

EMM Procedure 1. Initial Attach

Part 2. Call Flow of Initial Attach

Table of Contents

- I. Introduction
- II. Initial Attach Procedure
- III. EPS Entity Information: Before/After Initial Attach
- IV. Closing

This document, Part 2 of Initial Attach, discusses detailed initial attach procedures in EMM Case 1. EMM Case 1 concerns initial attach procedures for a user attaching to a network for the first time, as categorized as Attach Case 1 in Part 1. Below, we will provide a description of those procedures and their related function blocks explained in Part 1. We will also summarize what kinds of information are set in the EPS entities after the procedures.

January 16, 2014

(Initial Released: September 22, 2011)

www.netmanias.com

NMC Consulting Group (tech@netmanias.com)

About NMC Consulting Group

NMC Consulting Group is an advanced and professional network consulting company, specializing in IP network areas (e.g., FTTH, Metro Ethernet and IP/MPLS), service areas (e.g., IPTV, IMS and CDN), and wireless network areas (e.g., Mobile WiMAX, LTE and Wi-Fi) since 2002.
Copyright © 2002-2014 NMC Consulting Group. All rights reserved.

Netmanias LTE Technical Documents

Visit <http://www.netmanias.com> to view and download more technical documents.

Index	Topic	Document Title	Document presented here
1	Network Architecture	LTE Network Architecture: Basic	
2	Identification	LTE Identification I: UE and ME Identifiers	
3		LTE Identification II: NE and Location Identifiers	
4		LTE Identification III: EPS Session/Bearer Identifiers	
5	Security	LTE Security I: LTE Security Concept and LTE Authentication	
6		LTE Security II: NAS and AS Security	
7	QoS	LTE QoS: SDF and EPS Bearer QoS	
8	EMM	LTE EMM and ECM States	
9		Eleven EMM Cases in an EMM Scenario	
10		LTE EMM Procedure 1. Initial Attach - Part 1. Cases of Initial Attach	
11		LTE EMM Procedure 1. Initial Attach - Part 2. Call Flow of Initial Attach	O
12		LTE EMM Procedure 2. Detach	
13		LTE EMM Procedure 3. S1 Release	
14		LTE EMM Procedure 4. Service Request	
15		LTE EMM Procedure 5. Periodic TAU	
16		LTE EMM Procedure 6. Handover without TAU - Part 1. Overview of LTE Handover	
17		LTE EMM Procedure 6. Handover without TAU - Part 2. X2 Handover	
18		LTE EMM Procedure 6. Handover without TAU -Part 3. S1 Handover	
19		LTE EMM Procedure 7. Cell Reselection without TAU	
20		LTE EMM Procedure 8 & 9. Handover and Cell Reselection with TAU	
21		LTE EMM Procedure 10 & 11. Move to Another City and Attach	
22	PCC	LTE Policy and Charging Control (PCC)	
23	Charging	LTE Charging I: Offline	
24		LTE Charging II: Online (TBD)	
25	IP Address Allocation	LTE IP Address Allocation Schemes I: Basic	
26		LTE IP Address Allocation Schemes II: A Case for Two Cities	

Abbreviations

AKA	Authentication and Key Agreement
AMBR	Aggregated Maximum Bit Rate
ASME	Access Security Management Entity
EMM	EPS Mobility Management
EPS	Evolved Packet System
GUTI	Globally Unique Temporary Identifier
HSS	Home Subscriber Server
IMSI	International Mobile Subscriber Identity
LTE	Long Term Evolution
MM	Mobility Management
MME	Mobility Management Entity
NAS	Non Access Stratum
NAS-MAC	Message Authentication Code for NAS for Integrity
TAI	Tracking Area Identity
UE	User Equipment

I. Introduction

Now, we will look into EMM Case 1: Initial Attach by Unknown UE [1]. This case is when a user turns on his UE and attempts to attach to a network for the first time after subscribing to the LTE network/service. It was previously categorized as Attach Case 1 in Part 1 [2].

This document, Part 2, is organized as follows: Chapter II explains the detailed procedures in EMM Case 1 (Initial Attach with IMSI), focusing on the functions required in the case, as described in Part 1. Chapter III summarizes what information is changed in each EPS entity after initial attach in Attach Case 1.

II. Initial Attach Procedure

Figure 1 illustrates initial attach procedures in EMM Case 1, along with function blocks required in each procedure, as defined in Part 1.

