to manage accounts and initiate payments from their digital wallet
- **Trusted Service Manager (TSM):** The TSM connects payment cards virtually into mobile wallets securely. Over the air and in a matter of seconds, the TSM enables the user to enter their account number into mobile wallets, authenticates with the financial institution, and enables that payment credential to be used from within the mobile wallet. Smart phones enabled with these technologies allow consumers to migrate all of the "plastic" in their

leather wallets such as credit and debit cards, loyalty accounts, gift cards, and more, to a mobile wallet. With account information stored in their handheld device, consumers can make payments with a “tap” of their phone on the contactless readers.

- **Voice:** To conduct a transaction, users simple place a voice call to the platform, and acquire access to their account through Voice Biometrics-based authentication.

7.4.5.2. Mobile Wallet Transaction

Using a mobile wallet to make a payment is incredibly simple. When it is time to pay, the user turns on his or her phone’s screen (if the screen is off, when the phone is dormant for instance, the NFC chip will not work), opens the wallet application, enters their pin number, and passes the phone within a few inches of the contactless payment symbol. The payment transaction is then processed just like a conventional card transaction. In addition, relevant offers, discounts, and coupons can be passed from the wallet along with the payment in that same tap of the phone.

7.5 SIM Application Toolkit

The SIM Application Toolkit is a standard set of commands, under GSM, which defines how the card should interact with the outside world and extends the communication protocol between the card and the handset. It is designed as a client server application. With SIM Application Toolkit, the card has a proactive role in the handset, i.e., the SIM initiates commands independently of the handset and the network. This enables the SIM to build up an interactive exchange between a network application and the end user and access, or control access to, the network. The SIM also gives commands to the handset such as displaying menus and/or asking for user input.

STK is an important API for securely loading applications to the SIM. It allows the mobile operator to create/provision services by loading them into the SIM without changing anything in the GSM handset. One convenient way for loading applications to the SIM is over-the-air via Short Message Service (SMS). Once loaded, applications on the SIM can be activated via various event triggers registered by the application at the STK. Occurrences such as an incoming/outgoing call or SMS message, call duration, and/or location of the mobile can all act as triggers. Control software with the SIM monitors such events and reports activities via SMS to a network based application server. This facilitates smartcard-based value-added services such as mobile prepay and location-based services.

A serious limitation to this technology is the process of up-gradation. Updating STK applications and menus stored on the SIM can be difficult after the customer takes delivery of the SIM. To deliver updates, either the SIM must be returned and exchanged for a new one (which can be costly and inconvenient) or the application updates must delivered over-the-air (OTA) using specialized, optional SIM features. STK has essentially no support for multimedia, only basic pictures. The STK technology has limited independent development support available.

7.6 Mobile PKI

Authentication and Digital Signature in Mobile environment

A PKI enabled mobile solution facilitates Digital Signature and authentication for mobile applications, where transactions can take place directly from a mobile phone. The Mobile phone is used as a device for creation and storage of private credentials of the user. These credentials are then used for authenticating and digitally signing transactions.

The options for enablement of PKI in mobile includes hardware implementations like Cryptographic SIM, Memory card as Cryptographic token and software implementations such as software cryptographic module in Mobile Phone.

Cryptographic SIM based digital signatures are created using a specialized SIM card that contains both the digital signature capability as well as all the functionalities of a normal SIM card. However, a tie-up with the mobile operator is required for enabling this service

In a Memory Card Based Digital Signature, the memory card is a special cryptographic token that has the key generation software embedded in it along with signature creation software. When a user wishes to perform a transaction over the mobile phone he simply needs to insert the memory card and enter the password as in the case of a USB crypto token. Once the password is applied, the private key is used to sign the transaction. There is no memory size restriction as in the case of a SIM card. The memory card is highly portable and can be carried anywhere. The memory card can be detached and kept aside when not made use of whereas the single SIM based cards needs to be inside the phone always.

Software crypto module in mobile phone can also be used for enabling Digital Signatures. Here the facilities are implemented through an Application Toolkit or applet installed on the mobile phone. This software based solution facilitates easier deployment of applications.

Uses of Mobile PKI

PKI enablement on mobile phones will facilitate mobile commerce applications such as banking, payments, etc, whereby transactions can take place directly from the mobile phone anytime, anywhere – wherever mobile based secure transaction is required.

For legally valid transactions carried out from mobile phones, the provisions laid down under the Information Technology (IT) Act, its Rules & Regulations and Guidelines issued by the Controller of Certifying Authorities, must however be complied with. The same are available at http://cca.gov.in

7.7 e-Authentication

Electronic Authentication (or “e-Authentication”) is the process of electronic identification of a user. E-Authentication provides a simple, convenient and secure way for the users to access government services via Internet/mobile. An authenticated identity is linked to the online services delivered by government agencies through the process of “Authorization”. Authorization deals with the permissions or privileges granted to a user to access particular services provided by a system.

e-Authentication helps to build up confidence and trust in online transactions and encourages the use of the electronic environment as a channel for service delivery. In online transactions, data is communicated electronically through internet and mobile services. With the increased incidences of online transactions, there is a need to set up suitable e-authentication processes and solutions after assessing the risks associated with these transactions.

For Mobile Based Applications

For mobile based applications, there are five levels of application sensitivity ranging from Level 0 to Level 4. The Level 0 is the lowest level of application sensitivity whereas Level 4 is the highest. A Level 0 mobile application will not require any form of authentication and will be used for providing public information over a mobile device. All applications will therefore authenticate users using Level 1 authentication by default. Sensitivity of the application should be defined during application development cycle. This would enable the application to call proper authentication scheme at the right time. Application sensitivity will determine the calling of a suitable authentication mechanism from Level 1 through Level 4 at the appropriate stage.

A summary of the five levels is provided below:

Level 0:

This level implies no authentication. The user can avail the government service through various mechanisms such as SMS, USSD (Unstructured Supplementary Service Data), IVR (Interactive Voice Response) etc. using her mobile phone and can access all information that is made available for public use.

Level 1:

This is the basic authentication mechanism using username and password. The user would receive the username & password after successful enrolment in e-Pramaan. The user will receive the password through SMS or print mailer. Aadhaar based authentication involving matching of Aadhaar number with demographics can also be used appropriately for verifying the identity of the users.

Level 2:

At Level 2, a user will prove her identity using username, password and OTP. At the time of accessing a government service, the user will first provide her username and password or Aadhaar number with demographics and will then be prompted to enter the OTP.

Alternate Option (only for smart phones): In this case, the user needs to prove her identity through username and password (or Aadhaar number with demographics) plus the random OTP generated through the OTP Generator (i.e. two factor authentication). The user will be required to download and install an “OTP Generator” from a trusted website (either provided by the government or by an authorised agency).

Level 3:

At Level 3, the user needs to prove her identity through username and password plus a modified SIM or SD/microSD card/other medium containing the user's digital certificate (i.e. through a two factor authentication). Biometrics based verification using the Aadhaar authentication process may also be used at this level.

Level 4 (for biometric enabled phones/devices):

At Level 4, the citizen will prove her identity using a two factor authentication which will necessarily include biometrics as one of the factors while the other factor could either be a soft token (OTP) or a username/password. This is the highest level of authentication security that would be provided to a citizen/internal privilege user (e.g. a department user). For this purpose, the mobile phone of the user should be equipped with a biometric reader in order to capture the fingerprint or iris (as specified by the UIDAI). Biometric verification would be done in accordance with the Aadhaar authentication process.

