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

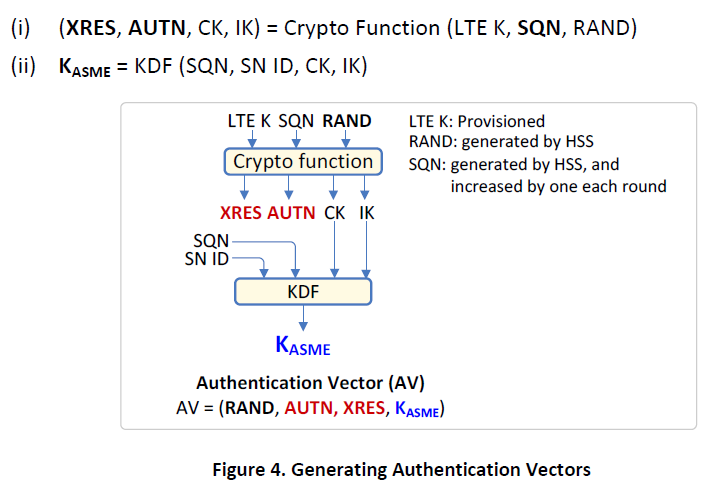
Authentication Information Request (IMSI, SN ID) ：

• 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。

**1.5 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。

**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。

**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。

**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。

**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

**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：

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，

**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。

**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。当为用户创建一个EPS会话时，资源分配和QoS都由PCRF的控制策略所决定，所以，P-GW向PCRF提供用户信息，然后获得PCRF下发的资源分配和QoS；P-GW向PCRF发送CCR (CC-Request) message ：

CCR (IMSI, UE IP, PDN ID (APN), Subscribed QoS Profile (QCI, ARP, APN-AMBR (UL/DL)), ECGI, TAI)

• IMSI: a fixed subscriber ID

• UE IP: an IP address to be used by a user when using services in PDN

• PDN ID: APN to be used by a user

• 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

**8)** [PCRF 🡪SPR] Requesting Access Profiles

PCRF向SPR请求用户的接入配置文件。Profile Request

**9)** [PCRF 🡨SPR] Returning Access Profiles

SPR返回access profile，其中Profile Response参数包括SDF Filter, QCI, ARP, APN-AMBR (UL/DL), Charging Method (e.g. Offline), Changing Reporting Action (e.g. Start Reporting ECGI, TAI), etc 。

**10)** [PCRF] Determining Policies

PCRF产生建立EPS会话的PCC策略。

**11)** [P-GW 🡨PCRF] Acknowledging EPS Session Establishment

PCRF下发PCC策略给P-GW，CCA (CC-Answer) message ：

CCA (IMSI, PCC Rule (SDF Filter, QCI, ARP, APN-AMBR (UL/DL), Charging=Offline, Change Reporting Action (Start Reporting ECGI, TAI))

**12)** [P-GW] Policy Enforcement

P-GW收到PCC策略后，将它用到每个SDF上，然后在SDFs和EPS承载之间建立映射，并准备用在默认EPS承载上的QoS。

**13) ~ 15)** EPS Session Creation Response

P-GW将关于QoS的信息告诉MME，通过发送Create Session Response message 。

**13)** [S-GW 🡨P-GW] EPS Session Creation Response

P-GW分配一个上行S5 TEID (S5 P-GW TEID)来建立到S-GW的S5 GTP，P-GW向S-GW发送Create Session Response message ，参数包括：

Create Session Response (UE IP, EPS Bearer ID, S5 P-GW TEID, Authorized QoS Profile (QCI, ARP, APN-AMBR (UL/DL)), TFT (UL), Change Reporting Action (Start Reporting ECGI, TAI))

**14)** [S5 Bearer: Uplink] S5 Bearer Established

完成13步时，就建立了上行S5 GTP-U隧道，S-GW和P-GW之间就可以互相传输业务了。

**15)** [MME 🡨S-GW] EPS Session Creation Response

S-GW收到P-GW的消息，将S5 P-GW TEID 存储下来，用于上行传输业务；S-GW分配一个S1 GTP隧道的上行S1 TEID (S1 S-GW TEID)，用在S1承载上，并且将S1 S-GW TEID 发送给MME Create Session Request message

**16)** [MME] Why MME Keeps S5 P-GW TEID?

当UE的位置更新的时候，S-GW可能会改变，MME保存S5 P-GW TEID 是为了通知UE新的S-GW。

**17)** [S1 Bearer: Uplink]

完成第15步时就建立了上行S1 GTP-U的隧道，但是eNB还没有拿到S1 S-GW TEID ，所以eNB还不能向S-GW发送数据。

**18)** [MME] Calculating UE-AMBR

MME计算UE-AMBR ，AMBR可以被运营商用来限制签约用户的总速率，它不是针对某一个Bearer，而是针对一组Non－GBR的Bearer。

**19)** Determining Information needed for E-RAB and NAS Signaling

收到S-GW的消息后，MME就可以将资源分配给UE了。MME可以设置E-RAB（DRB+S1 bearer数据无线承载和S1承载），并控制S-gW和eNB。MME向UE发送Attach Accept ：

