

Beschreibung zum SSD

17. Mai 2007 – Fabio Ferrari

1. Aus dem Festnetz bekommt die GMSC über die ISUP Signalisierung, die Initial Address Message (IAM) Nachricht mit der Telefonnummer (MSISDN) des Gesprächspartners übermittelt.
2. Die GMSC sendet nach Erhalt der IAM Nachricht eine Send Routing Information (SRI) an das Home Location Register (HLR), um die aktuelle MSC des Teilnehmers zu ermitteln.
3. Das HLR ermittelt anhand der übergebenen MSISDN die IMSI des Teilnehmers und findet somit auch seine aktuelle MSC und deren VLR. Nun sendet das HLR eine Provide Roaming Nachricht an das MSC, um diese über den ankommenden Anruf zu informieren.
4. Im MSC/VLR wird die übergebene IMSI einer temporären Mobile Station Roaming Number (MSRN) zugeordnet, die dann an das HLR zurückgegeben wird.
5. Das HLR gibt die MSRN schliesslich transparent an die GMSC zurück.
6. Die GMSC verwendet die so erhaltene MSRN für die Weitervermittlung des Gesprächs an die MSC/VLR. Statt der ursprünglichen MSISDN des Teilnehmers enthält diese IAM Nachricht nun die MSRN.
7. In der MSC/VLR wird die MSRN dann verwendet, um die IMSI des Teilnehmers und seine Daten im VLR zu finden. Dies ist möglich, da bei der Zuteilung der MSRN bei der Anfrage des HLR diese Beziehung gespeichert wurde. Nachdem die Teilnehmerdaten im VLR gefunden wurde, wird nun der Teilnehmer von der MSC in der Location Area gesucht, die in seinem VLR Eintrag gespeichert ist. Dazu schickt die MSC eine Paging Nachricht an die entsprechende BSC.
8. Die BSC wiederum schickt daraufhin in jede Zelle der betreffenden Location Area eine Paging Nachricht, die dann auf dem Paging Channel PCH ausgestrahlt wird.
9. Das Endgerät erhält über den PCH eine Nachricht, dass das Netz mit ihm Kontakt aufnehmen will. Es sendet deshalb über den Random Access Channel (RACH) eine Channel Request Anfrage. Diese wird über den „Zufallskanal“ gesendet, da die Teilnehmer einer Zelle nicht untereinander synchronisiert sind. (Achtung! Kollisionsgefahr) Es ist ja nicht gewährleistet, dass nicht zwei Endgeräte versuchen, zur selben Zeit auf das Netzwerk zuzugreifen.
10. Die BSC überprüft daraufhin, ob ein freier Signalisierungskanal (SDCCH) vorhanden ist und aktiviert diesen in der BTS.
11. Bestätigung ob Aktivierung durchgeführt werden konnte.
12. Danach schickt die BSC auf dem Access Grant Channel (AGCH) eine Immediate Assignment Nachricht mit der Nummer des zugeteilten SDCCH zum Endgerät zurück. Der SDCCH x wird nun für die weitere Kommunikation verwendet.
13. Nach erfolgreicher Verbindungsaufnahme, sendet das Endgerät eine Location Update Request Nachricht an das Netzwerk. Bevor das Netzwerk diese bearbeitet, wird der Teilnehmer zuerst authentifiziert und danach die Verschlüsselung (Ciphering) aktiviert.
14. Die MSC fordert nun beim HLR/Authentication Center so genannte Authentication Triplets an. Teil dieser Anforderung ist die IMSI des Teilnehmers.

