Mobile e-Governance Services

Mobile e-Governance services is an integration technology. It best demonstrates its value when integrating heterogeneous systems because it supports many kinds of programming languages, run times, and networks. When there is a need to connect applications from incompatible environments, the stage is set for Mobile e-Governance services.

VS RAGHUNATHAN
Senior Technical
Director, NIC Chennai
raghunathan.vs@nic.in

R RAMESH
Technical Director, NIC
Tamil Nadu
rramesh@nic.in

Edited by **R. Gayatri**

The mobile computing environment poses several challenges to those who offer services in terms of operating system, browser environment, connectivity, Geo-reference, security etc. The services that are offered over the mobiles can be classified into online and offline services. Online services are synchronous and demand continuous connectivity. Offline communications are asynchronous and use the connectivity whenever available. The mobile browser based services are online and connects to the website and services that are offered on internet. SMS, One-Time-Password (OTP) etc. are offline services. Open-X-data, mobile client programs such as midlets, android applications, iPhone applications etc. can be programmed to work both online and offline.

SMS

The text messages such as SMS is being used in variety of ways to confirm to the user about the service availability, status of the service, credit/debit details, service acknowledgments, reference links etc. The citizen application can incorporate SMS interface through a local modem or through the SMS gateway. The local modem solutions are limited in terms of message handling, queuing, scalability, maintainability, both push and pull handling etc. Open source solutions such as Kannel SMS gateway solutions have been implemented at the collectorate, high-court level by NIC in many states. The preferred way of incorporating SMS services is through the SMS gateway and NIC offers the SMS gateway solution. NIC facilitates SMS traffic between all service providers and mobile subscribers, including mission-critical messages, SMS for enterprises, content delivery etc.. Considering SMS messaging performance and cost, as well as the level of messaging services, SMS gateway provides aggregators or SS7 providers. The Central or State Government department can register themselves with NIC SMS gateway and integrate the push/pull messages as per requirement in their applications. This has been extensively used in variety of applications at the central and state level with the technical support from NIC.

ONE TIME PASSWORD

One-time password (OTP) is a password that is valid for only one transaction or authentication session and expires after the defined time period. OTP is not vulnerable for reply attacks as they are not valid after the short period defined. OTP has open standards like

HOTP (HMAC-based One Time Password algorithm; **IETF-RFC 4226**) from Initiative For Open Authentication (OATH).

TOTP (Time-based One-time Password Algorithm; **IETF-RFC**) an extension of HOTP to support time based moving factor. This is also from OATH.

OTP technology can be used in combination with the usual password based authentication to provide strong authentication, in this case two factor authentication.

Mobile-OTP is a free Open Source based "strong authentication" solution for java capable mobile devices like phones or PDAs. The solution is based on time synchronous one time passwords. It consists of a client component and a server component. The mobile client generates one time

passwords by hashing the following items using MD5:

- the current epoch-time in a 10 second granularity
- the 4-digit PIN that a user enters
- a 16-hex-digit secret that has been created when the device was initialized (Init-Secret)

When entering a PIN, the mobile client displays the first 6 digits of the MD5-hash. This is the One Time Password. The One Time Password can be verified by the server, as the server also knows the current time, Init-Secret and PIN of the user. To compensate time differences, the server will accept passwords from 3 minutes in the past to 3 minutes in the future. In addition, different time offsets can be specified for each user on the token and/or the server. Each password will be accepted only once. After 8 successive failed authentication attempts a user gets locked out. Authentication is based on two factors: a PIN known by the user and the Init-Secret stored on the mobile device.

Applications implementing OTP can thwart authentication token reply attacks and password sniffers.

ONLINE MOBILE SERVICES

Online mobile services are mostly enabled through the mobile enabled web-sites. The guidelines for development of rich and dynamic mobile web applications can be obtained from http://www.w3.org/TR/mwabp/. The basic principles of mobile web applications recommended by W3C are

- **Set Users Free**
  - Ensure the user is informed about use of personal and device information
  - Enable automatic sign-in
  - Offer users a choice of interfaces
  - Don't change focus when dynamically updating page sections
- **Design for flexibility**
  - Design for multiple interaction methods
  - Ensure text flows
  - Prefer server-side detection where possible
  - Use client-side detection when necessary
  - Use device classification to simplify content adaption
  - Support a non-JavaScript variant if appropriate
- **Remember web principles**
  - Replicate local data
  - Ensure consistency of state between devices
  - Do not execute unescaped or untrusted JSON data
  - Use fragment Ids to drive application view
- **Spare the network**
  - Use transfer compression
  - Cache resources by fingerprinting resource references
  - Cache AJAX data
  - Minimize external resources
  - Avoid redirects
  - Optimize network requests
  - Use cookies sparingly
- **Exploit mobile-specific features**
  - Make telephone numbers click-to-call
  - Consider mobile-specific technologies for initiating web applications
  - Use the meta view-port element to identify the screen size
  - Use appropriate client-side storage
- **Optimize response time**
  - Aggregate static images into a single composite resource (sprites)
  - Include background images inline in CSS
  - Keep DOM size reasonable
  - Minimize perceived latency
  - Optimize for application start-up time

MOBILE CLIENT PROGRAMS:

Mobile client programs need to use the best practices recommended by W3C for online applications. However there are few challenges while offering the client programs they are Multiple platforms, Mobile specific variations for features and limitations, Client-side version management and deployment.