8. Reference implementation of guidelines through Mobile Seva

DeitY has launched a massive countrywide initiative on mobile governance, called "Mobile Seva", to provide government services to the people through mobile phones and tablets. **Mobile Seva** has been developed by DeitY as the core infrastructure for enabling the availability of public services through mobile devices. Mobile Seva enables the integration of the mobile platform with the common e-Governance infrastructure consisting of State Data Centres (SDCs), State Wide Area Networks (SWANs), State and National Service Delivery Gateways (SSDGs/NSDG). It enables a government department to integrate both web and mobile based services seamlessly and enhances the access to electronic services tremendously leveraging the very high penetration of mobile phones, especially in rural areas. Availability of government-wide shared infrastructure and services enables rapid development and reduced costs for the departments in rolling out mobile based services.

As a part of this initiative, the **Framework for Mobile Governance** was notified in February 2012. The SMS Gateway was operationalized in July 2011. As on date, 1004 Central and State Govt. Departments are using Mobile Seva for providing SMS-based services, and over 90.2 Crore SMS notifications have been sent to citizens for various mobile based services. The most prolific users of the "PUSH SMS" are Department of Agriculture in the central Government, MeeSeva project in Andhra Pradesh and Department of IT in Madhya Pradesh, etc. Citizens can now directly interact with Government Departments through SMS. As on date, 316 public services have been made available to the citizens. The highest number of "PULL SMS" services have been provided by UIDAI, MeeSeva and the Election Commission of India.

These services have been made available through the short-code 166 with the long-term vision of providing all non-emergency public services in the country through this short code.

A Mobile Applications Store (m-App Store) has also been developed by DeitY as part of Mobile Seva. The Mobile Governance Portal and the m-App Store can be accessed at http://mgov.gov.in/. The m-Appstore currently hosts 300 live mobile applications. The live applications can be downloaded and installed free of cost on a mobile phone by any person.

The live m-apps consist of Polling Station Location app for the Election Commission of India that has been used to map polling stations in the country. Another useful m-app is the GIST Hindi language as well other 11 Indian languages' on-screen keyboard driver & editor for Android devices. There is also an application for translating text from English to Hindi and other 11 languages through SMS.

A Mobile Payment Gateway has also been integrated with Mobile Seva which allows a person to make payment for government services through his or her mobile phone. USSD and IVRS based services have also been developed and are currently being piloted.

Mobile Seva is being developed around open standards and cloud-based solutions by DeitY through its organization C-DAC. Mobile Seva has been scaled up for implementation at the national level for meeting the ever-increasing demands from government departments interested in reaching out to the citizens through mobile devices. Citizens can visit http://mgov.gov.in/ for more information.

8.1 SMS Based Service through MOBILE SEVA

Figure 3 depicts a schematic for a typical SMS based service by a government department or an agency through the MOBILE SEVA of DeitY.

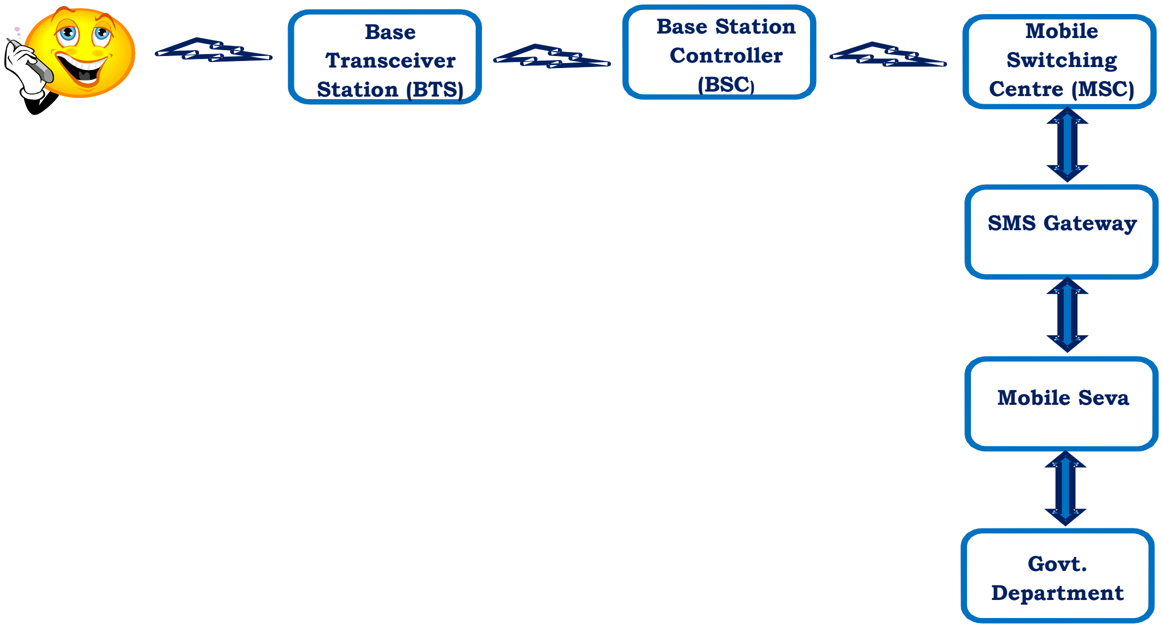

Base Transceiver Station (BTS)
Base Station Controller (BSC)
Mobile Switching Centre (MSC)
SMS Gateway
Mobile Seva
Govt. Department