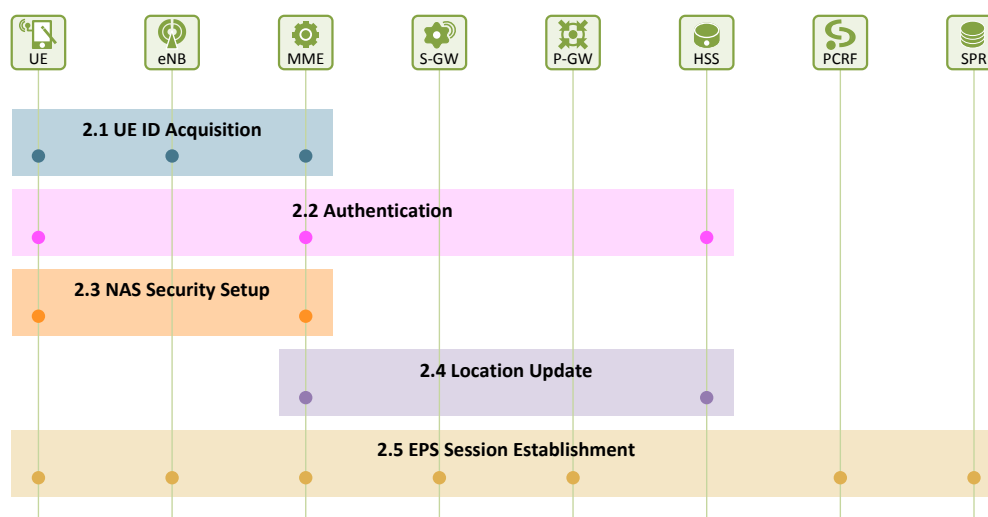


Figure 1. Summary of Initial Attach Procedures

2.1 IMSI Acquisition

Figure 2 shows the first step in the procedures. By the end of this first step, the MME obtains an IMSI from the UE. The UE attempts to initially attach to the network by sending an **Attach Request** message, with its IMSI in it, and the MME obtains the IMSI from the message. For the purpose of explanation, this step can be further divided into two sub-steps: ① the UE stays in the initial state after radio link synchronization, and ② the UE establishes ECM connection for delivering an **Attach Request** message to the MME. The ECM connection establishment phase can be further divided into two sub-phases: (1) RRC connection establishment, and (2) S1 signaling connection establishment.