Care should be taken when implementing mobile web services because only a subset of the API is supported by the mobile Web services specification

The Mobile client has to be developed for multiple platforms such as Nokia's Symbian, Google's Android, Apple's iOS, RIM's BlackBerry OS, Microsoft's Windows Phone, Linux, HP's webOS, Samsung's Bada, Nokia's Maemo and MeeGo. Java Platform, Micro Edition, or Java ME, is a Java platform designed for mobile phones (especially feature phones) and set-top boxes. Java ME was formerly known as Java 2 Platform, Micro Edition (J2ME).

Java ME technology consists of three elements namely configurations, Profiles and optional packages. The configuration for small devices (less capable) are called Connected Limited Device Configuration (CLDC) and for more capable devices the configuration is known as Connected Device Configuration (CDC).

It is always preferable to have the client programs which needs less revisions on the client side as frequent updates on the client side is not rec-

Mobile Client Programs

ommended. This can be achieved by consuming services for every requirement from the server-side so that the variants are managed at the server-side instead of altering the client-program. Preferably REST services can be used. If the client needs to be secured, a client serialization with the IMEI (International Mobile Equipment Identity) number of the device is recommended so that the client program does not work on other devices.

Mobile client programs can be written for both online and offline use. Open source solutions such as openXdata for data collection is widely used which supports low-cost mobiles, includes visual designer and supports multimedia and GPS. Location based services are possible using the GPS data. One can start downloading from ***http://www.openxdata.org/demo*** and start experiencing this solution on their low-cost mobile. Only requirement is the Java enabled mobile and GPRS/3G connectivity. This is widely used for location based survey/activity record needs.

In the offline mode the application can collect data and the data can be send to the server using SMS or via Internet using a Desktop intermediate. Continuous network coverage is not required for offline applications.

As the mobile camera can be used for multiple requirements, the client programming based on the camera are numerous. One such open source solution is the 2D barcode reader. The encoded data in the 2D barcode which can carry more than 8K of data using the open standard 2D bar codes such as QR Code, DM Code and PDF417 can be decoded using the mobile bar code readers which are freely available for downloads. This can be used for variety of anywhere, anytime services where the encoded data can point to an URL containing the information that is required. The URL can be open URL for public information such as status of service request and the URL can carry server side authentication for private data such as individual health records, financial transactions etc.

MOBILE BANKING

Using IMPS (Inter-Bank Mobile Payment Service) one can send money instantly from the savings bank account using one's mobile number along with a 7 digit MMID (Mobile Money Identifier) number. To receive funds one has to generate MMID. In order to transfer money using IMPS the user has to follow the following steps

- Use the client application provided by the service provider and select Transfer Funds option
- Enter 10 digit mobile number, 7 digit MMID and the Amount and confirm
- Follow the authentication method used by the service provider and the money is transferred instantly

The SMS will inform the transaction status. One can transfer upto Rs. 50,000 as this is encrypted method as per RBI regulations

The same facility is available over SMS instead of the client program where the limit is Rs 5,000 as per RBI regulations

LOCATION BASED SERVICES (LBS)

The idea of location based services has been catching up for the past few years. Location is a very important data point when it comes to mobile computing, and your lat/long coordinates and even what direction you are facing and what particular object you're looking at are important parameters for your searching. This solution can be used in fleet management, tracking, optimised routes, current status of movement, inventory movement within campus/factory etc. Every smartphone company these days wants to offer you something that would couple you with your nearby cellphone towers, local resources and people in your immediate area. When the Government Service Centres such as nearest CSC, Post-

Office, Police Station, Hospital, RTO office, Taluk Office, Collectorate are available as spatial layers with point features for individual locations, Location based Services become more useful on the move. The LBS can answer the queries such as how far, where, route, direction with added public transport facilities to reach the service or the utility centre.

Google's 'What's Nearby' is a location-based search that's part of an updated Google Maps app on Android devices, and soon to be available on the web-based Google Maps on other devices What it does is to simply give you a list of the ten closest places (restaurants, shops, points of interest) that are near your location. While doing the search the voice enabled query or search is also enabled using Google's 'Search by Voice' feature

Mobile client programs can also carry out search based on the pictures taken from a location. 'Google Goggles' is a picture-based search tool, wherein you can take a picture of something and have Google return search results based on it. This could be good to identify something you don't recognize, or learn more about something you do.