Figure 3: SMS Based Service through MOBILE SEVA

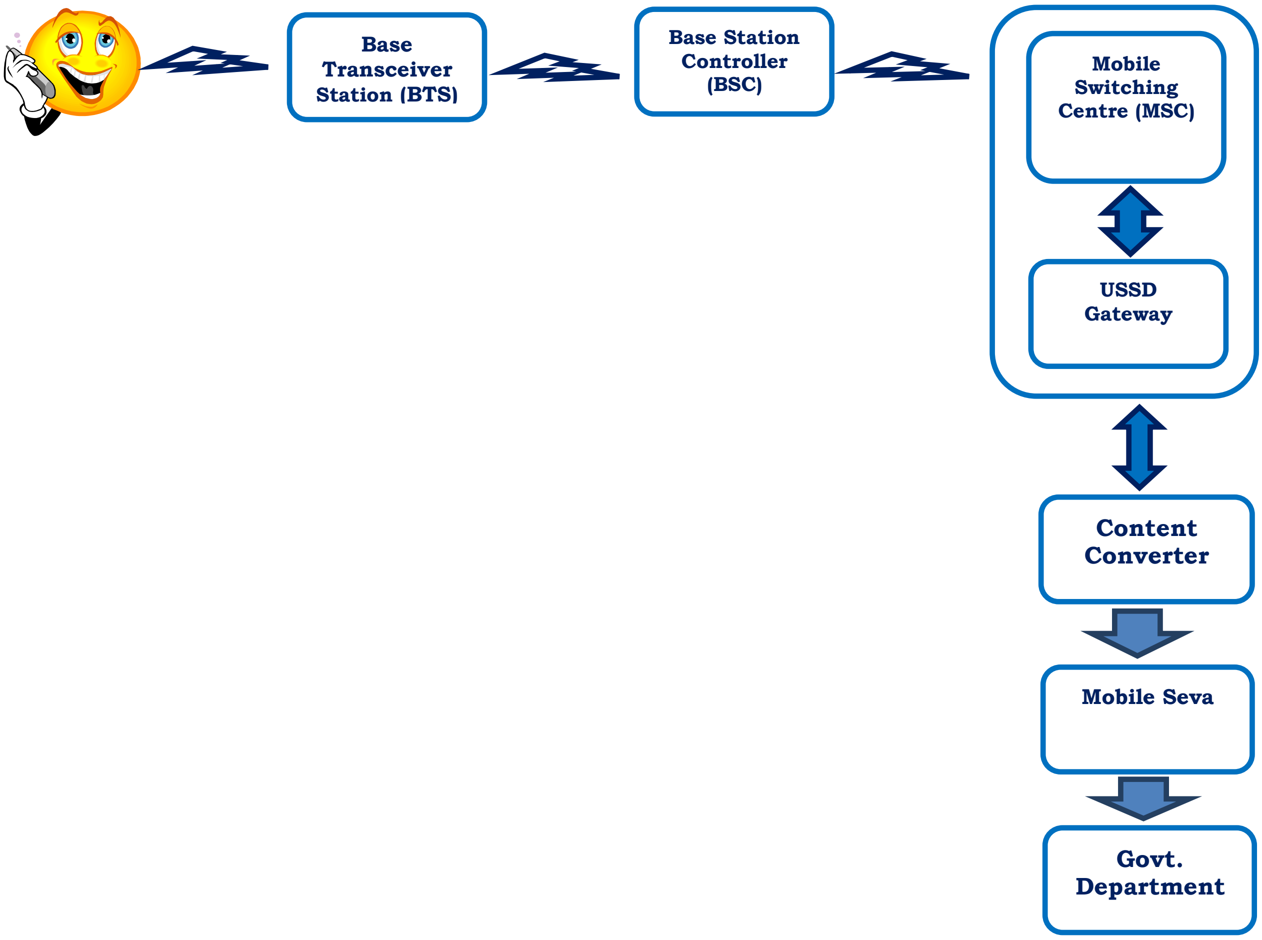
Integration for Pull and Push SMS

Various government departments and agencies can use simple step-by-step procedures for integrating their services for Pull and Push SMS with the MOBILE SEVA. For using the 51969, 166 or 98223166166 short code of MOBILE SEVA for these services, detailed procedures are provided in the "Integration Document for Pull and Push SMS" in Annexure II.

8.2 USSD Based Services through MOBILE SEVA:

Figure 4 depicts a schematic for a typical USSD based service by a government department or an agency through the MOBILE SEVA of DeitY.

Figure 4: *USSD Based Service through MOBILE SEVA*


Base Transceiver Station (BTS)
Base Station Controller (BSC)
Mobile Switching Centre (MSC)
USSD Gateway
Content Converter
Mobile Seva
Govt. Department

The request is sent by User by using pre-designated code where it is forwarded via BTS and BSC to reach MSC. In case of USSD, the MSC access is limited currently to be accessed by Telcos. CDAC, implementing the project plans to keep the SS7 or Sigtran Connectivity Server under their control. The Content server is responsible for creation of menu and constantly outputs menu to the user until it reaches the specific service. Then it is forwarded to MOBILE SEVA which uses the HTTP request to map the Department and sends/serves the request finally the response is forwarded back via MSC+ USSD Gateway, BTS to concerned User.

8.3 IVRS Based Service through MOBILE SEVA

Figure 6 depicts a schematic for a typical IVRS based service by a government department or an agency through the MOBILE SEVA of DeitY.

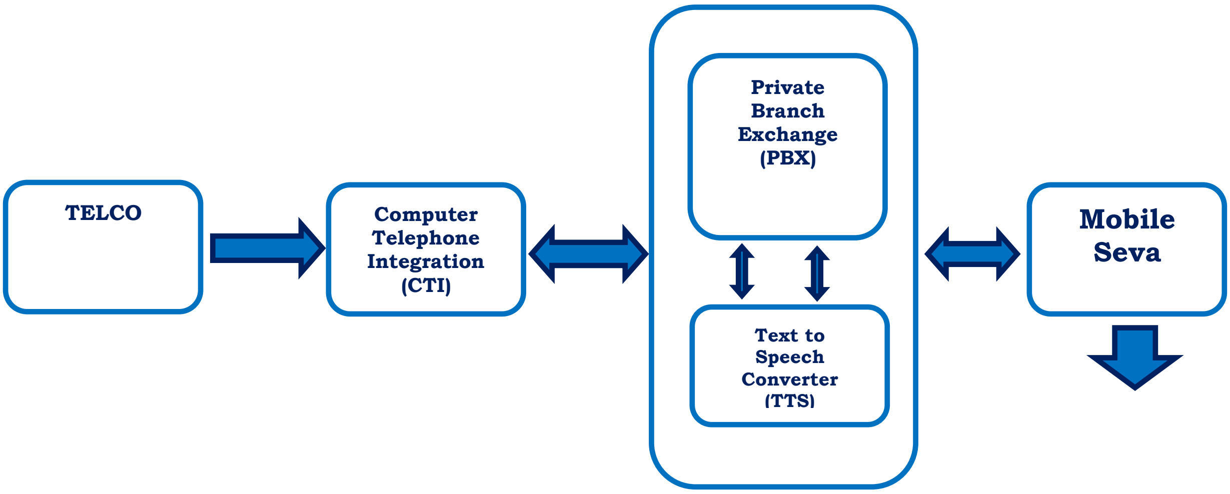

TELCO
Computer Telephone Integration (CTI)
Private Branch Exchange (PBX)
Text to Speech Converter (TTS)
Mobile Seva

Figure 6: IVRS Based Service through MOBILE SEVA

User calls the predefined Number, Telcos forward the request using PRI lines in TDM format and CTI then Converts into TDMOE over Ethernet ports to PBX for routing/dispatching the calls till the exact service is located. The TTS connected is used to offer service in different languages. The once the exact service is identified then HTTP request is sent to MOBILE SEVA and in turn mapped to concerned department to serve the request and send back the response via TTS to the User.

8.4 Mobile Governance Application Store (m-Gov Apps Store):

A mobile applications (m-apps) store has been created by DeitY to facilitate the process of development and deployment of suitable applications for delivery of public services through mobile devices. The m-apps store is integrated platform of MOBILE SEVA and it uses the MOBILE SEVA infrastructure for deployment of such applications. The store is based upon service oriented architecture and cloud based technologies using open standards as far as practicable. This open platform is developed and deployed in conjunction with the MOBILE SEVA for making the additional value added services available to the users irrespective of the device or network operator used by them. Further m-apps store may be divided into two categories one for Govt. centric services another for citizen centric services.

M-Governance application store (http://apps.mgov.gov.in/) hosts the various mobile applications for government services. Any Government departments/Agency can host mobile application on the M-Gov apps store for users to download and start using the services. The Government department's backend needs to be ready for integrating with MOBILE SEVA platform for delivering the services via mobile Application to the user. Applications can also be developed by independent developer or any company, which after testing and verification processes are allowed to host them on the app store. There are different views for the citizens, developers and the administrators. Citizens and developers need to register before they access it. Citizen can download these applications from this App Store on the individual handsets and using these applications they can access government services anytime from anywhere. There are three versions of app store, one for normal web, second for mobile web, and third version will be a native application which will reside on the mobile phone itself.

8.5 Mobile PKI through MOBILE SEVA

Figure 9 depicts a schematic for a typical service by a government department or an agency using mobile PKI through the MOBILE SEVA of DeitY.