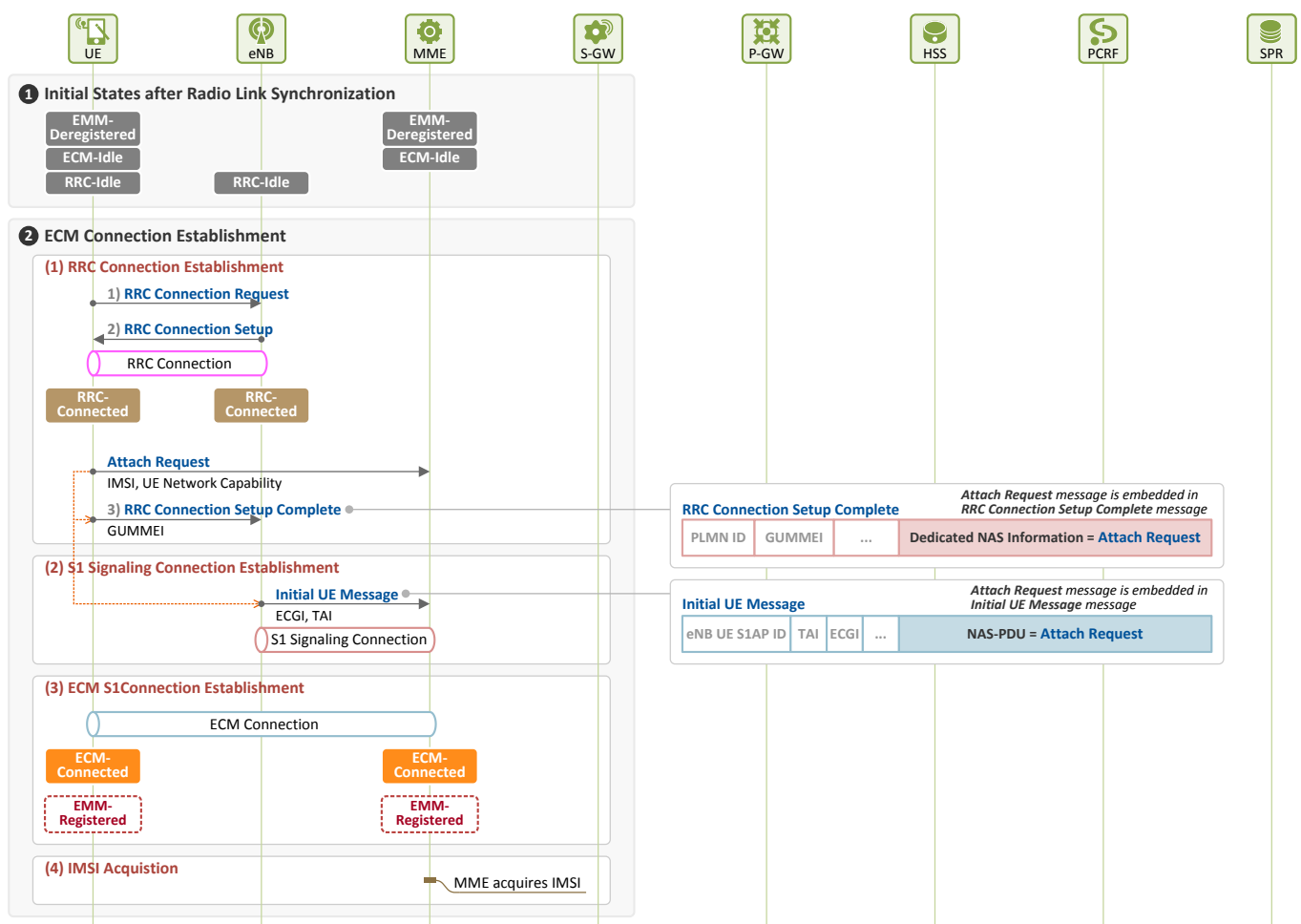


Figure 2. Procedure for IMSI Acquisition

① Initial State after Radio Link Synchronization

In order for a UE to request initial attach to a network, communication with an eNB is essential. So, the UE selects an eNB (cell) through PLMN selection and cell search procedures, and has the radio link synchronized (PLMN selection and cell search procedures are out of the scope of this document, and thus will not be covered here). Then, the user can communicate with the eNB. At this time, the UE is in EMM-Deregistered, ECM-Idle, and RRC-Idle state.

② ECM Connection Establishment

On NAS layer, the UE sends an **Attach Request** (including **IMSI** and **UE Network Capability**) message to

request initial attach to the NAS layer of the MME.

In order for the **Attach Request** message to be delivered, ECM connection is required between the UE and the MME. And for the ECM connection, RRC connection between the UE and the eNB, and S1 signaling connection between the eNB and the MME are required. NAS messages are sent as RRC messages (**RRC Connection Setup Complete** message) when passing through the RRC connection, and then as S1AP messages (**Initial UE Message**) through the S1 signaling connection.

(1) RRC Connection Establishment

An RRC connection is established between the RRC layers of the UE and the eNB. Once established, the connection is used when delivering messages to the RRC layers or their upper layers, NAS layers, in the control plane. The procedure for establishing an RRC connection is as follows:

1) [UE → eNB] RRC Connection Request

An UE requests an RRC connection by sending an **RRC Connection Request (Establishment Cause=“Mobile Originating Signaling”)** message to an eNB. The “Mobile Originating Signaling” is a value used in the Establishment Cause field when a UE requests Attach, Detach or TAU (Tracking Area Update). The message sent by the UE is delivered to the eNB through SRB 0, the SRB (Signaling Radio Bearer) used by all UEs in a cell, and CCCH (Common Control Channel), a logical channel.

2) [UE ← eNB] RRC Connection Setup

The eNB allocates a SRB (SRB1) dedicated to the UE by sending the UE an **RRC Connection Setup** message, which is delivered through SRB 0 and CCCH. The uplink/downlink radio resources of the UE are controlled by the eNB. So, after completing this step, the UE can use the radio resources by using the SRB configuration allocated through the **RRC Connection Setup** message. Then it transits to EMM-Deregistered, ECM-Idle and RRC-Connected state.

3) [UE → eNB] RRC Connection Setup Complete

The UE notifies the eNB that the RRC connection setup is completed by sending it an **RRC Connection Setup Complete** message through SRB 1 and DCCH (Dedicated Control Channel). For efficient delivery, the **Attach Request** message¹ that was delivered to the NAS layer is sent to the eNB when delivering the **RRC Connection Setup Complete** message, as embedded in the Dedicated NAS Information field (DedicatedInfoNAS) of the **RRC Connection Setup Complete** message.