Beschreibung zum SSD

17. Mai 2007 – Fabio Ferrari

15. Das Authentication Center sucht anhand der IMSI den Ki des Teilnehmers und den zu verwendenden Authentifizierungsalgorithmus, der A3 genannt wird. Mit der Ki wird dann das Authentication Triplet gebildet. **RAND** → 128 Bit Zufallszahl, **SRES** → wird aus Ki und RAND mit Ar erzeugt, **Kc** → Auch der Ciphering Key Kc wird aus Ki und Rand erzeugt. Er wird für die Verschlüsselung des Datenverkehrs nach erfolgreicher Authentifizierung verwendet. RAND, SRES (und Kc) werden anschliessend der MSC übergeben, die die eigentliche Authentifizierung des Teilnehmers vornimmt.
16. Nun sendet die MSC dem Endgerät die Zufallszahl (RAND) in einer Authentication Request Nachricht.
17. Das Endgerät übergibt die Zufallszahl der SIM Karte, die dann mit der Kopie von Ki un dem Authentifizierungsalgorithmus A3 die Antwort, also die SRES* berechnet. Diese schickt dann das Endgerät zur MSC zurück.
18. Stimmen SRES* und SRES? Überein, ist der Teilnehmer erfolgreich authentifiziert.
19. Die Aktivierung der Verschlüsselung erfolgt mit der Ciphering Command Nachricht durch die MSC. Diese Nachricht enthält unter anderem Kc, der von der BTS für die Verschlüsselung verwendet wird. Bevor die Nachricht an das Mobiltelefon weitergeleitet wird, entfernt das BSS jedoch Kc aus der Nachricht, da dieser nicht über die Luftschnittstelle übertragen werden darf. Würde j auch keinen Sinn ergeben, da SIM selber berechnet.
20. Bestätigung
21. Dem Endgerät wird nun eine neue Temporäre ID (TMSI) zugeteilt, die auf der Luftschnittstelle beim Verbindungsaufbau und Paging statt der IMSI verwendet wird. Da eine ständige wechselnde TMSI den Teilnehmer beim nächsten Verbindungsaufbau identifiziert ist sichergestellt, dass die Identität des Teilnehmers auch während des nicht verschlüsselten Teils der Kommunikation geschützt ist.
22. Anschliessend wird dem Endgerät der erfolgreiche Location Area Update bestätigt und die Verbindung getrennt.
23. Erst jetzt wird das Endgerät über den eingehenden Anruf über eine Setup Nachricht informiert. Teil dieser Nachricht ist auch die Nummer des Anrufers, sofern diese nicht unterdrückt ist.
24. Telefon bestätigt den eingehenden Anruf
25. Der Aufbau des Sprachkanals wird immer von der MSC bei der BSC beantragt. Sie schickt eine Assignment Request Nachricht an die BSC.
26. DIE BSC überprüft daraufhin, ob in der gewünschten Zelle ein freier Traffic Channel (TCH) vorhanden ist und aktiviert diesen in der BTS.
27. Danach wird das Endgerät über den SDCCH benachrichtigt, dass ein TCH für die weitere Kommunikation zur Verfügung steht.
28. Das Endgerät wechselt dann auf den TCH und FACCH und sendet ein SABM Frame zur BTS.
29. Diese sendet daraufhin ein UA Frame als Bestätigung über die korrekte Verbindungsaufnahme an das Endgerät zurück.
30. Danach sendet das MS ein Assignment Complete an die BSC zurück.
31. Diese Nachricht wird auch die MSC weitergegeben. SDCCH wird freigegeben.
32. Das Endgerät schickt nun eine Alerting Nachricht zur MSC und teilt ihr dadurch mit, dass der Teilnehmer über den eingehenden Anruf informiert wird (das Telefon klingelt).

Beschreibung zum SSD

17. Mai 2007 – Fabio Ferrari

33. Die MSC ihrerseits gibt die Information über die Address Complete Nachricht ACM an die GMSC weiter. Auch diese gibt die Information über eine ACM Nachricht an das Festnetz weiter.
34. Nimmt der mobile Teilnehmer das Gespräch an, schickt das Endgerät eine Answer Nachricht zur MSC.
35. Diese leitet die Information dann über eine Answer Nachricht (ANM) zur GMSC weiter. Von dort aus wird dann das Festnetz wiederum durch eine ANM Nachricht informiert, dass das Gespräch durchgeschaltet wurde.
36. Auch während der eigentlichen Sprachverbindung werden ständig Signalisierungsnachrichten ausgetauscht. Am häufigsten werden zweifellos Nachrichten mit Messergebnissen zwischen Endgerät, BTS und BSC ausgetauscht. Wenn nötig, kann die BSC während der bestehenden Verbindung ein Handover zu einer anderen Zelle veranlassen. Dazu wird als erstes in der neuen Zelle ein TCH aktiviert.
37. Danach schickt die BSC dem Endgerät über die alte Zelle ein Handover Command über den Fast Associated Control Channel (FACCH). Wichtige Informationen in dieser Nachricht sind die neue Frequenz und die Nummer des Timeslots des neuen TCH.
38. Das Endgerät ändert dann seine Sende/Empfangsfrequenz, synchronisiert sich ggf. mit der neuen Zelle.
39. Das Endgerät sendet in vier aufeinander folgenden Bursts des Timeslots und eine Handover Access Nachricht.
40. Im fünften Burst des Timeslots wird eine SABM Nachricht gesendet.
41. Hat die BTS den Handover korrekt erkannt, schickt diese eine Establish Indication Nachricht zum BSC und eine UA Nachricht zum Endgerät.
42. Aus Sicht des Endgeräts ist der Handover damit beendet. Die BSC muss jedoch noch den TCH in der alten Zelle abbauen und dem MSC eine Nachricht über den erfolgten Handover schicken. Diese Nachricht ist jedoch nur informativ und hat auf der MSC keinen Einfluss auf den weiteren Verbindungsablauf.
43. Beendet einer der beiden Teilnehmer das Gespräch, schickt die jeweilige Seite eine Disconnect Nachricht.
44. Nach Abbau des Sprachkanals zum Endgerät und dem Senden einer ISUP Release Complete Nachricht ist die Verbindung dann komplett beendet.