信令名字：

信令内容：

**1.1首先是IMSI的获取过程**

MME获取UE的IMSI：UE将IMSI放入Initial attach request message里面，MME获取IMSI；这个过程可以分为两步：UE和eNB同步上+建立ECM连接：

***1.1 radio link synchronization***

UE通过PLMN和小区搜索过程来选择eNB并进行无线连接同步，同步完成后，UE可以和eNB通信，UE已经在EMM中注册，但是ECM-IDLE，RRC-IDLE。

***1.2 ECM Connection Establishment***

UE 的NAS层需要发送Initial attach request（including IMSI and UE Network Capability）到MME的NAS层来建立附着，那么，在此之前需要在UE和MME之间建立ECM connection；UE和eNB之间是RRC连接，Attach Request message放在了RRC Connection Setup Complete message 里面；eNB和MME之间是S1信令接口连接，Attach Request message放在了Initial UE Message的NAS-PDU里面：

**(1) RRC Connection Establishment**

1) [UE🡪eNB] RRC Connection Request

2) [UE🡨eNB] RRC Connection Setup

3) [UE🡪eNB] RRC Connection Setup Complete

Attach Request message放在了RRC Connection Setup Complete message 里面。

**(2) S1 Signaling Connection Establishment**

S1信令连接由一对ID定义（eNB UE S1AP ID---eNB从UE获得的；MME UE S1AP ID---MME为UE产生的）；eNB获得eNB UE S1AP ID来建立S1信令连接，并将Attach Request message放在Initial UE Message的NAS-PDU里面传输。Initial UE Message (eNB UE S1AP ID, NAS-PDU, TAI, ECGI, RRC Establishment Cause)：

• eNB UE S1AP ID: eNB从UE获得的ID，用于eNB与MME建立S1信令连接；

• NAS-PDU:UE到MME的NAS层的信息(Attach Request)

• TAI: UE的TA位置（MCC+MNC+TAC）

• ECGI: UE所在小区的位置

• RRC Establishment Cause = mo-Signaling: indicates the signaling was generated by a UE

当MME接收到Initial UE Message 后，MME会为UE生成MME S1AP UE ID，这两个ID都产生后，eNB和MME之间的S1信令连接就完成了，MME S1AP UE ID用于MME下行鉴定UE。

**(3) ECM S1 Connection Establishment**

通过上面两步，UE和MME的NAS层的ECM连接完成。

**(4) IMSI Acquisition**

MME的NAS层从Attach Request message获得UE的IMSI和security capability 。

**1.2 Authentication**

鉴权过程发生在UE和MME之间，分为两步：（1）MME从HSS那里为UE获取鉴权向量，此过程走的是MME和HSS之间Diameter协议下的S6a接口；（2）MME和UE相互鉴权，此过程走的是MME和UE之间的NAS协议。

**(1) Acquisition of Authentication Vectors**

**1)** [MME🡪HSS] Authentication Information Request

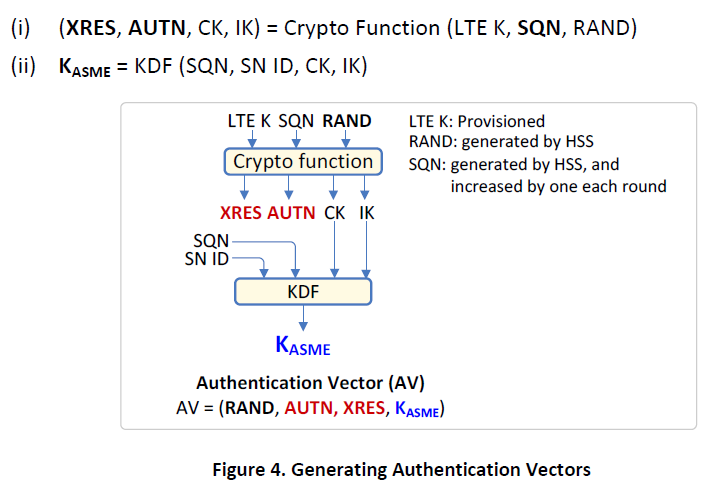
Authentication Information Request (IMSI, SN ID) ：

• IMSI: Subscriber identifier (a fixed value provisioned at HSS for a UE)

• SN ID: indicates the serving network of a subscriber, and consists of an PLMN ID (MCC+MNC)

**2)** [HSS] Generating Authentication Vectors

HSS用IMSI中的LTE K和SN ID来产生鉴权向量。



最后得到的鉴权向量：Authentication Vectors (RAND, AUTN, XRES, KASME)

• RAND: HSS产生这个随机数给UE，UE用这个随机数产生他的鉴权向量；

• AUTN: HSS产生这个鉴证令牌给UE，UE产生产生的鉴权向量中的AUTN与这个HSS给他的进行比较来认证网络。

• XRES: HSS产生这个给MME，MME将拿着这个和UE发送回来的RES进行对比来认证用户。

• KASME: HSS和UE产生这个key用来接入网络，HSS将这个key给MME来使UE接入网络；这个key也是MME和UE产生NAS security keys的基础key。