(2) S1 Signaling Connection Establishment

Control messages between the eNB and the MME are sent over S1-MME interface as embedded in S1AP messages. S1AP messages are delivered through S1 signaling connections dedicatedly established for each user. The S1 signaling connections are defined by an ID pair (eNB UE S1AP ID, MME UE S1AP ID) allocated by the eNB and the MME for identifying UEs.

In Figure 2, an **Attach Request** message, the first NAS message, arrives at the eNB before S1 signaling connection is established. The eNB then allocates an eNB UE S1AP ID for establishment of S1 signaling

¹ This Attach Request message is an EMM message, and includes PDN Connectivity Request message, an ESM message, when being sent. This document concerns EMM only, and thus ESM messages embedded in EMM messages are not discussed in the document. However, their parameters are mentioned here as needed.

connection, and sends the MME an **Attach Request** message, as embedded in an **Initial UE Message**. The **Attach Request** message is delivered as embedded in the NAS-PDU field of the **Initial UE Message**. The **Initial UE Message** consists of the following information elements:

Initial UE Message (eNB UE S1AP ID, NAS-PDU, TAI, ECGI, RRC Establishment Cause)

- **eNB UE S1AP ID**: ID identifying UEs in an eNB over S1-MME interface (Uplink)
- **NAS-PDU**: a NAS message (**Attach Request**)
- **TAI**: shows the TA a UE is located in
- **ECGI**: shows the cell a UE is located in
- **RRC Establishment Cause = mo-Signaling**: indicates the signaling was generated by a UE

When the MME receives the **Initial UE Message** from the eNB over S1-MME, it allocates an MME S1AP UE ID for the UE. Now with this newly allocated ID and the previously allocated eNB UE S1AP ID, S1 signaling connection between the two entities are established. The MME UE S1AP ID is used later when the MME identifies UEs over S1-MME interface (Downlink).

(3) ECM S1 Connection Establishment

Through Steps (1) and (2) above, the ECM connection between the NAS layers of the UE and the MME is established. Then, the UE transits to EMM-Registered², ECM-Connected and RRC-Connected state.

(4) IMSI Acquisition

The NAS layer of the MME acquires the IMSI of the UE from the **Attach Request** message sent from the NAS layer of the UE, and finds out the UE's security capability by learning what security algorithms the UE can use from the UE's network capability information.

After collecting the UE's IMSI and security capability information from the **Attach Request (IMSI, UE Network Capability)** message received from the UE, the MME performs the authentication and NAS security Setup procedures for secured delivery of NAS messages, by using the collected information, and in accordance with the EPS-AKA (Evolved Packet System-Authentication and Key Agreement). The two procedures - authentication and NAS security setup - are described in Sections 2.2 and 2.3, respectively. As they are already explained in details in our LTE Security documents [3][4], they will be discussed briefly here in this document.

² To be accurate, the UE is in EMM-Registered-Initiated state. However, since this document defines the EMM state as either EMM-Deregistered or EMM-Registered, the UE is considered to be in EMM-Registered state.

2.2 Authentication

Authentication procedure between a UE and a network (MME) is described in Figure 3. The procedure consists of the following two steps: Step (1), authentication vector acquisition, during which the MME acquires authentication vectors from the HSS for the UE, and Step (2), mutual authentication, during which the MME and the UE are mutually authenticated. Step (1) is performed over the S6a interface between the MME and the HSS using Diameter protocol, while Step (2) is performed between the UE and the MME using a NAS protocol.