•给UE分配GUTI来代替IMSI

•产生控制TAU (TAI list allocation, TAU Timer value)的参数

•为eNB’s use产生UE-AMBR

•分配一个E-RAB ID

**20)** [UE 🡨MME] Attach Accept

Attach Accept message 是嵌在Initial Context Setup Request message和RRC Connection Reconfiguration message两条信令里面的，Attach Accept message ：

UE IP address allocated by the P-GW, the GUTI, TAI list, EPS Bearer ID, UE-AMBR values allocated by itself, and QoS parameters received from the S-GW

**21)** [MME] Creating KeNB

MME产生KeNB,用于接入层的安全连接，为了保证eNB和UE之间的无线连接的安全。

**22)** [eNB 🡨 MME] Requesting E-RAB Setup

MME向eNB发送Initial Context Setup Request message 来让eNB和S-GW建立S1承载，eNB和UE建立DRB（数据无线承载），参数包括：

Initial Context Setup Request (UE-AMBR (UL/DL), E-RAB ID, E-RAB QoS (QCI, ARP), S1 S-GW TEID, KeNB, , UE Security Algorithm, NAS-PDU)

• UE-AMBR(UL/DL): QoS parameter that can only be controlled by eNB (because a user uses the same eNB no matter what APN the user is using)

• E-RAB ID: allocated by MME, and used by eNB as an EPS bearer ID

• E-RAB QoS: determined by MME based on the EPS bearer QoS received from P-GW

• S1 S-GW TEID: uplink S1 TEID value received from S-GW

• KeNB: generated by MME from KASME, and used by eNB for derivation of AS security keys

• UE Security Algorithm: included in the Attach Request message received from UE, and used by eNB along with KeNB for AS security setup.

• NAS-PDU: NAS message (Attach Accept)

**23)** [S1 Bearer: Uplink]

第22步完成后，eNB收到了S1 S-GW TEID ，所以eNB可以向S-GW上传业务了。

**24) ~ 27)** AS Security Setup

eNB接收到MME的信息后，eNB就会和UE通信来建立DRB，但是为了保证通信的安全性，eNB要进行接入层安全设置。

**24)** [eNB] Generating AS Security Keys

eNB从收到的KeNB来产生AS security keys(KRRCint, KRRCenc and KUPenc)。

**25)** [UE 🡨 eNB] Helping UE to Generate AS Security Keys

eNB向UE发送Security Mode Command (AS Security Algorithm, MAC-I) message ，来帮助UE产生AS security keys (KRRCint，KRRCenc and KUPenc)。

**26)** [UE] Generating AS Security Keys

UE产生AS security keys用eNB帮它选择的AS security算法。

**27)** [UE 🡪 eNB] AS Keys Generation Complete

经过第26步后，AS security keys 就在UE和eNB之间成功设置了。UE向eNB发送Security Mode Complete (MAC-I) message 来告诉eNB我ok了，之后UE和eNB之间的RRC消息就是被加密和完整性保护了。

**28) ~ 29)** DRB Establishment

**28)** [UE 🡨 eNB] Reconfiguring RRC Connection

eNB分配上下行DRB IDs，然后配置DRB的QoS参数，用来建立无线连接的EPS承载。完了再通过安全保护的RRC送法RRC Connection Reconfiguration message给UE，RRC连接是在UE发送附着请求时就已经建立，但是，现在必须要重新配置参数，RRC连接要依照网络的下发的参数来配置，才能接入网络。过程是：UE的RRC层收到RRC Connection Reconfiguration message，对RRC连接参数进行重新配置；然后将这个信令里面的Attach Accept message 里取出来发送到NAS层，UE的NAS层收到这条消息的时候，它就获得了UE IP地址和GUTI，并用于之后的通信。

**29)** [DRB Establishment: Uplink and Downlink] DRB Establishment Complete

第28步完成后，UE就能和eNB进行上下行的业务传输了。

**30)** [eNB] Allocating a Downlink TEID for S1 Bearer

第28步完成后，eNB为S1承载分配一个下行的TEID，用来建立下行S1 GTP-U隧道。

**31)** [eNB 🡪 S-GW] E-RAB Setup Response

eNB为S1承载分配一个下行的S1 TEID (S1 eNB TEID)，然后将这个TEID通过Initial Context Setup Response message 发送给MME，MME则可以将这个TEID发送给S-GW。

**32)** [UE 🡪 MME] Sending Attach Complete Message

UE发送Attach Complete message给MME。

**33)** [UE][MME] EMM State

现在UE和MME都保持着EMM注册状态。

**34)** [MME 🡪 S-GW] Requesting S1 Bearer Modification

MME将S1 TEID (S1 eNB TEID)包含在Modify Bearer Request message发送给S-GW。

**35)** [MME 🡨 S-GW] Responding to S1 Bearer Modification Request

S-GW向MME发送Modify Bearer Request message作为回应MME自己收到了，现在S-GW可以向eNB发送下行业务了。

**36)** [S1 Bearer: Downlink] S1 Bearer Setup Complete

第35步完成后，S1承载就建立完成了，eNB和S-GW可以见互相传输业务了。截至目前，默认EPS承载就建立完成，UE和P-GW可以完整的通信了。