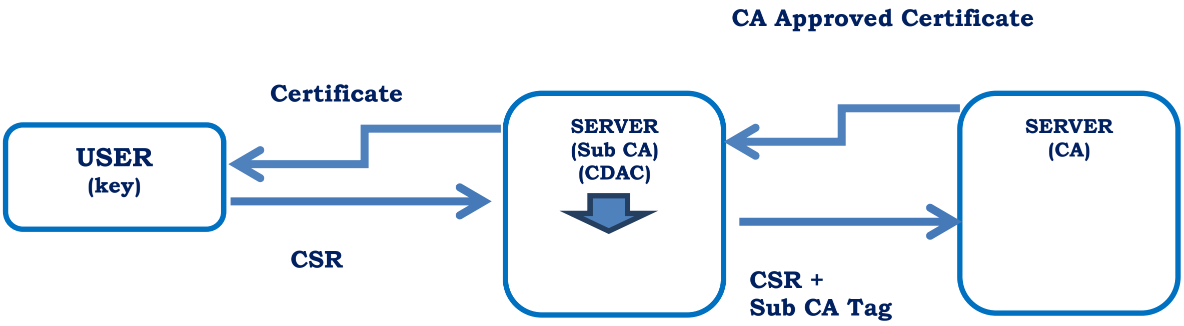


Figure 9: Mobile PKI through MOBILE SEVA

CSR is Certification Signing Request, Using the Public key a CSR is generated. The details and Public key constitues CSR which is forwarded to Sub CA (CDAC) forwards the CSR with Sub CA Tag, authorized by CDAC to CA. CA then approves and issues the Certificate which is sent back to sub CA and forwarded back to User.

The solution will have two components:

1. Certificate Authority (CA) Server
   - Generates certificate for mobile devices
   - Keeps certification revocation list
2. Mobile PKI application
   - Generates public/private key pair
   - Registers public key with CA (After successful registration receives a x.509 certificate from CA)
   - The generated private key and the certificate will be stored on the mobile phone encrypted with SHA2
   - Available on the Mobile Application Store

This application can be used mobile commerce application, to authenticate mobile devices, to digitally sign documents, etc.

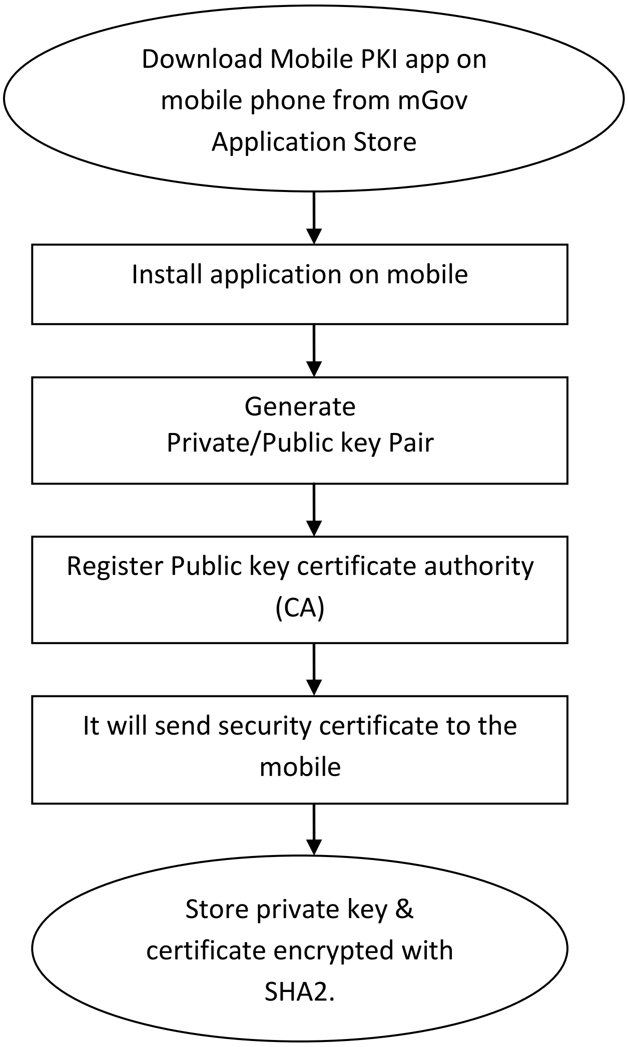

Download Mobile PKI app on mobile phone from mGov Application Store
Install application on mobile
Generate Private/Public key Pair
Register Public key certificate authority (CA)
It will send security certificate to the mobile
Store private key & certificate encrypted with SHA2.

Figure 10: Mobile PKI Solution

Standard Protocols and Specifications for Mobile Seva

For SMS Gateway	: SMPP
For USSD Gateway	: SS7/Sigtran
For IVRS	: PRI Line

9. Mobile Compliant Websites

The mobile compliant website is created specifically for mobile browsing. Web sites of all Government Ministry and Departments shall be made mobile-compliant, using the "One Web" approach. In existing or new mobile compliant websites m dot {m.} may be prefixed. The mobile Web is seen as independent, but not isolated from the traditional Web. Many websites and portals already have their own mobile-friendly versions, offering only the most important information or services in comparison to the traditional sites. Mobile sites can be viewed on traditional browsers and many traditional sites (if simple enough or accessed via smartphone) can be viewed on mobile browsers. But it is recommended to create both versions with corresponding re-directs. Despite the current lack of formalized standards, there are some factors which are increasingly becoming accepted as best practices. The World Wide Web Consortium (W3C) is constantly evolving their Web guidelines. They have now turned their attention towards better mobile website coding and structuring with a mobile Web initiative known as Mobile Web Best Practices (MWBP and MWABP). Creating content (including images, text and beyond) that can be correctly formatted on most phones is the required to deliver public services smoothly for ease of access to users.

9.1 The Challenges of the Mobile Web and Mobile Apps

m-Web and m-Apps does face a number of challenges like cost, digital divide, English language skills, availability of applications in local languages, trust, data overload, m-Technologies, digital inclusion, social factors, regulatory policies and framework . The major challenge confronting m-Web and m-Apps is the use of heterogeneous operating systems on mobile devices, leading to redevelopment of m-App. m-Technologies must be interoperable across the different platforms. Being small and portable, mobile devices can be easily stolen or lost, putting the data stored in them at peril. Sending vital information over mobile is not secure as the mobiles are easily traceable through surveillance system so security and privacy are also considered to be the major obstacles for m-Governance applications.

As mentioned, navigation on a mobile site also poses quite a challenge. As most handsets only have a basic alphanumeric keyboard and no mouse function, excess scrolling and typing makes it difficult for the user. Screen sizes vary between phone models and the browser used can see the same site being rendered differently on identical phone models, making mobile Web development a tricky task. Beyond navigational and formatting concerns, there are many different types of connections to the mobile Web and service providers around the world, adding even more uncertainty to the medium. Mobile Web designers always need to bear varying bandwidth speeds and costs in mind. Some have super-quick connections with smartphones and full QWERTY keyboards, while most are browsing on the equivalent of an obsolete dial up connection. Thus, keeping mobile sites trim and streamlined is vital. The mobile users entering into the department site will have to make sure that they are directed to the mobile version. The mobile version should also ensure that about varing screen size, ensuring images are automatically resized according to the phone model. Excessive navigation or menus needs to be avoided and ensure that the fonts and colors used are supported.

The department of Electronics and Information Technology (DeitY) has formulated a policy framework for mobile governance which looks at ways in which mobile devices can be used to provide public services especially in rural areas. As per the policy framework all government websites has to be mobile compliant.

No matter the size of Department and its operation, optimizing the website for the mobile revolution provides users with a superior mobile experience which would enable them easy access to avail public services on mobile devices.

9.2 W3C Standards for Mobile Web and Mobile Apps

Mobile compliant websites must follow following technologies developed w.r.t. W3C Standards:

Graphics, Multimedia, Device Adaptation, Forms, User interactions, Data storage, Personal Information Management, Sensors and hardware integration, Network, Communication and Discovery, Packaging, Performance & Optimization.