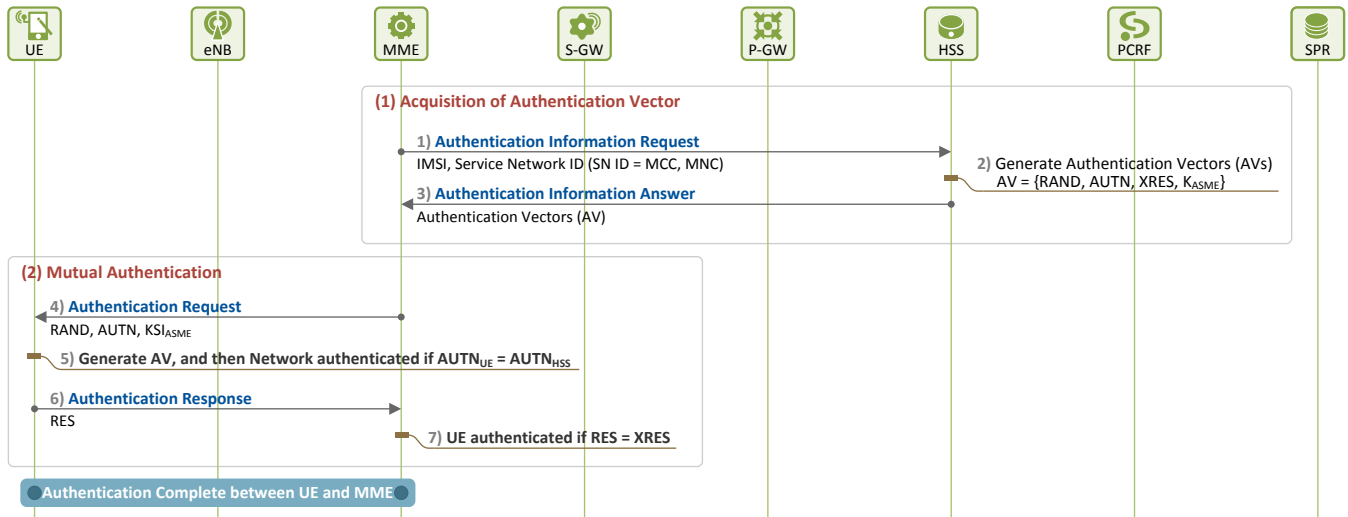


Figure 3. Procedure for Authentication

(1) Acquisition of Authentication Vectors

1) [MME → HSS] Authentication Information Request

The MME sends the HSS an **Authentication Information Request** message, requesting authentication vector(s) (AV) for the UE that has an IMSI. At this time, it includes the UE's SN ID (Serving Network ID) along with the IMSI in the message to make sure the HSS reflects the UE's current serving network information (i.e. which operator's network the UE is using) when generating authentication vectors for the UE. Main parameters in the **Authentication Information Request** message are:

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

The HSS³ generates authentication vectors by using the LTE master key (LTE K) in the IMSI and the serving network ID (SN ID) of the UE. Authentication vectors are generated through the two steps as seen in Figure 4. First, the HSS generates SQN and RAND, and then inputs the values of {LTE K, SQN, RAND} in the crypto function to generate the values of {XRES, AUTN, CK, IK}. Next, it inputs the values of {SQN, SN ID, CK, IK} in the key derivation function to derive K_{ASME}.

³ As in the LTE Security I document, AuC and HSS are collectively referred to as HSS for the sake of convenience in this document.

- (i) $(XRES, AUTN, CK, IK) = \text{Crypto Function}(\text{LTE K}, SQN, RAND)$
- (ii) $K_{ASME} = \text{KDF}(SQN, SN\ ID, CK, IK)$

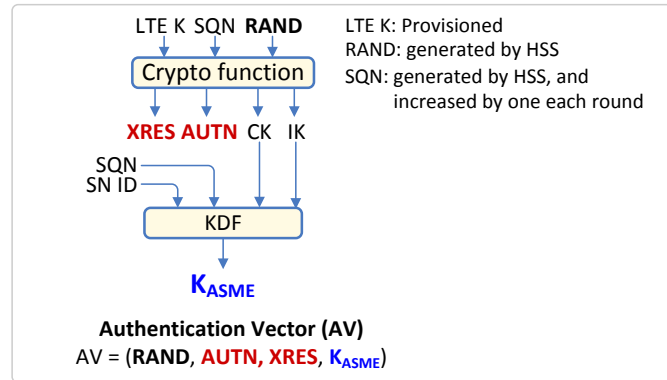


Figure 4. Generating Authentication Vectors

The final form of authentication vectors is $\{RAND, AUTN, XRES, K_{ASME}\}$, and the roles of each authentication vector element are as follows:

Authentication Vectors (RAND, AUTN, XRES, K_{ASME})

- **RAND**: a random number generated by HSS and delivered to UE. The UE uses it when generating its authentication vectors.
- **AUTN**: an authentication token generated by HSS and also delivered to UE. The UE, after generating its authentication vectors, compares the value of this token with that of the token it generates itself for authenticating a network.
- **XRES**: a value generated by HSS. MME keeps this value to itself without sending it to UE, and then later compares it with RES sent by the UE after network authentication to authenticate a user.
- **K_{ASME}**: the top-level key in an access network, generated by UE and HSS, and delivered by the HSS to MME for its use in the access network. It serves as a base key of MME and UE when generating NAS security keys.

