3.3.6 Establishment of a GSM Call

There are three possible connections involving a GSM network—Land to Mobile (L_M), Mobile to Land (M_L) and Mobile to Mobile (M_M).

GSM-call originated by a land phone

In this case the call is originated by a Land phone and destined to an MS, i.e. L_M connection is to be considered. When a call originates from a Land phone, it is forwarded to the MSC through PSTN. The MSC checks from HLR/VLR whether the called MS is available in the network. If it is available, the MSC pages all the BSCs/BTSs under the control of the MSC to track the MS. From this point the BTSs take the responsibility for tracking the MS. A traffic channel is assigned for setting up the call after a number of message exchanges between BTS and MS. The activities of BTSs and MS to track the MS and (if the MS is tracked) to set up the call are summarized in the following steps.

- BTS broadcasts on paging channel (PCH) to track the MS
- MS
  - Detect the page
  - Reply the page and requests for accessing the network with a Random Access Channel (RACH)
- BTS
  - Grant the request over AGCH by assigning a channel SDCCH/SACCH to the MS
  - Request the MS over SDCCH to send data for authentication
- MS
  - Send authentication data on SDCCH
- BTS
  - Send call set-up and connection request over SDCCH
- MS
  - Acknowledge the request on SDCCH
- BTS
  - Assign TCH to the MS

GSM-call originated by a cell phone

In this case an MS originates the call whereas the call may be destined either to a land phone or to another MS, i.e. M_L and M_M connections are to be considered. When a call originates from an MS, it acquires a traffic channel to set up the call by exchanging messages between BTSs and MS. The following steps summarize the activities of the originating MS and BTSs.

- MS
  - Monitor the BCCH
  - Synchronize to a nearby BTS
  - Request to the BTS for accessing the network on RACH

- BTS
  - Respond the request on AGCH
  - Grant the request over AGCH by assigning a channel SDCCH/SACCH to the MS
  - Request the MS over SDCCH to send data for authentication
- MS
  - Send authentication data on SDCCH
- BTS
  - Send call set-up and connection request over SDCCH
- MS
  - Acknowledge the request on SDCCH
- BTS
  - Assign TCH to the MS

For the connection M_M, the originating MS gets permission for accessing the network and acquires traffic channel (TCH) by exchanging messages between BTS and MS as shown in 'GSM-call originated by cell phone'. On the other hand, the called MS gets permission to access the network and acquires TCH only after the MS is tracked. The message exchange between BTS and the called MS is performed as the steps shown in 'GSM-call originated by land phone'.

3.3.7 Channel Usage during GSM Call

In case of L_M and M_M connections, that is when called unit is an MS, all the tasks shown in Figure 3.8(a), (b) and (c) are done for providing channel to the called MS to set up and release the call. However, for M_L and M_M connections, that is when call is originated by an MS, the tasks shown in Figure 3.8(a) and (c) are performed for providing channel to the originating MS to set up and release the call. Therefore, for M_M connection first the tasks (a) and (c) are performed for giving channel to the originating MS, and then all the tasks (a), (b) and (c) are performed for providing channel to the called MS.