ANNEXURE I

MOBILE SEVA: Frequently Asked Questions (FAQs)

1 What are the objectives of Mobile Seva?

Mobile Seva is an innovative initiative aimed at mainstreaming mobile governance (m-Governance) in the country. It aims to leverage wireless and new media technology platforms, mobile devices and applications for delivery of public information and services to all citizens and businesses. It aims at widening the reach of, and access to, public services to all citizens in the country, especially in the rural areas by utilizing the much greater penetration of mobile phones in the country. It also leverages the innovative potential of mobile applications in providing public services. The overall strategy aims at making India a world leader in harnessing the potential of mobile governance for inclusive development.

Mobile Seva provides a complete ecosystem for enabling the delivery of various electronic government services through mobile devices in an efficient manner with minimum effort for the participating Government departments and agencies. Mobile Seva will also help in enhancing the interoperability of mobile-based services among various Government departments and drastically reduce the cost and time for development and deployment of applications for m-governance services.

2 What are the functionalities that are available on Mobile Seva?

Mobile Seva provides all possible mobile based channels for service delivery, e.g., SMS, USSD, IVRS and mobile applications. It will also provide location based services (LBS) and cell broadcasting services (CBS). It provides integrated hardware and software to test and deploy the m-governance applications. It provides various mobile based options for the citizens to apply for and receive public services through their mobile devices irrespective of the network operators to whom they've subscribed. It will also have an integrated system for delivering the IVR based services through mobile and fixed telephone. Mobile Seva will support the delivery of both voice and data services and content in a network and device independent manner to the extent possible and feasible. It will also offer shared tools like data collection, helpdesk services, APIs, SDKs to the Government departments and agencies that wish to deploy mobile applications for public services. It will also have a provision for metered access so that various agencies and partners of Mobile Seva can account for any fee based services based upon their actual delivery.

3 Who own Mobile Seva?

Mobile Seva is owned by the Department of Electronics and Information Technology (DeitY), Government of India. The technical implementation of Mobile Seva is being done by the Centre for Development of Advanced Computing (C-DAC), a DeitY organisation.

4 How will Mobile Seva account for fee-based services?

Mobile Seva has a provision for metered access so that various agencies and partners of Mobile Seva can account for the fee-based services.

5 Who will be responsible for notification of the guidelines for mobile applications?

The guidelines for mobile applications will be formulated and notified by the Department of Electronics and Information Technology, Government of India.

6 Who will be responsible for service fulfilment?

The responsibility for service fulfilment shall lie with the respective Government department or agency. Mobile Seva will only serve as the channel between the citizen and the participating Government department or agency.

7 Can the participating department have an alternate mobile initiative?

Any Government department or agency at the central or state or local level interested in providing mobile services would be encouraged to provide its services through Mobile Seva to avoid duplication of infrastructure.

8 What are the various delivery channels envisaged to be supported by Mobile Seva?

Mobile Seva supports the following delivery channels for development and deployment of mobile-based applications for public services. As the mobile-based technologies are constantly evolving, more channels may be added in future as the need arises.

- SMS (Short Message Service)
- Mobile applications based on SMS and IP
- IVR (Interactive Voice Response)
- WAP (Wireless Application Protocol)
- USSD (Unstructured Supplementary Service Data)
- CBC (Cell Broadcast)
- SIM Toolkit (STK)/Dynamic STK, 3G-Video
- Others (WiFi/ WLan etc.)

9 Is e-Governance a prerequisite for m-Governance?

Though m-governance may be seen as an extension of e-governance services, existence of e-governance services is not a prerequisite for deployment of m-governance services. The mobile-based innovative public services to be deployed under the ambit of this framework and implementation strategy are aimed at extending the reach of electronic public services to all citizens, especially those who are unable or unwilling to access public services through internet or those who simply prefer to use mobile devices. Government departments and agencies can directly start providing m-governance services through Mobile Seva though they may not be currently offering any e-governance services.

10 What are the steps to be followed by a Government department to register services for m-governance?

Government departments and agencies can directly register for Mobile Seva through the eSMS option on the Mobile Seva portal at: https://services.mgov.gov.in/. Please refer to 'Department Services' tab on the Mobile Seva home page for further details. DeitY and C-DAC shall provide all the necessary guidance and assistance to all Government departments and agencies to develop mobile based applications for delivering their services.

11 Who will be responsible for creation of mobile-ready content?

The concerned Government departments and agencies will be responsible for creating and updating mobile-ready content for their respective services.

12 What steps will DeitY take to promote the m-Governance initiative?

DeitY, C-DAC,NIC or other designated agencies, will undertake awareness creation and capacity building exercises for according greater visibility to the mobile governance initiative amongst various stakeholders and potential beneficiaries across Government, industry, and civil society and citizens.

ANNEXURE II

Reserve Bank of India

Mobile Payment in India - Operative Guidelines for Banks

1. Introduction

1.1 With the rapid growth in the number of mobile phone subscribers in India (about 261 million as at the end of March 2008 and growing at about 8 million a month), banks have been exploring the feasibility of using mobile phones as an alternative channel of delivery of banking services. A few banks have started offering information based services like balance enquiry, stop payment instruction of cheques, record of last five transactions, location of nearest ATM/branch etc. Acceptance of transfer of funds instruction for credit to beneficiaries of same/or another bank in favor of pre-registered beneficiaries have also commenced in a few banks. Considering that the technology is relatively new and due care needs to be taken on security of financial transactions, there has been an urgent need for a set of operating guidelines that can be adopted by banks.

1.2 For the purpose of these Guidelines, “mobile payments” is defined as information exchange between a bank and its customers for financial transactions through the use of mobile phones. Mobile payment involves debit/credit to a customer’s account’s on the basis of funds transfer instruction received over the mobile phones.

1.3 Providing the framework for enabling mobile payments services to banking customers would generally involve the collaboration of banks, mobile payments service providers and mobile network operators (MNOs). The service can also be provided as a proximity payment system, where the transactions are independent of the MNOs. In mobile payment systems, the banks provide the basic service framework, ensure compliance to KYC/AML norms, creates a risk management and mitigation framework, and ensures settlement of funds. The mobile payments service providers are intermediaries for providing the technology framework for the implementation of the mobile payments services. The mobile network operators provide the telecom infrastructure and connectivity to the customers. Their role is limited to providing the SMS/WAP/GPRS/USSD/NFC GSM or CDMA voice and data services connectivity and in hosting the certain technology solutions like USSD. In a Non-MNO based systems, proximity or contactless channels like IRDA, RFID, Optical, NFC, etc. are used for communication between POS and the mobile phone of the customer.

1.4 As a first step towards building a mobile payment framework in India, these guidelines are meant only for banking customers – within the same bank and across the banks. It would be the responsibility of the banks offering mobile payment service to ensure compliance to these guidelines.

1.5 A brief description of the regulatory framework for mobile payments in a few countries is given at Annexure II-A.

2. Regulatory & Supervisory Issues

2.1 Only such banks which are licensed and supervised in India and have a physical presence in India will be permitted to offer mobile payment services to residents of India.

2.2 The services should be restricted to only to bank accounts/ credit card accounts in India which are KYC/AML compliant.

2.3 Only Indian Rupee based services should be provided.

2.4 Banks may use the services of Business Correspondents for extending this facility, to their customers. The guidelines with regard to use of business correspondent would be as per the RBI circular on Business correspondents issued from time to time.

2.5 The guidelines issued by RBI on ‘Risks and Controls in Computers and Telecommunications’ vide circular DBS.CO.ITC.BC. 10/ 31.09.001/ 97-98 dated 4th February 1998 will equally apply to Mobile payments, since Mobile devices used for this purpose have embedded computing and communication capabilities.

2.6 The RBI guidelines on “Know Your Customer (KYC)” and “Anti Money Laundering (AML)” as prescribed by RBI from time to time would be would be applicable to customers opting for mobile based banking service.