**3)** [MME 🡨HSS] Delivering Authentication Vectors

HSS将产生的鉴权想向量(RAND, AUTN, XRES, KASME)放在Authentication Information Response (AV4) message 中送给MME，MME用这个信息和UE进行互相认证。

**(2) Mutual Authentication**

LTE需要用户和网络互相认证。MME将鉴权向量{RAND, AUTN, XRES, KASME}中的RAND和AUTN发送给UE，UE用这两个参数产生自己的鉴权向量，用来认证网络，MME自己拿着XRES和KASME来认证UE和产生NAS security key，互相认证的过程如下：

**4)** [UE 🡨MME] Request by MME for User Authentication

MME将Authentication Request (RAND, AUTN, KSIASME) message发送给UE，KSIASME是KASME的index。

**5)** [UE] UE产生鉴权向量并认证网络:UE用RAND产生SQN，用SQN产生自己的

AUTNUE，并与从MME收到的AUTNHSS比较来认证网络，最后将KSIASME存储下来。

**6)** [UE 🡪MME] Delivery of User RES to MME

UE认证完网络后，将自己的RES放在Authentication Response (RES) message里发送给MME，让MME可以认证UE。

**7)** [MME] Network’s Authenticating the UE

MME用从HSS收到的XRES和从UE收到的RES对比来认证UE。

至此，UE和网络（MME）就已经互相认证了，下面，UE和MME将为NAS message建立安全链路。

**1.3 NAS Security Setup**

认证完成后，MME初始化NAS安全设置，来保证NAS信息在UE和MME之间安全的交换。过程如下：

**1)** [MME] Generating NAS Security Keys

MME用从HSS收到的KASME 来产生NAS security keys（NAS integrity key (KNASint) and a NAS encryption key (KNASenc)）；

**2)** [UE 🡨MME] Helping UE to Generate NAS Security Keys

MME发送Security Mode Command (KSIASME, Security Algorithm, NAS-MAC) message给UE，帮助UE产生NAS security keys；

**3)** [UE] Generating NAS Security Keys

UE使用MME给他选择的NAS安全算法来产生NAS security keys（KNASint and KNASenc），若UE产生的KNASint 通过了Security Mode Command message 中的完整检查，则NAS security keys设置成功并且能工作在UE和MME之间。

**4)** [UE 🡪MME] NAS Security Key Generation Complete

UE向MME发送Security Mode Complete (NAS-MAC) message，并且这个信息是经过UE用NAS Security Key来进行加密和完整性保护后的信息。

至此，UE和MME之间的安全性设置已经完成，他们之间传递的信息以后都会被加密和保护完整。

**1.4 Location Update**

当鉴权和NAS安全设置完成后，MME可以注册用户到网络了。MME告诉HSS用户已经被注册到网络并告诉HHS相关的注册信息，并从HSS下载用户相关的信息。这个位置更新的过程走的是MME和HSS之间的S6a接口的Diameter协议：

**1)** [MME 🡪 HSS] Notifying UE Location

MME发送Update Location Request (IMSI, MME ID) message 给HSS，告诉他UE的注册信息并且请求获得UE用户的信息。

**2)** [HSS] UE Location Update

HSS注册MME ID代表着这个UE是位于哪个MME内。

**3)** [MME 🡪HSS] Delivering User Subscription Information

HSS通过Update Location Answer message 发送UE用户信息给MME，MME用UE用户信息来创建EPS会话和默认EPS承载；Update Location Answer (IMSI, Subscribed APN, Subscribed P-GW ID, Subscribed QoS Profile) ：

• Subscribed APN: 指UE要接入的目的网络（wap or net来上网？）；

• Subscribed P-GW ID: 指UE要接入的目的网络所走的P-GW的ID

• Subscribed QoS Profile5 (UE-AMBR(UL/DL), QCI, ARP, APN-AMBR(UL/DL))

- UE-AMBR (UL/DL): the aggregate bandwidth of all non-GBR bearers that a UE can have Determined by MME and controlled by eNB.

- QCI, ARP, APN-AMBR (UL/DL): QoS applied to the Subscribed APN

**4)** [MME] Storing Subscription Information

MME通过Update Location Answer message 接收到用户信息，并存储起来。MME从下载下来的用户信息可以知道用户订阅的服务，哪个APN和分配哪种QoS水平的资源。

**2.5 EPS Session Establishment**

基于用户信息，MME为用户建立EPS会话和EPS默认承载，这样，MME就可以用用户需要的QoS为每一个用户分配网络/无线资源。The MME, based on the subscription information, establishes an EPS session and a default EPS bearer for the user. By doing so, the MME allocates the network/radio resources for providing each user with satisfying QoS they are subscribing to. Figure 7 and Figure 8 illustrate procedures for establishing an EPS session and a default EPS bearer, respectively.

**1) [MME] Assigning EPS Bearer ID**

MME从5~15中选择一个值，并将这个值分配为EPS承载ID（EBI）来为新接入的用户建立默认EPS承载。The MME selects a value from 5~15, and allocates it as an EPS Bearer ID (EBI) in order to establish a default EPS bearer for the newly attached user.