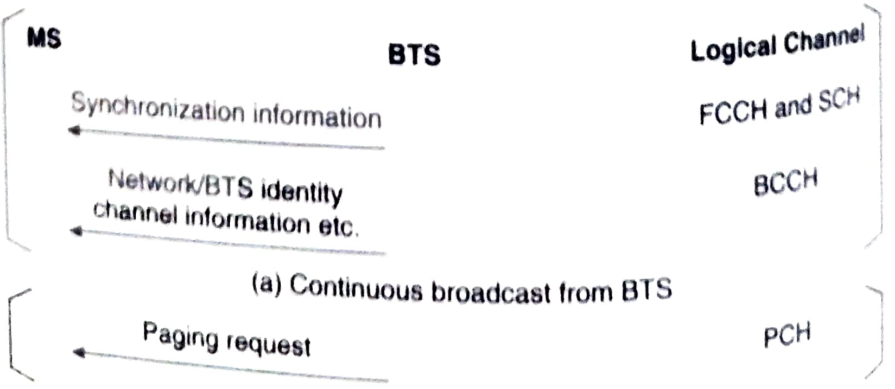
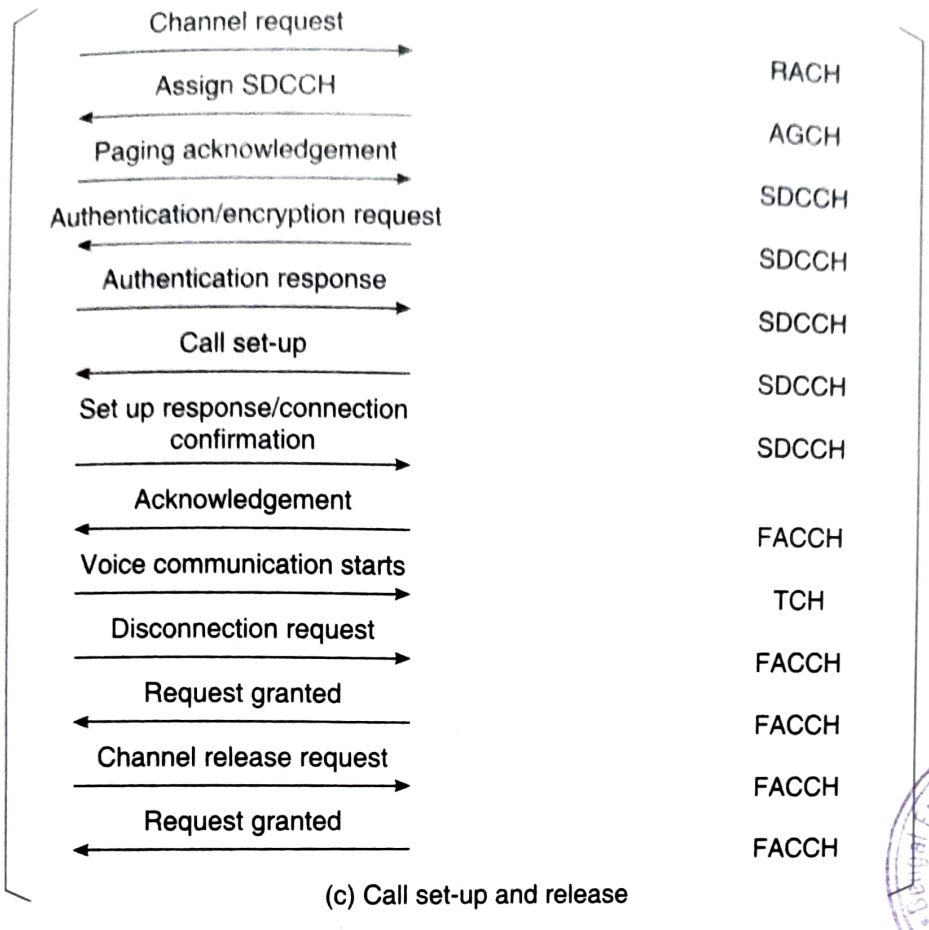


Figure 3.8 *Contd.*



(c) Call set-up and release

Figure 3.8 Usage of GSM channels.

3.3.8 User Validation in GSM

In GSM, subscriber identity module (SIM) of an MS contains international mobile subscription identity (IMSI), authentication key K_i, A_3 algorithm and A_g ciphering key generating algorithm. The authentication process of GSM-based systems check the validity of SIM. It is analogous to a challenge-and-response process.

The GSM network sends a 128-bit random number to an MS as the challenge. The MS feeds the random number (challenge) and K_i to the A_3 algorithm to generate a signed response (SRES). The SRES in turn is sent back to the network. The network compares the received SRES with the SRES supplied by the authentication centre (AC). If there is a match, the subscriber is recognized as valid. Upon confirming the user validity, the A_3 algorithm is run at the both ends of the air interface to generate a ciphering key (K_c) considering the random number and K_i as the inputs. The K_c is used as input to the A_g algorithm for encryption and decryption of data.

In GSM-1900/AMPS, a dual mode MS, the user validation process is a key-based authentication process similar to that as discussed in Section 2.11.2. Here, a mobile station intending to make a call runs an algorithm to generate a data called MS-AUTHR (mobile station generated

authentication result). The IMSI is keyed with a hidden authentication key K (corresponds to AMPS A-key) and used as input to the algorithm. The MS-AUTHR along with keyed IMSI are sent to the network. The network also generates a network generated authentication result (NT-AUTHR). The MS-AUTHR and NT-AUTHR are then compared. If underscores should be replaced by hyphen they match, the call is authenticated. As the mobile station specific IMEI (equivalent to ESN of AMPS) is not used in the authentication process, a valid SIM in the form of a card can be used with any valid GSM mobile station and can be authenticated.

