Global System for Mobile Communication Technology

Mobile Device Investigations Program

Technical Operations Division

DHS - FLETC

GSM Technology

Global System for Mobile Communication or Groupe Special Mobile

To standardize cellular communication thoughout Europe

Prior to it's development a number of incompatible systems served Europe

GSM Technology

With GSM, European companies agreed to a set of standards

GSM is a open source system

Allows access to code

All operate based on these standards

GSM Technology

GSM operates on the 900 MHz, 1800 MHz and 1900 MHz

GSM uses Digital Communication System or DCS 1800 and is the worlds main 2G standard

When the FCC issued 1900 MHz to PCS in the United States it was based on GSM

DCS 1900 is considered the GSM standard for North America and is called North American GSM.

GSM Technology

GSM is now a worldwide standard

GSM uses Time Division Multiple Access or TDMA technology as their air interface standard

TDMA has limited capabilities

GSM is strictly controlled by a Memorandum of Understanding (MOU)

GSM Architecture and Subsystems

Open architecture according to the Open Systems Interconnect or OSI model for layers 1,2, and 3.

Layer 1 – Physical Layer

Layer 2 – Data Link Layer

Layer 3 – Network Layer

GSM carriers can go to any GSM manufacturer

GSM Architecture and Subsystems

GSM uses voice coders/decoders or vocoders

Vocoders are firmware and chips sets that digitize the human voices

Voice that is sampled and channelized is housed in the vocoder

GSM Architecture and Subsystems

Vocoders packetize the sample of the human speech and transmits it through the handset to the base station

Distant-end vocoders decode the pulses and routes the call to the MSC

A full-rate vocoder allows for eight (8) conversations over a channel

Half-rate vocoders samples at half the rate of speed and allows for more effective use

GSM Architecture and Subsystems

By standard the GSM network is divided into four (4) subsystems

1. The Base-Station Subsystem
2. The Network Subsystem
3. The Operation and Support Subsystem
4. The Mobile Station Subsystem (The Mobile Unit)

Pages 10 through 12 redacted for the following reasons:
- -
(b)(7)e

Page to be removed

Page to be removed

GSM Subsystems - Network Subsystem

The Network Subsystem is in affect the Mobile Switching Center

The central part of the network.

The MSC provides connection to the Public Switched Telephone Network (PSTN) and the Integrated Services Digital Network (ISDN) using SS7 based interconnection.

GSM Subsystems - Network Subsystem

The MSC provides subscriber management functions such as;

- mobile registration
- location updating,
- authentication
- call routing to roaming subscribers.

The Home Location Register (HLR) and the Visitor Location Register (VLR) are located within the MSC.

GSM Subsystems - Network Subsystem

The HLRs database contains different types of information;

1. Every Subscriber Identity Module (SIM) card issued by the Mobile Phone Operator.

   The SIM has a unique identifier called the International Mobile Subscriber Identifier or IMSI,

   IMSI is a primary key to each HLR.

GSM Subsystems - Network Subsystem

2. The SIM card keeps track of all Mobile Subscriber Integrated Services Digital Network Number or MSISDNs.

   These are the telephone numbers that have called the mobile unit.

   It is used for making and recieving voice calls and SMS.

   The MSISDN can have a second number for receiving data and fax.

   Each MSISDN is also a primary key in the rational database.

GSM Subsystems - Network Subsystem

Examples of other data stored in the HLR in a SIM record;

- GSM services the subscriber has requested or been given
- General Packet Radio Service or GPRS settings allow the subscriber access to packet services
- Current location of the subscriber; providing a Serving GPRS Support Node (SGSN- packet roaming)
- Call Divert or Call Forwarding settings

GSM Subsystems - Network Subsystem

In theory the HLR data is stored for as long as the subscriber is with the mobile phone operator

The HLR is a systems that directly receives and processes Mobile Application Part (MAP) transactions and messages.

If the HLR fails the system fails. The HLR manages the Location updates as mobile phones roam.

The HLR is now a powerful server more so than telephone switch hardware

GSM Subsystems - Network Subsystem

HLR connects and interacts with a number of other components on the system

- The Gateway MSC for handling incoming calls
- The VLR for handling request from mobile phones to attach to the network
- The SMSC for handling incoming SMS
- The voice system for delivering notification to the mobile phone that a message is waiting

GSM Subsystems - Network Subsystem

The main function of the HLR is to manage the movement of SIMs and mobile phones by;

- Managing and updating the position through location areas identified with a Local Call Area (LCA). Updates the users location
- Send subscriber information to the VLR when the users roams
- Act as a go between for the GMSC or SMSC with the VLR - receive text or voice messages
- Remove the user of the VLR when he/she has left that roaming area

GSM Subsystems - Network Subsystem

Visitor Location Register (VLR) Database - stores information about all the mobiles that are currently under the jurisdiction of the MSC

The most important is the current Location Area Identity or LAI.

LAI identifies under which BSC the Mobile Station is currently

This information is vital in the call setup process.

Whenever an MSC detects a new MS in its network, it creates a new record in the VLR,

Updates the HLR of the mobile subscriber, apprising it of the new location of that MS.

GSM Subsystems - Network Subsystem

VLR is a temporary database of the subscribers that have roamed into the area

Each base Station is served by only one VLR

No one subscriber can be on more that one VLR at any given time.

VLR are either linked directly to the V-MSC or are integrated with a special software interface.