3. Registration of customers for mobile service

3.1 Banks should offer mobile based banking service only to their own customers.

3.2 Banks should have a system of registration before commencing mobile based payment service to a customer.

3.3 There can be two levels of mobile based banking service - the first or basic level in the nature of information like balance enquiry, SMS alert for credit or debit, status of last five transactions, and many other information providing services and the second or standard level in the nature of financial transactions such as payments, transfers and stop payments. The risk associated with the basic level of information services is much less compared to the standard level of actual payment services. Prior registration of the customers would be necessary irrespective of the type of service requested. For the standard level service one time registration should be done through a signed document.

4. Technology and Security Standards

4.1 The technology used for mobile payments must be secure and should ensure confidentiality, integrity, authenticity and non-repudiability. An illustrative, but not exhaustive framework is given at Annexure II-B.

4.2 The Information Security Policy of the banks may be suitably updated and enforced to take care of the security controls required specially for mobile phone based delivery channel.

5. Inter-operability

5.1 When a bank offers mobile payments service, it may be ensured that customers having mobile phones of any network operator should be in a position to request for service. Restriction, if any, to the customers of particular mobile operator(s) may be only during the pilot phase.

5.2 To ensure inter-operability between banks and between their mobile payments service providers, it is recommended that banks may adopt the message formats being developed by Mobile Payments Forum of India (MPFI). Message formats such as ISO 8583 , which is already being used by banks for switching of ATM transactions , may be suitably adapted for communication between switches where the source and destination are credit card/ debit cards/pre-paid cards.

5.3 The long term goal of mobile payment framework in India would be to enable funds transfer from account in one bank to any other account in the same or any other bank on a real time basis irrespective of mobile network a customer has subscribed to. This would require inter-operability between mobile payments service providers and banks and development of a host of message formats. Banks may keep this objective while developing solution or entering into arrangements with mobile payments solution providers.

6. Clearing and Settlement for inter-bank funds transfer transactions

6.1 For inter-bank funds transfer transactions, banks can either have bilateral or multilateral arrangements.

6.2 To meet the long term objective of a nation-wide mobile payment framework in India as indicated at para 5.3 above, a robust clearing and settlement infrastructure operating on a 24x7 basis would be necessary. Pending creation of such an infrastructure on a national basis, banks may enter in to multilateral arrangement and create Mobile Switches / Inter-bank Payment Gateways with expressed permission from RBI.

7. Customer Complaints and Grievance Redressal Mechanism

7.1 The customer /consumer protection issues assume a special significance in view of the fact that the delivery of banking services through mobile phones is relatively new. Some of the key issues in this regard and the legal aspects pertaining to them are given at Annexure II-C.

8. Need for Board level approval

8.1 Banks should get the Mobile payments scheme approved by their respective boards / Local board (for foreign banks) before offering it to their customers. The Board approval must document the extent of Operational and Fraud risk assumed by the bank and the bank's processes and policies designed to mitigate such risk.

8.2 Banks who have already started offering mobile payment service may review the position and comply to these guidelines within a period of three months from issuance of these guidelines.

Annexure II-A

International Experience

There is very little material available on the regulatory frame work for mobile payments by central banks. Although there are a number of research articles available, they refer to the practices available rather than regulatory guidelines. Efforts to collect specific regulatory guidelines, from a few countries where person to person remittance through mobile channel has been implemented, have not been a success. Mobile payment framework in most countries is covered under the General Electronic Banking Guidelines. However, on the website of Consultative Group for Assisting the Poor(CGAP), there are several discussion papers on mobile payments. Examples of Kenya, Philippines, South Africa and Tanzania have been described in great detail. In these countries, cash-in and cash-out for the purpose of remittance is permitted to be done by the distributors of mobile companies. State Bank of Pakistan has also placed a 'Draft policy paper on Regulatory Framework for Mobile Payments in Pakistan' on their website for public comments.

Annexure II-B

Technology and Security Standards

The security controls/guidelines mentioned in this document are not exhaustive. The guidelines should be applied in a way that is appropriate to the risk associated with services provided by the bank through the mobile platform, the devices used, the delivery channels used (SMS, USSD, WAP, WEB, SIM tool kit based, Smart phone application based, IVR, IRDA, RFID, NFC, voice, etc) and the system which processes the mobile transactions and enables the interaction between the customers, merchants, banks and other participants.

2. The mobile payments could get offered through various mobile network operator based channels (SMS, USSD, WAP, WEB, SIM tool kit, Smart phone application based, IVR, voice, etc) and non MNO based proximity or contactless channels (IRDA, RFID, Optical, NFC, etc) and these various mobile channels offer various degrees of security and interaction capability. While the objective of the RBI is to have a fully functional digital certificate based inquiry/transaction capabilities to ensure the authenticity and non-repudiability, given the complexities involved in getting this through all the channels and given the need for enabling mobile payments to facilitate financial inclusion objectives, it is suggested that the banks evaluate each of these channels in terms of security and risks involved and offer appropriate services and transactions. Banks are also advised to provide appropriate risk mitigation measures like transaction limit (per transaction, daily, weekly, monthly), transaction velocity limit, fraud checks, AML checks etc. per channel depending on the nature of the security features, risk perception by the bank offering the services and interaction capabilities.

3. It is suggested that the banks issue a new mobile pin (mPIN). To facilitate the mobile payments mPIN may be issued and authenticated by the bank or by a mobile payment application service provider appointed by the bank. Banks and the various service providers involved in the m-banking should comply with the following security principles and practices with respect to mPIN :

a) Implement a minimum of 4 digit customer mPIN (6 digit mPIN may be the desirable goal)

b) Protect the mPIN using end to end encryption

c) Do not allow the mPIN to be in clear text anywhere in the network or the system

d) Authenticate the mPIN in tamper-resistant hardware such as HSM (hardware security modules)

e) Store the PIN in a secure environment

f) In case of offline authentication, the banks should ensure that a proper process is put in place to positively identify the customer the first time when the service is being enabled. An offline PIN may be used as the authentication parameter with security levels being as strong as in the case of online authentication. The bank may choose to issue its own offline PIN or adopt a customer-defined PIN.

g) A second factor of authentication may be built-in for additional security and as such the second factor can be of the choosing of the bank

4. All transactions that affect an account (those that result in to an account being debited or credited, including scheduling of such activity, stop payments, etc) should be allowed only after authentication of the mobile number and the mPIN associated with it in case of MNO based payment service. In case of Non-MNO based mobile proximity payment, specific static or dynamic identifier should be used as second factor authentication along with mPIN.. Two factor authentication may be adopted even for transactions of information nature such as balance enquiry, mini statements, registered payee details. ,

5. Proper system of verification of the mobile phone number should be implemented, wherever possible. This is to guard against spoofing of the phone numbers as mobile phones would be used as the second factor authentication. It may also be suggested but not mandatory, that either card number or OTP (one time passwords) be used as the second factor authentication rather than the phone number.

6. Proper level of encryption should be implemented for communicating from the mobile handset to the bank's server or the server of the mobile payments service provider, if any. Proper security levels should be maintained for transmission of information between the bank and the mobile payments service provider. The following guidelines with respect to network and system security should be adhered to:

a) Use strong encryption for protecting the sensitive and confidential information of bank and customers in transit

b) Implement application level encryption over network and transport layer encryption wherever possible.

c) Establish proper firewalls, intruder detection systems (IDS), data file and system integrity checking, surveillance and incident response procedures and containment procedures.

d) Conduct periodic risk management analysis, security vulnerability assessment of the application and network etc at least once in a year.

e) Maintain proper and full documentation of security practices, guidelines, methods and procedures used in mobile payments and payment systems and keep them up to date based on the periodic risk management, analysis and vulnerability assessment carried out.

f) Implement appropriate physical security measures to protect the system gateways, network equipment's, servers, host computers, and other hardware/software used from unauthorized access and tampering. The Data Centre of the Bank and Service Providers should have proper wired and wireless data network protection mechanisms.