3.4 IS-95

The first CDMA-based digital cellular standard is the Interim Standard 95 commonly known as IS-95. The brand name for IS-95 is cdmaOne. As it uses CDMA, the network capacity does not put a strict ceiling on the number of users in IS-95.

In a CDMA system, the encoded voice is digitized and divided into packets. These packets are tagged with unique "codes". Then the packets are mixed with all other packets in the local CDMA network. It is then routed towards destination. At the receiving end only the packets with the codes destined for it are accepted.

The users share a common channel for transmission within a cell. Users in adjacent cells also use the same radio channel. In other words, the frequency spectrum is reused. The spreading factor used in IS-95 is 128 with the maximum user data rate 9.6 kbps. Forward and reverse links use different spreading techniques. As discussed in Section 3.2.3, optionally IS-95 employs two-phase or multiple spreading. One phase provides mutual orthogonality among all users in one cell and the other phase provides mutual orthogonality among the users in different cells. Rake receivers[12] are used at both the base station and mobile station to resolve and to combine multi-path components.

3.4.1 System Architecture

Figure 3.9 shows the IS-95 system architecture including interfaces. This section describes the tasks performed by each module of the system.

Inter-Working Function (IWF): It is the interface (L of Figure 3.9) between a wireless system and the telephone network. IWF converts data, transmitted over the air interface, to a format recognized as well as carried by the public telephone network, e.g. PSTN. It also synchronizes transfer between

[12] In DSSS, receivers face a problem during reconstruction of the original data due to multi-path propagation. Signal reaches to a receiver from multiple paths having different delays and path loss. Rake receivers apply a mechanism to solve this problem and reconstruct the original data.

a circuit-switched network and the packet-switched network, and that effectively enables an MSC to communicate with other networks.

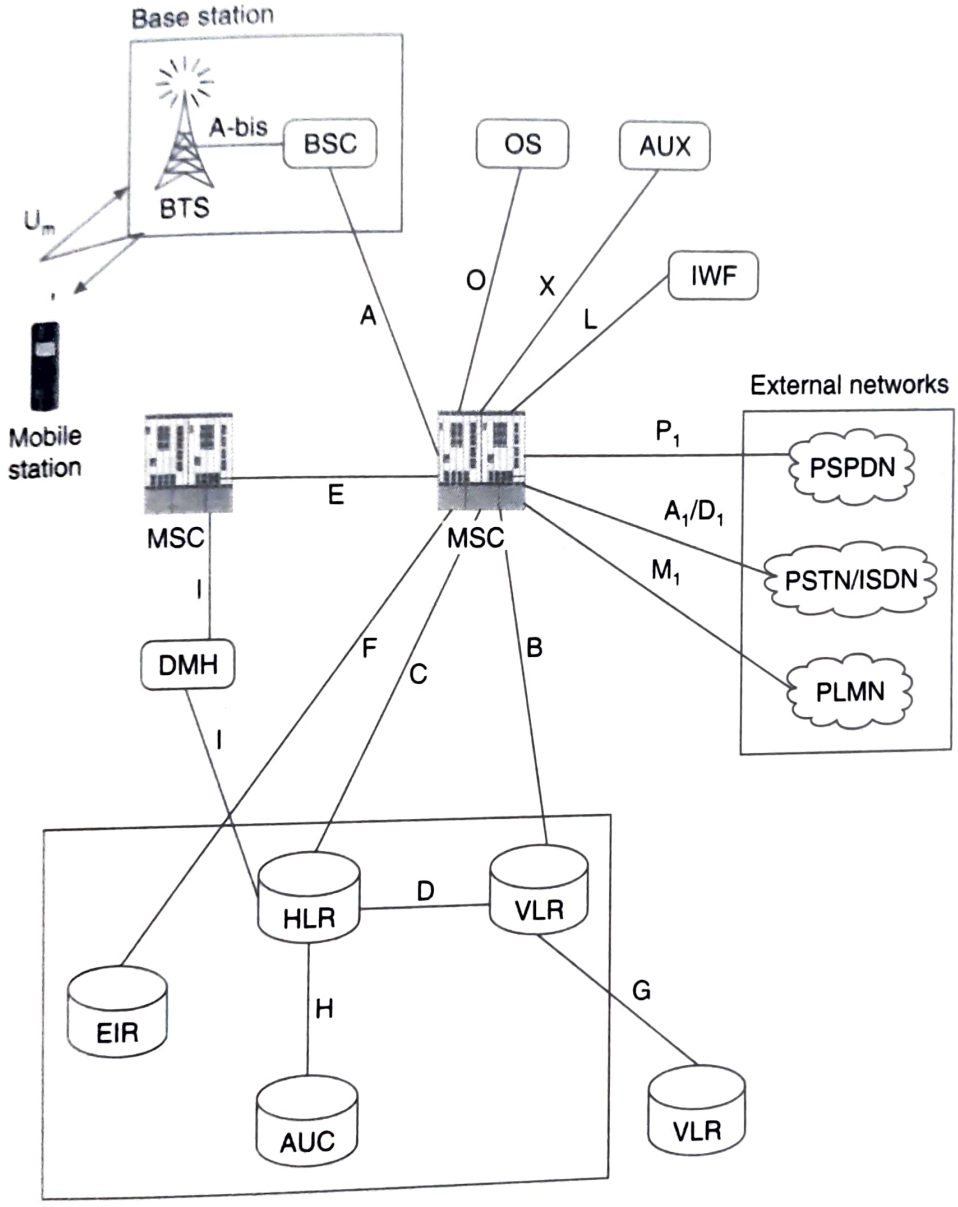


Figure 3.9 IS-95 architecture.

Operation System (OS): The OS is responsible for overall management of the wireless network. Its interface with MSC is denoted as 'O'.

Auxiliary (AUX) equipment: An MSC is connected with a number of auxiliary equipments such as signal transfer point (STP), short message service centres (SMSCs) and voice mailbox system. The interface is denoted as 'X' in Figure 3.9.

Data Message Handler (DMH): The responsibility of DMH is to collect billing data. DMH is connected with MSC by an interface 'I'. It provides: (i) a standard for call detail and billing record format, (ii) procedures and messages required to perform such record transmission between systems.

HLR/VLR/AUC: HLR (Home Location Register), VLR (Visiting Location Register) and AUC (Authentication Centre) are involved in mobility management, handover, and user validation. The tasks of these components in GSM system are described in Section 3.3.1. The HLR contains static database comprising subscribers' information such as ESN (electronic serial number), IMSI (international mobile station identity), user profiles, present location of a user, etc. to manage subscribers' mobility. On the other hand, the VLR keeps dynamic database comprising visiting users' ESN, profiles collected from the user's HLR. The AUC takes care of user validation, elaborated in Section 3.4.4.

Interfaces with other networks

The following interfaces exist between MSC and other networks.

A_1/D_1: The MSC is connected with PSTN (public switch telephone network) by analog interface A_1 and by digital interface D_1, it is connected with ISDN (integrated switch digital network).

M_1: The interface between MSC and other wireless network, i.e. PLMN (public land mobile network) is M_1. The PLMN may be another cellular network.

P_1: An MSC can communicate with other PSPDN (packet-switched public data network) such as X.25 and IP-based network. The interface is shown as P_1 in Figure 3.9.

3.4.2 Protocol Layers and Channels in IS-95

The IS-95 standard does not explicitly mention the functions of each protocol layer. However, the functions of each layer very much exist. In the air interface, i.e. between a mobile station and the base station, a set of protocols is used. It describes a three-layer stack—(i) physical layer, (ii) medium access control (MAC) and link access control (LAC) sublayers and (iii) upper layer.

(i) Physical layer

The IS-95 standard defines the transmission of signals in physical layer in both the forward (downlink) and reverse (uplink) directions. Every IS-95 service provider receives 12.5 MHz spectrum. The 10% of available cellular spectrum, i.e. 1.25 MHz is occupied by each channel. Unlike other cellular standards, the user data rate (but not the channel chip rate) changes in real time depending on the voice activity and requirements of the network.

Forward channels

In the forward direction, radio signals are transmitted by BTSs. Every BTS is synchronized with a GPS receiver. All forward transmissions are BPSK[13] (binary phase shift keying) with a chip rate of 1,228,000/s. Multiple spreading

[13] The simplest form of phase shift keying considering two phases.

is used for this transmission. Each signal is spread with a walsh code of length 64 and a pseudo-random noise code (PN code) of length 2^{15} causing a PN roll-over period[14] of 80/3 ms. The walsh codes differentiate transmissions within a cell. The PN codes are used to isolate cells (BTSs) that are using the same frequencies. The same PN sequence is used in all BTSs and the offset for each BTS is unique.

Forward broadcast channel: A forward channel consists of pilot channel, synchronization channel, maximum seven paging channels and at most sixty-three forward traffic channels. The pilot, synchronization and paging channels are considered as the broadcast channel. The details of IS-95 channels are shown in Figure 3.10.

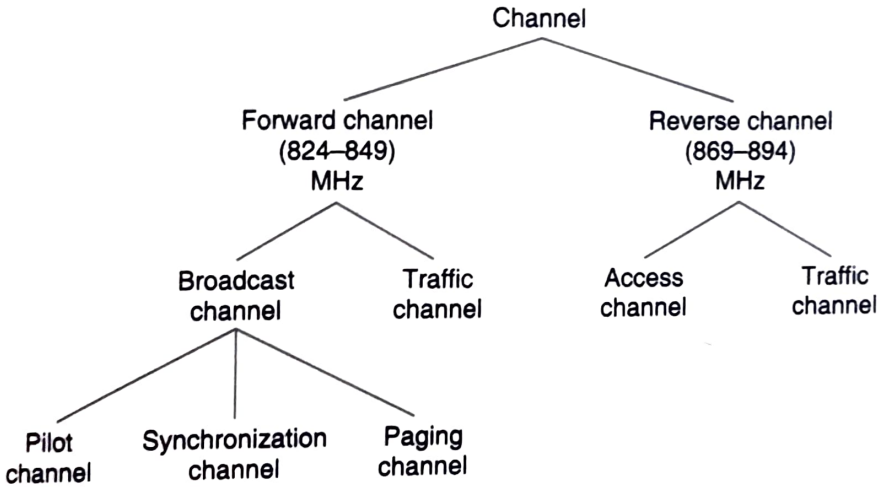


Figure 3.10 IS-95 Channel structure.

Pilot channel. The *pilot channel* consists of an unmodulated PN sequences spread with walsh code 0. The power control is not required in the pilot channel. It does not carry any data. Each BTS in the network is assigned a PN offset in steps of 64 chips. Each pilot transmits the same spreading sequence at different time offset.

Each MS continuously monitor pilot channels. With the help of broadcast information sent over pilot channel, an MS distinguishes different BTSs comparing signal strength received by the MS. The monitoring of pilot channel and measurement of signal strength received from different BTSs by an MS help to take decision of handoff.

Synchronization channel. A *synchronization (sync) channel* provides system parameters to an MS that are required to synchronize with the network and obtain a paging channel. The channel continually broadcasts sync messages for the MSs. The messages contain information about the network including its identity, version of radio interface being supported, PN offset used by BTS, etc. It uses walsh 32 for spreading and operates at 1200 bps. It also helps the MSs for acquiring a paging channel.

[14] The period with which the sequence reproduces.

Once an MS finds a strong pilot channel, it listens to the sync channel and decodes the sync channel message to build up a highly accurate synchronization with the system time. As the sync channel message contains network-ID, the MS can know whether it is currently in roaming.

Paging channel The *paging channel* carries either control information for call set-up or paging messages, when an incoming call from BTS to MS is to be served by them. It does not require any power control. There are three possible rates used in the paging channel—9600, 4800 and 2400 bps. All the rates are encoded to 19200 symbols per second. The messages on paging channel convey detailed network parameters and also carry higher-priority messages dedicated to setting up a call to and from the MSs. Typical messages on the paging channel include pages, traffic channel assignments and short messages.

Forward traffic channel: The forward traffic channels are used to transmit voice or data to an MS. There may be maximum 63 forward traffic channels—the exact number depends on the number of paging channels and the presence of synchronization channels. Channels are logically separated by the unique walsh codes. Such traffic channels carry the individual user information (voice or data). Since voice and data are intermittent, the traffic channels support variable rate (1200, 4800, 9600 bps) operation.

Reverse channels

The reverse channels are the access and traffic channels. At the BTS receiver the signal carried by the reverse channels is a combination of output signals from all the MSs within the BTS's coverage area. The reverse channel allows up to 62 traffic channels and 32 access channels. However, the number of channels in use at any point of time may be considerably lower.

Reverse traffic channel. Reverse channels use OQPSK (offset quadrature phase shift keying) for power efficiency. All data transmitted on the reverse channel are convolutionally encoded, block interleaved, modulated by a 64-ary orthogonal modulation and spread prior to transmission.

Access channel. An access channel allows an MS to communicate with the system when it needs to initiate an action such as registration, call origination or it needs to respond to the messages received on a paging channel. Since multiple MSs may attempt access at the same time, the access channel utilises suitable protocol for contention management. The data rate for the access channel is 4800 b/s.

(ii) MAC and LAC sublayers

The MAC sublayer provides a control function to manage resources supplied by the physical layer and coordinates their usage by LAC sublayer. Once a call is established, an MS uses traffic channel that allows voice or data bits to be multiplexed with signalling message fragments. The signalling

message fragments are assembled in the LAC. The LAC in turn sends complete signalling messages to the upper layer. The MAC provides multiplexing and QoS control. The QoS is implemented by prioritizing requests and resolving conflict messages.

(iii) Upper layer

The overall control of the system is taken care of by the upper layer. Both the voice and data messages pass through the upper layer.

3.4.3 Establishment of a IS-95 Call

Like GSM, there are three possible connections involving a IS-95 network—Land to Mobile (L_M), Mobile to Land (M_L) and Mobile to Mobile (M_M).

IS-95-call originated by a land phone

In this case the call is originated by a Land phone and destined to an MS that is L_M connection is to be considered. Here, the call is forwarded to BTSs through MSC in the same way as described in Section 3.3.6. Once the call is forwarded to the BTSs, the BTSs take the responsibility for tracking the MS. A traffic channel is assigned for setting up the call after exchanging messages between BTS and MS. The activities of BTSs and MS to track the MS and set up (if the MS is tracked) a call are summed up in the following steps.

- BTS broadcast on paging channel to track the MS
- MS
  - Detect the page
  - Acknowledge on access channel
- BTS
  - Configure the transmitter and receiver by walsh code and PN code respectively
  - Send this information on paging channel
- MS
  - Receive paging channel
  - Configures transmitter and receiver by PN code and walsh code respectively
  - Send authentication information on access channel
- BTS
  - Authenticate the MS
  - Send an alert message for ringtone
- MS
  - Acknowledge the alert by ringing
- BTS
  - Assign traffic channel to the MS

IS-95-call originated by a cell phone

In this case an MS originates the call whereas the call may be destined to either a Land phone or to another MS that is M_L and M_M connections

are to be considered. When a call originates from an MS, it acquires a traffic channel to set up the call by exchanging messages between BTSs and MS. The following steps sum up the activities of the originating MS and BTSs.

- MS
  - Monitor the pilot and sync channel
  - Synchronize to a network BTS
  - Seek network access permission on access channel
  - Monitor paging channel for BTS response
- BTS
  - Grant the access request on paging channel
- MS
  - Send authentication information on access channel
- BTS
  - Authenticate the MS
  - Assign traffic channel to the MS

Like GSM, in case of M_M connection, the originating MS gets permission of accessing the network and acquires traffic channel by exchanging messages between BTS and originating MS as in 'IS-95-call originated by cell phone'. On the other hand, the destination MS gets permission to access the network and acquires traffic channel only after the MS is tracked. The message exchange between BTS and destination MS is performed following 'IS-95-call originated by land phone'.

3.4.4 User Validation in IS-95

The user validation process is similar to the process used for GSM (discussed in Section 3.3.8). Instead of A_3 algorithm in GSM, the CAVE (cellular authentication and voice encryption) algorithm is stored in an MS. The network and the MS share a secret key referred as SSD (shared secret data) consisting of two parts: SSD-A and SSD-B, each of 64 bits. A BTS broadcasts time to time a 32-bit random number as the so-called challenge. Each MS feeds the received challenge, SSD-A, ESN (electronic serial number) and MIN (mobile identification number) to the CAVE algorithm to obtain a SRES (signed response). The SRES is then sent to the network's authentication centre (AUC). If there is a match between SRES from MS and the SRES computed at AUC, the MS is authenticated. Once authentication is over, the network sends encryption key and voice privacy mask[15] to the MS. The encryption key and voice privacy mask are used for encryption of signalling message and voice respectively.

[15] In IS-95, each MS is provided a unique long code as mask based on its ESN. This mask is known as voice privacy mask that is applied to the voice data to provide privacy at both downlink and uplink data transfer over air interface.