3) [MME ← HSS] Delivering Authentication Vectors

The HSS sends the authentication vectors, as included in the **Authentication Information Response (AV⁴)** message to the MME. The MME then uses this information to perform mutual authentication with the UE in Step (2).

(2) Mutual Authentication

LTE requires mutual authentication between a user and the network. So, a user must authenticate the network, and the network must authenticate the user. Once the MME received authentication vectors $\{RAND, AUTN, XRES, K_{ASME}\}$ from the HSS, it sends RAND and AUTN on to the UE so that the UE can generate authentication vectors, and authenticate the network. However, the MME keeps XRES and K_{ASME} to use for user authentication and NAS security key derivation, respectively. K_{ASME} is not passed on to the UE (but generated when the UE generates authentication vectors), but KSI_{ASME}, an index for K_{ASME}, is delivered to the UE, instead. Mutual authentication procedures between the UE and MME are

⁴ HSS may generate more than one authentication vectors (AV) and deliver them to MME. However, only one authentication vector is assumed in this document.

as follows:

4) [UE ← MME] Request by MME for User Authentication

The MME delivers the information (RAND, AUTN) required for the UE to generate authentication vectors, and KSI_{ASME} , as included in the **Authentication Request (RAND, AUTN, KSI_{ASME})** message to the UE.

5) [UE] User's Authenticating the Network: Generating Authentication Vectors and Authenticating the Network

After receiving the **Authentication Request (RAND, AUTN, KSI_{ASME})** message from the MME, the UE first generates SQN from AUTN, and then authentication vectors as the HSS did (in Figure 4). Next, the UE compares its own AUTN ($AUTN_{UE}$) and the AUTN received from the MME ($AUTN_{HSS}$) to authenticate the network, and stores KSI_{ASME} as an index of K_{ASME} .

6) [UE → MME] Delivery of User RES to MME

After completing network authentication by comparing the AUTN values, the UE sends its own RES value to the MME, as included in the **Authentication Response (RES)** message, so that the MME can authenticate the user.

7) [MME] Network's Authenticating the UE

Upon the receipt of the **Authentication Response (RES)** message from the UE, the MME compares the RES value generated by the UE and the XRES value it received from the HSS, to authenticate the user.

Once the above steps are completed, the UE and the network (MME) are mutually authenticated. Now, the two begins the procedure for establishing NAS security setup for secured delivery of NAS messages.

2.3 NAS Security Setup

Once user authentication is completed, the MME initiates the NAS security setup procedure so that NAS messages can be securely exchanged between the two entities. Figure 5 shows the call flows in the NAS security setup procedure.

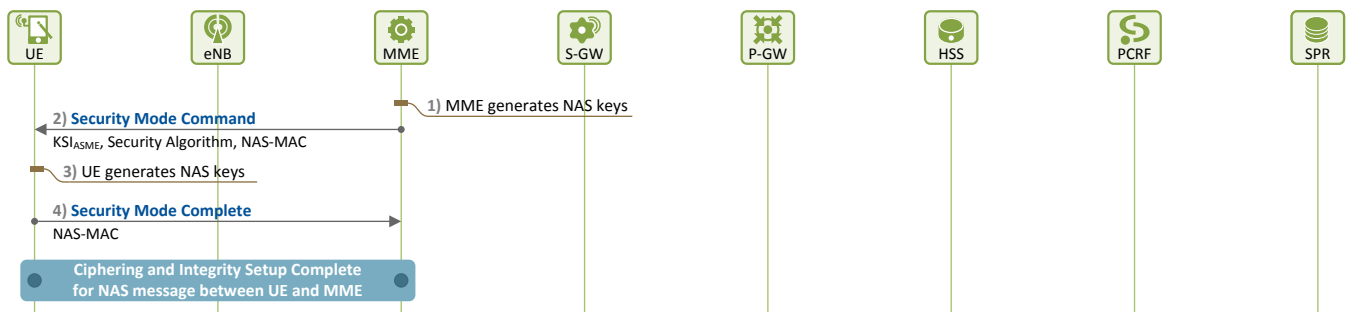


Figure 5. Procedure for NAS Security Setup

1) [MME] Generating NAS Security Keys

The MME selects ciphering and integrity algorithms to be applied to NAS messages from the **Attach Request** message received from the UE. Next, it derives a NAS integrity key (K_{NASint}) and a NAS encryption key (K_{NASenc}) from K_{ASME} , to be applied to NAS messages.

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

The MME informs the UE of the selected security algorithms, by including them in a **Security Mode Command** (KSI_{ASME} , **Security Algorithm**, **NAS-MAC**) message, helping the UE to generate NAS security keys. The message is sent with its integrity-protected (by including NAS-MAC).

3) [UE] Generating NAS Security Keys

When the UE receives the **Security Mode Command** message, the UE generates NAS security keys (K_{NASint} and K_{NASenc}) by using the NAS security algorithm that the MME selected, and performs an integrity validation on the **Security Mode Command** message by using the NAS integrity key (K_{NASint}). If the message passes the integrity check, it can be seen that the NAS security keys are successfully set and properly working between the two entities.

4) [UE → MME] NAS Security Key Generation Complete

The UE informs the MME of the successful generation of NAS security keys by sending a **Security Mode Complete** (**NAS-MAC**) message, after having it encrypted and integrity protected using the generated keys.

After completing the above steps, the procedure for NAS security setup between the two entities ends. Then messages between the two thereafter are securely delivered, as encrypted and integrity-protected.

2.4 Location Update

Once the procedures for authentication and NAS security setup are completed, now the MME has to register the subscriber in the network, and find out what services the subscriber can use. To this end, the MME notifies the HSS the subscriber is registered in the network and located in its TAs, and then downloads information about the subscriber from the HSS. All these are done through the location update procedure, and by using Diameter protocol over the S6a interface between the MME and the HSS. The call flows during this procedure are as in Figure 6.

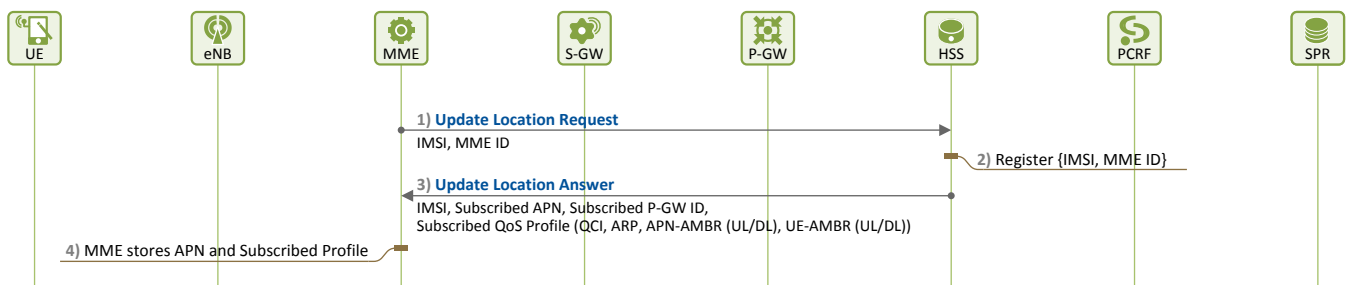


Figure 6. Procedure for Location Update

1) [MME → HSS] Notifying UE Location

The MME sends an **Update Location Request (IMSI, MME ID)** message to the HSS in order to notify of the UE's registration and obtain the subscription information of the UE.

2) [HSS] UE Location Update

The HSS registers the MME ID to indicate in which MME the UE is located in.

3) [MME ← HSS] Delivering User Subscription Information

The HSS sends the MME subscription information of the subscriber as included in an **Update Location Answer** message, so that the MME can create an EPS session and a default EPS bearer for the subscriber. The subscription information included in the **Update Location Answer** message is as follows:

Update Location Answer (IMSI, Subscribed APN, Subscribed P-GW ID, Subscribed QoS Profile)

- **Subscribed APN:** APN that a user is subscribing to (e.g. Internet service)
- **Subscribed P-GW ID:** an ID for P-GW through which a user can access the Subscribed APN
- **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

The MME receives the **Update Location Answer** message from the HSS, and stores the subscription information from the message.

From the downloaded subscription information, the MME can check what services the user is subscribing to, and to which APN and with what QoS level the resources are to be allocated.

⁵ For more information, see our technical document, "LTE QoS: SDF and EPS Bearer QoS" [5].

2.5 EPS Session Establishment

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.