GSM Subsystems - Network Subsystem

Relevant data stored there are;

- IMSI – the subscriber's identity number
- Authentication Data
- MSISDN – the subscriber's phone number
- GSM services the subscriber has access to
- Access Points (GPRS) that are subscribed to, and
- The HLR address of the subscriber

GSM Subsystems - Network Subsystem

The VLR also connects to;

- The Visited MSC (V-MSC), to pass data needed for certain procedures i.e, authentication and call setup
- The HLR to request data for the mobile phones attached to it's service area
- Other VLR to transfer data as the MS roams from one area to the next accessing new VLRs

GSM Subsystems - Network Subsystem

The VLR primary functions are

- To inform the HLR that a MS has arrived in the particular area covered by the VLR
- To track where the subscriber is within a VLR area when it is not active
- To validate (allow/disallow) which services the subscriber may use

GSM Subsystems - Network Subsystem

The VLR primary functions are

- To allocate roaming numbers during the process of incoming calls
- To purge the subscribers record if he/she becomes inactive while in its area
- To delete the subscribers record when the subscriber moves into another VLRs area based on the rules of the HLR. The VLR is reset daily

GSM Subsystems - Network Subsystem

Other functions associated with the Network Substation are;

- The Authentication Center - provides authentication of the MS and encryption of services
- The Equipment Identity Register (EIR) – Using the IMSI, the EIR keeps track of valid MS. If one is lost, stolen or service discontinued it is blacklisted on the EIR
- Billing Center (BC) – produces the tolls generated by the VLR and HLR for each subscriber and the roaming data
- Short Message Service Center (SMSC) – the sending and receiving of short messages

Page 28 redacted for the following reason:
- - - - - - - - - - - - - - - - - - - -
(b)(7)e

GSM Subsystems Operations and Support Subsystem

The Operations and Support Subsystem – the command and control center used to monitor the GSM system.

If there is a particular system failure the OSS can identify the problem and determine what course of action is needed

GSM Subsystems - Mobile Station Subsystem

The Mobile Station (Mobile Phone) Subsystem – also known as the User Equipment. GSM phones are segmented for a number of reasons.

The MS has four main components;

1. The Mobile Terminal
2. The Terminal Equipment
3. Terminal Adapter
4. Subscriber Identity Module or SIM

GSM Subsystems - Mobile Station Subsystem

The Mobile Terminal or Handset – identification information is held on the SIM card

The handset's main functions are to transmit, receive, encode and decode voice transmissions.

The SIM card contains the GSM operating program, customer and carrier specific data.

GSM Subsystems - Mobile Station Subsystem

Programmed at the sales office, the SIM card provides authentication, information storage, subscriber account information and data encryption.

SIM cards and handsets are interchangeable.

SIM card will recall all information stored on it, including programmed numbers, SMS saved, ring tones, Contact list and the like.

GSM Subsystems - Mobile Station Subsystem

Some of the Network Specific items used to authenticate and identify subscribers on the Network are;

Integrated Circuit Card ID or ICCID – International ID, stored in the SIM card and stamp of the card

International Mobile Subscriber Identity or IMSI- Mobile operators connect mobile phone calls and communicate with their market through SIM cards

Local Area Identity or LAI – Networks are divided into local areas with a unique number. When you travel from one area to another the unique number is logged in the SIM.

GSM Subsystems - Mobile Station Subsystem

Operator Specific Emergency Number – like “112” or E911 these numbers (5) are programmed into the SIM

Short Message System Center Number or SMSC number – the number used to sent text messages

Service Providers Name or SPN – the telecommunications service providers name and ID

Service Dialing Numbers or SDN – numbers associated with the service provider

GSM Subsystems - Mobile Station Subsystem

Advice of Charges – what are the parameters in which the account will charged

Value Added Services or VAS – what type of service i.e. Internet access is associated with the account

Depending on storage capacity any type of data may be stored.

In Europe some subscribers store their medical records on their SIM card.

Any data!!!!!!!

GSM Subsystems - Mobile Station Subsystem

Authentication Key or Ki – a 128-bit value used to authenticate the SIM to the mobile network. Assigned by the operator the Ki is contained on the service providers HLR.

GSM was designed from the start with security in mind. The SIM card aids in this security, making fraud on a GSM network unlikely.

Using a series of secret keys and algorithms thwarted cloning of GSM devices.

GSM Subsystems - Mobile Station Subsystem

In GSM Call Handoff, or Call Handover is different in that it is mobile device assisted.

The mobile phone continually monitors base stations in vicinity measuring the strength in the MSC.

The six best prospects are sent back to the MSC who then determines when the handoff will be conducted.

GSM

Often described as a true Intelligence Network, GSM is called the first true wireless network because;

- It has an open, distributed architecture
- The separation of switching and service control functions
- Full use of SS7 as the signaling infrastructure
- Its clearly defined and specified interfaces
- The nature of its IN structure

General Packet Radio Service (GPRS) and Enhanced Data Rates for Global Evolution (EDGE - CDMA), are 3G GSM based standards

GSM Adjunct Systems

GSM standards define that certain Adjunct or Secondary Systems work with GSM technology. Some of note are;

- The Gateway MSC or GMSC – The purpose of which is to query the HLR and determine the location of the subscriber. Calls from another network i.e. PSTN will first go through the GMSC.

- Short Message Service Center or SMSC – The node that stores and forwards short messages to and from the mobile station.

GSM Adjunct Systems

- The Equipment Identity Register or EIR – identifies what equipment i.e. handsets are acceptable in a GSM Network

- The Interworking Function or IWF – used for circuit switched data and fax services. It is basically a modem bank

GSM v CDMA

There is a debate as to how long TDMA or IS-136 cell phones will be in existence. GSM and CDMA system now dominate the market.

Both work well on their own as well as with each other.

Some CDMA mobile units use a Removable – User Identity Module or R-UIM which is similar to a SIM. There are Dual R-UIM that allow for use in both GSM and CDMA units.

Both seem positioned to be in place for a period of time.