7. The dependence of banks on mobile payments service providers may place knowledge of bank systems and customers in a public domain. Mobile payment system may also make the banks dependent on small firms (i.e mobile payment service providers) with high employee turnover. It is therefore imperative that sensitive customer data, and security and integrity of transactions are protected. It is necessary that the mobile payments servers at the bank’s end or at the mobile payments service provider’s end, if any, should be certified appropriately, say through a PCI DSS certification or in compliance with each participant banks security guidelines. In addition, banks should conduct regular information security audits on the mobile payments systems to ensure complete security. Further, if a mobile payments service provider aggregates and processes transaction, including verification of mPINs, additional security measures such as a Hardware Security Module (HSM) must be deployed over and above link encryption to ensure that mPIN data is protected adequately.

8. It is recommended that for channels such as WAP and WEB which do not contain the phone number as identity, a separate login ID and password be provided as distinct from the internet banking either by bank or the payment service provider. It is recommended that Internet Banking login ids and passwords may not be allowed to be used through the mobile phones. Allowing Internet banking login id and password usage on the mobile phone may compromise their usage on the Internet banking channel. This restriction may be communicated to the customers while offering mobile payments service. However, Internet Banking login ids and passwords can allowed to be used through the mobile phones provided a) https connectivity through GPRS is used and b) end to end encryption of the password and customer sensitive information happens.

9. Plain text SMS is the simplest form of communication through mobile phones, but is vulnerable to tampering. As long as there is a second level of check on the details of the transaction so as to guard against data tampering this mode of communication can be used for financial messages of micro payment transactions (say about rupees One thousand five hundred) and repetitive utility bill payment transactions (say not exceeding rupees two thousand five hundred).

Annexure II-C

Customer Protection Issues

Considering the legal position prevalent, there is an obligation on the part of banks not only to establish the identity but also to make enquiries about integrity and reputation of the prospective customer. Therefore, even though request for opening a savings / current account can be accepted over Mobile Telecommunication, these should be opened only after proper introduction and physical verification of the identity of the customer using prevalent KYC norms.

2. From a legal perspective, security procedure adopted by banks for authenticating users needs to be recognized by law as a substitute for signature. In India, the Information Technology Act, 2000, provides for a particular technology as a means of authenticating electronic record. Any other method used by banks for authentication should be recognized as a source of legal risk. Customers must be made aware of the said legal risk prior to sign up.

3. Under the present regime there is an obligation on banks to maintain secrecy and confidentiality of customers‘ accounts. In the mobile payments scenario, the risk of banks not meeting the above obligation is high on account of several factors. Despite all reasonable precautions, banks may be exposed to enhanced risk of liability to customers on account of breach of secrecy, denial of service etc., because of hacking/ other technological failures. The banks should, therefore, institute adequate risk control measures to manage such risks.

4. As in an Internet banking scenario, in the mobile payments scenario too, there is very limited or no stop-payment privileges for mobile payments transactions since it becomes impossible for the banks to stop payment in spite of receipt of stop payment instruction as the transactions are completely instantaneous and are incapable of being reversed. Hence, banks offering mobile payments should clearly notify the customers the timeframe and the circumstances in which any stop-payment instructions could be accepted.

5. The Consumer Protection Act, 1986 defines the rights of consumers in India and is applicable to banking services as well. Currently, the rights and liabilities of customers availing of mobile payments services are being determined by bilateral agreements between the banks and customers. Considering the banking practice and rights enjoyed by customers in traditional banking, banks' liability to the customers on account of unauthorized transfer through hacking, denial of service on account of technological failure etc. needs to be assessed and banks providing Mobile payments should consider insuring themselves against such risks, as is the case with Internet Banking.

6. Bilateral contracts between the payee and payee's bank, the participating banks and service provider and the banks themselves will form the legal basis for mobile transactions. The rights and obligations of each party must be clearly defined and should be valid in a court of law. It is likely that there will be two sets of contracts; one would be a commercial contract between service providers

and the second, a contract between the customer and the bank, to provide a particular service/ s. At all time, legal obligations of each party must be made clear through these contracts.

7. Banks must make mandatory disclosures of risks, responsibilities and liabilities of the customers in doing business through Mobile phone, through a disclosure template on their websites and/or through printed material.

8. The existing mechanism for handling customer complaints / grievances may be used for mobile payment transactions as well. However, the technology is relatively new, banks offering mobile payment service should set up a help desk and make the details of the help desk and escalation procedure for lodging the complaints, if any public on their websites. Such details should also be made available to the customer at the time of sign up.

9. In cases where the customer files a complaint with the bank disputing a transaction, it would be the responsibility of the service providing bank, to address the customer grievance. Banks may formulate chargeback procedures for addressing such customer grievances.

10. Banks may also consider covering the risks arising out of fraudulent/disputed transactions through appropriate insurance schemes.

11. The jurisdiction of legal settlement would be within India.

ANNEXURE III

MOBILE SERVICES DELIVERY GATEWAY SPECIFICATIONS:

The following are the interoperability standards that have been developed as part of the Gateway project. The Gateway Service Provider (GSP) is required to understand these standards in its entirety and implement the NSDG solution in compliance with these standards.

1. Interoperability Interface Protocol (IIP)
2. Interoperability Interface Specifications (IIS)
3. Inter-Gateway Interconnect Specifications (IGIS)
4. Gateway Common Services Specifications (GCSS)

The interoperability standards are currently being validated for approval by the e-Governance Standards Body constituted by the GoI. The sections below provide an outline of the interoperability standards. The standard documents themselves are a part of the RFP documentation.

1. **INTEROPERABILITY INTERFACE PROTOCOL (IIP)**

E-Governance infrastructure is necessarily a distributed one and there are a multitude of participants to this infrastructure. The communication between some of the key participants is critical to hold this infrastructure together need to be specified and standardized. The objective of Interoperability Interface Protocol (IIP) and Interoperability Interface Specification (IIS) is to standardize on the protocol and to specify the interface nature for this communication to take place.

IIP is the communication protocol that the Service Access Providers, e-Governance Gateway and the Service Providers need to comply with. This protocol is divided into two parts, one part targeted towards the Service Access Providers and one for the Service Providers. E-Governance Gateway as the infrastructure needs to support both the interfaces.

IIP is an asynchronous request-poll-retrieval protocol, with provisions for synchronous communication, which supports requests to be sent and receive a response through a polling mechanism or synchronously. The foundation of the protocol is based on message types and context based processing of messages. There are mechanisms for sending a request, communicating acknowledgements, querying the state of a request, sending and communicating responses and to handle error situations. The message types supported by this protocol are listed below:

- Submit Request - Used to send an service request
- Submit Acknowledgement - Used to acknowledge submission requests

- Submit Poll - Used for polling for responses
- Submit Response - Used to package the service response
- List Request - Used for querying submission state
- Delete Request - Used for ending a submission session
- Delete Response - Used as an indicator for submission session ending
- Submit Error - Used for responding to errors

Exchange of IIP compliant messages is intended to be the primary mode of communication between the Service Access Providers and the e-Governance Gateway as well as between the Service Providers and e-Governance Gateway. It is to be noted above that not all messages are required to be supported by the Service Access Providers and the Service Providers. Some of the above messages are mandated to be supported by the Service Access Providers and some for the Service Providers.