**2) [MME] Selecting P-GW**

MME选择哪个P-GW来接入这个APN。选择P-GW有两种方式：一是MME检查从HSS那里收到的APN，并基于从HSS那里获得的用户的信息，包含有P-GW ID，来选择P-GW；二是若没有这个信息，MME会询问DNS服务器，并得到一个APN和P-GW ID，来选择接入哪个P-GW。The MME checks the APN received from the HSS, and decides to which P-GW to connect to access the APN. This decision can be made based on the subscription information received from the HSS (specifically, P-GW ID). Or if there is no such information, the MME queries the DNS server for APN FQDN (e.g. internet.apn.epc.mnc05.mcc450.3gppnetwork.org), and selects one from the returned P-GW IP address list in accordance with its P-GW selection policies6. At this time, it also chooses which S-GW to go through to get the selected P-GW.

**3) ~ 4) Request for EPS Session Creation**

MME通过向P-GW发送**Create Session Request** message 来请求建立EPS会话和默认EPS承载，这个信息里面包括MME从HSS那里接受到的用户信息，P-GW收到这个信息后会将它用来向PCRF请求建立EPS会话。The MME requests creation of an EPS session and a default EPS bearer by sending a **Create Session Request** message to the P-GW selected in Step 2) above. Here, the MME includes the subscription information it received from the HSS in the message, so that the P-GW can use it when requesting PCRF for EPS session creation. At this time, UE-AMBR is not included as it is to be determined by the MME.

**3) [MME** **S-GW] Request for EPS Session Creation**

MME和S-GW的通信是通过C面GTP协议的S11接口，MME发送**Create Session Request** message给S-GW，参数包括：

**Create Session Request (IMSI, EPS Bearer ID, P-GW IP, APN, Subscribed Profile (QCI, ARP, APN-AMBR (UL/DL)), ECGI, TAI)**

**IMSI**: a fixed subscriber ID

**EPS Bearer ID**: a default EPS bearer ID assigned by MME

**P-GW IP**: an IP address of the P-GW that MME selected for EPS Session/Bearer creation

**APN**: APN that a user is subscribing to

**Subscribed Profile (QCI, ARP, APN-AMBR (UL/DL))**: QoS information to be applied when establishing an EPS default bearer

**ECGI**: a cell in which UE is located

**TAI**: a TA in which UE is located

The MME and the S-GW communicate over S11 interface in the control plane using GTP protocol (GTP-C).7 The MME sends the S-GW selected in Step 2) a **Create Session Request** message, with the following parameters:

**4) [S-GW** **P-GW] Request for EPS Session Creation**

S-GW和P-GW之间的通信是通过C面GTP协议的S5接口。S-GW分配一个下行的S5 TEID（**S5 S-GW TEID**）来建立S5 GTP到P-GW，让P-GW接收**Create Session Request** message，S-GW发送**Create Session Request** message 给P-GW，参数包括：The S-GW and the P-GW communicate over S5 interface in the user and control planes using GTP protocol (UP: GTP-U, CP: GTP-C). The S-GW allocates a downlink S5 TEID (S5 S-GW TEID) to establish S5 GTP to the P-GW indicated in the received **Create Session Request** message. Then, it sends the ID along with other parameters, as included in the **Create Session Request** message, to the P-GW.

**Create Session Request (IMSI, EPS Bearer ID, S5 S-GW TEID, APN, Subscribed Profile (QCI, ARP, APN- AMBR (UL/DL)), ECGI, TAI)**

**5) [S5 Bearer: Downlink]**

第四步完成时，下行的S5 GTP-U隧道就已经建立好了，P-GW就可以发送下行业务给S-GW了，Once Step 4) is completed, the downlink S5 GTP-U tunnel is created, allowing the P-GW to send downlink traffic to the S-GW. In Figures 7 and 8, the entity that allocates and sends a GTP tunnel TEID is marked as “fill” (●), and the one that receives it is marked as “empty” (**○**).

**6) [P-GW] Allocating User IP Address**

当P-GW接收到这个消息的时候，就知道了用户是想接入网络，所以他就给UE分配了一个IP地址，UE可以使用这个IP地址来使用APN。The P-GW, upon receiving the **Create Session Request** message, realizes the user is attempting to access the network again with IMSI. So, it allocates an IP address to the UE so that the UE can use it when using APN.

**7) [P-GW** **PCRF] Notifying of EPS Session Setup**

P-GW和PCRP之间的通信是通过Gx接口的Diameter协议，The P-GW and the PCRF communicate over Gx interface using Diameter protocol. When creating an EPS session for a user, resources allocation and QoS control for the user must be determined based on the services that the user is subscribing to. It is PCRF that is in charge of controlling policies concerning all the users who accessed to the network. So, the P-GW provides the PCRF with subscription information about the user, and obtains the PCRF’s authorization for resources allocation in accordance with the network operator’s policies. From the UE’s subscription information received from the MME, the P-GW gathers information required for the PCRF’s decision-making on the operator’s policies, and sends it to the PCRF through a **CCR (CC-Request)** message. An example of the message is as follows: