This scenario describes the call setup for a GSM originating call. A mobile user calling a landline subscriber is covered here.

Begin RR Connection Establishment

Call related information needs to be transported from the mobile phone to the Mobile Switching Center (MSC). This requires the establishment of a Radio Resource (RR) connection to MSC. The first phase of the call setup just sets up this RR connection.

RR CHANNEL REQUEST

The BSS allocates a Traffic Channel (TCH) to the mobile. The TCH allocation assigns a frequency and timeslot on that frequency. After the mobile receives this message, the mobile shall only use the specified resources for communication with the mobile network.

RR IMMEDIATE ASSOCIATION

The BSS transmits the radio resource assignment to the Mobile via the AGCH channel. The message also contains the time and frequency corrections. The time corrections allow the mobile to time its transmissions so that they reach the BSS only in the specified slot. The frequency corrections correct for the Doppler shift caused by the mobile's motion.

RR SABM + MM CM SERVICE REQUEST

This is the first message that is sent after tuning to the channel. The Mobile initiates a LAPm connection with the BSC by sending a Set Asynchronous Balanced Mode (SABM) message. The service request message meant for the MSC is also sent in this message.

RR UA

The BSS replies with Unnumbered Acknowledge (UA) to complete the LAPm setup handshake.

SCCP CONNECTION REQUEST + MM CM SERVICE REQUEST

The BSS receives the CM Service Request message from the mobile and forms a "BSSMAP COMPLETE LAYER 3 INFORMATION". The BSS then piggybacks the message on the SCCP connection request message.

Enable Ciphering

Since the subscriber has been successfully authenticated, the MSC initiates ciphering of the data being sent on the channel. The channel is ciphered so as to protect the call from eavesdropping.

Ciphering on the radio link is enabled in three steps. As a first step, the BSS starts expecting ciphered data from the mobile but continues to
send data in clear. Since the mobile has not been informed about the ciphering, all data received from the mobile will be in error.

The BSS sends the CIPHERING MODE COMMAND to the mobile. The mobile will be able to receive this message as the transmission from the BSS is still in clear.

Ciphering has already been enabled, so this message is transmitted with ciphering. The BSS will receive this message as it is already expecting ciphered data in the receive direction.

The third and final step in the ciphering handshake. The BSS enables the ciphering in transmit direction. From this point on ciphering is enabled in both directions.

BSS replies back to the MSC, indicating that ciphering has been successfully enabled.

At this point a connection has been setup between the Mobile and the MSC. From this point onward, the BSS is just acting as a conduit for transporting the signaling messages between the Mobile and the MSC.

MSC informs the BSS about the allocated voice circuit. The call is also switched from signaling to voice.

The BSS notifies the Mobile about the changeover to voice mode.

Mobile acknowledges.

The BSS responds back to the MSC.

Call release has been completed, now the RR connection is released by the MSC.

The BSS initiates RR release with the mobile.

The BSS informs the MSC that the RR connection has been released.

The mobile sends a disconnect message to release the LAPm connection.

The BSS replies with an Unnumbered Acknowledge message.

The BSS releases the TCH channel.