IIP provides the interoperable interface for communication and all the IIP messages are XML based, therefore readily usable by any application. This interface is the key for success of e-Governance Gateway.

2. INTEROPERABILITY INTERFACE SPECIFICATIONS (IIS)

IIP provides the protocol, the message formats and the associated semantics of the messages. However, it does not address the issues of the precise exchange of this information through a technology interface. Interoperable Interface Specification (IIS) address this issue. IIS provides the technological specification for exchanging of the IIP compliant message. To this end IIS provides the following:

- Mapping of the IIP message to a carrier protocol, SOAP
- Provides guidelines for messaging, in terms of message size etc.
- Provides facilities for optimization, through batching mechanism etc.

IIS compliments IIP by translating the message exchange into a viable form of messaging mechanism, such that optimization can be achieved by the implementing application. In terms of carrier protocol, IIS follows SOAP, as standardized by W3C, such that wide industry support is available in forms of ready libraries and implementations. IIS is always used in conjunction with IIP; therefore it is uniformly applicable to the Service Access Providers, Service Providers and e-Governance Gateway.

3. INTER-GATEWAY INTERCONNECT SPECIFICATIONS (IGIS)

The e-Governance Gateway infrastructure under various administrations in India will form a hierarchical constellation of which every state and centre Gateway will be a part. However, for this constellation to be realized and successfully operational there needs to be a set of predefined guidelines and standards, which will govern various aspects of the constellation, such as its structure, behavior and policy. The IOI Gateway Interconnect Specification (IGIS) is targeted towards providing such a comprehensive documentation of all aspects of the Gateway Constellation. The primary aim of this standard is to provide the specifications and protocols required for construction of the Gateway Constellation. In this endeavor, the document provides specifications at the following levels:

- Gateway Constellation Structure
- Service Resolution and Service Information Propagation
- Operational Guidelines for Gateway Constellation
- Gateway Interconnect Protocol (GIP)

This specification defines the structure of the Gateway Constellation, the communication mechanisms between various gateways in the constellation, facilities to propagate a service request to its required destination and the policy guidelines applicable to each of the participating gateways in the constellation and the constellation as a whole. This specification is intended to provide the basis on which the Gateway Constellation will be realized. The specification and its associated protocol (s) may be realized with the help any suitable technology and means. In effect, this specification is a technology neutral specification, guideline and protocol enumeration for the Gateway Constellation.

Conformance to IGIS is required by any Gateway that needs to be a part of the Gateway Constellation and is therefore mandated for all state level and centre level Gateways.

4. Gateway Common Services Specification (GCSS)

These specifications are a compilation of a common set of services for NSDG Gateway. These services are considered generic enough in nature, such that they required by more than one government department and Service Access Providers. The generic nature of the services warrant their existence at NSDG Gateway Level, such that substantial reuse of these services can be achieved and individual applications in the eGovernance space of India (present and future) can are spared, metaphorically, the reinvention of the wheel. The set of service specifications contained in this document is expected to expand over time as and when new generic services are integrated into the eGovernance framework of India, therefore, this document intends to serve as the single and authentic source for all such service specifications and undoubtedly a living document, which shall witness many updates and augmentations.

ANNEXURE IV

List of Abbreviations

AML	Anti Money Laundering
CDMA	Code Division Multiple Access
GPRS	General Packet Radio Service
GSM	Global System for Mobile
IDS	Intruder Detection System
IRDA	Infrared Data Association
ISO	International Standards Organization (Sometimes also written as International Organization for Standardization)
IVR	Integrated Voice Response
KYC	Know Your Customer
MNO	Mobile Network Operator
mPIN	Mobile Personal Identification Number
MPFI	Mobile Payment Forum of India
NFC	Near Field communication.
OTP	One Time Password
PCI-DSS	Payment Card Industry Data Security Standard
PIN	Personal Identification Number
RFID	Radio Frequency Identification
SIM	Subscriber Identity Module
SMS	Short Messaging Service
USSD	Unstructured Supplementary Service Data
WAP	Wireless Application Protocol
IMPS	Immediate Mobile Payment System

ANNEXURE V

Future Options/Technologies

Converged Mobile Handset (CMH) and Unlicensed Mobile Access (UMA)

Converged Mobile Handset (CMH) comprising advanced PC functions will be ubiquitous in future.

A single cordless handset which routes calls and data packets over fixed-line broadband networks when they are at home, but switches seamlessly over to a mobile network when they are out. It is based on a technology called Unlicensed Mobile Access (UMA), which lets users make mobile calls using their own Wi-Fi or Bluetooth systems and broadband connections.

Mobile Intelligent Agents (MIA)

Mobile Intelligent Agents (MIA) will migrate from host to host automatically in a network based on location and time to implement various m-Gov Apps efficaciously and handily.

Seamless handover is required in VoIP mobility services in order to limit the period of the service disruption experienced by a MN when moving between different IP subnets. Seamless handover method involves sending multiple copies of the mobile agents to potential MN locations of movement for early authentication. Both VPN and multi-homing techniques play an important role in the reduction of the handover delay and packet loss ratio.

Ultra Wide Band (UWB)

Use of high-end technology in Ultra Wide Band (UWB) will provide the proper utilization of bandwidth and nanotechnology can result in less power consumption, more memory, reduced size and high speed for m-Devices.

Ultra-wideband is a radio technology which may be used at a very low energy level for short-range, high-bandwidth communications using a large portion of the radio spectrum. This method is used in wireless networking to achieve high bandwidth connections with low power utilization. Ultra-wide band wireless radios send short signal pulses over a broad spectrum. For example, a UWB signal centered at 5 GHz typically extends across 4 GHz and 6 GHz. This wireless communications technology can currently transmit data at speeds between 40 to 60 megabits per second and eventually up to 1 gigabit per second.

Mobile Cloud Computing & Virtualization

Development and deployment of cloud apps for mobile devices, to ensure the cloud enabled services using mobile technologies.

Mobile virtualization is a technique by enabling the multiple operating systems run simultaneously on a mobile device. Techniques like Xen ARM are in the process of development of these features. Mobile cloud and other remote computing models provisions constraint-less computing to these tiny devices.

Fifth Generation (5G) technology

Fifth Generation (5G) technology will provide internet speed of 10 Gigabit per second, which is 100 times faster than the mobile technology used these days.

ANNEXURE VI

References

1. https://www.negp.gov.in/

2. http://deity.gov.in/content/draft-electronic-delivery-services-bill-2011

3. http://www.trai.gov.in/WriteReadData/PressRealease/Document/PR-TSD-Oct--13.pdf

4. https://mgov.gov.in/index.jsp

5. http://www.3gpp2.org/public_html/specs/CS0015-0.pdf

6. http://www.3gpp2.org/public_html/specs/X.S0065-0_v1.0_20120505.pdf

7. http://www.w3.org/Mobile/Specifications

8. http://www.w3.org/html/wg/drafts/html/master/Overview.html

9. http://www.tiresias.org/research/guidelines/telecoms/ivr.htm

10. http://mobileactive.org

11. http://mobileactive.org/howtos/mobile-phones-data-collection

12. http://www.idc.com/getdoc.jsp?containerId=prUS23946013

13. http://www.w3.org/Mobile/mobile-web-app-state/

14. http://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=1365

15. http://www.uniphore.com/mobility-solutions/mobile-wallet.html

16. S.K. Katara, and P.V. Ilavarasan, “Mobile Technologies in e-Governance: A framework for implementation in India”, 7th International Conference on Theory and Practice of Electronic Governance (ICEGOV2013), Seoul, Republic of Korea, ACM Press.