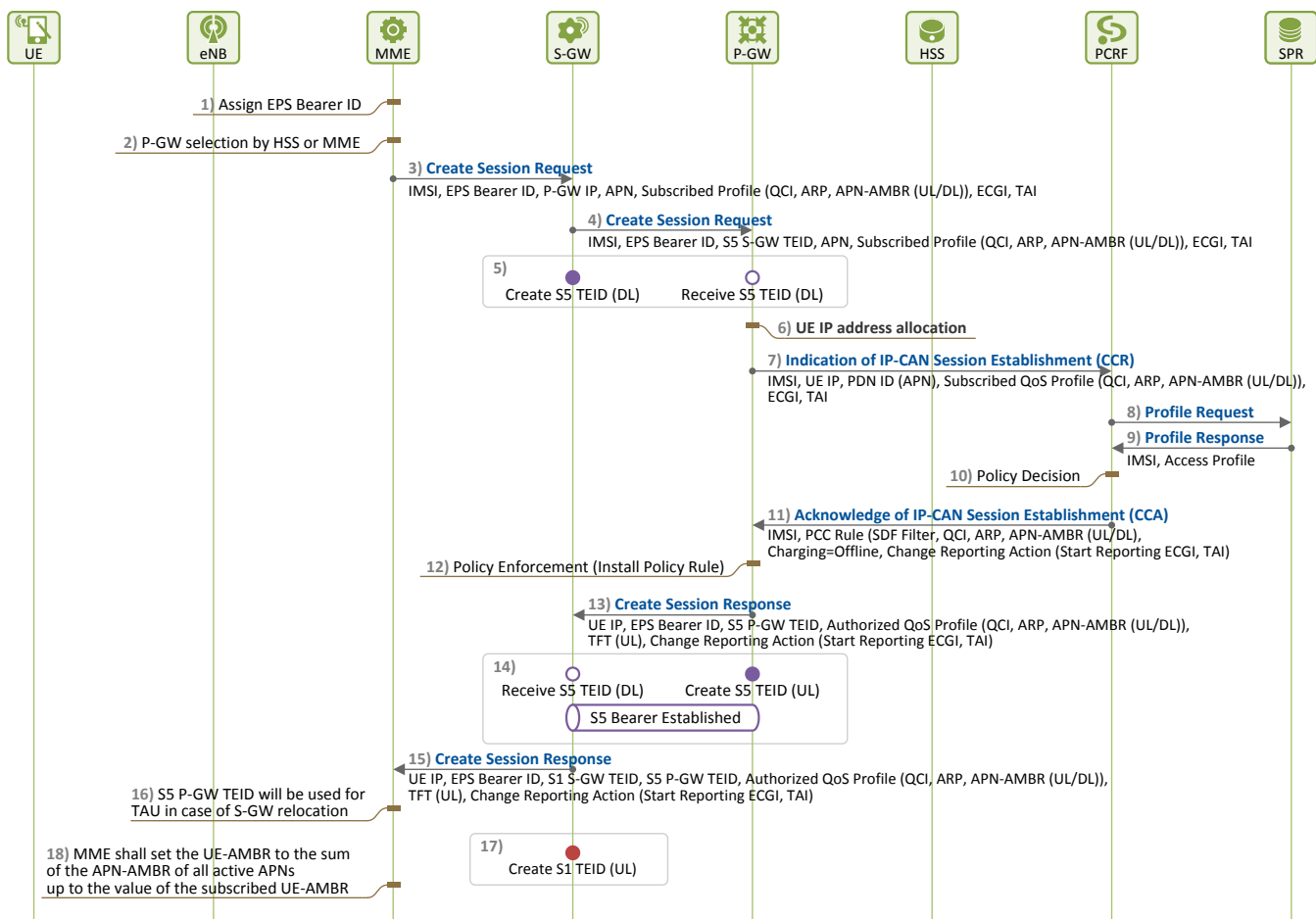


Figure 7. Procedure for EPS Session Establishment (1)

1) [MME] Assigning EPS Bearer ID

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

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.

⁶ The P-GW selection policies are out of the scope of this document, and hence will not be discussed here.

3) ~ 4) Request for EPS Session Creation

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

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:

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

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]

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

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

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

⁷ For the purpose of simpler description, when discussing parameters relating to GTP tunnel establishment, only values on the user plane (GTP-U) will be mentioned, and those on the control plane (GTP-C) will not.

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:

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

The PCRF requests the SPR for the user's access profile to determine PCC policies for the user.

9) [PCRF ← SPR] Returning Access Profiles

The SPR returns an access profile for the user. The profile may include information such as 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

The PCRF determines PCC policies for the EPS session to be established based on the user access profile.

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

The PCRF delivers the PCC policies determined in Step 10) to the P-GW, as included in a **CCA (CC-Answer)** message. An example of the message is as follows:

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

The P-GW applies the PCC policies received from the PCRF. As the PCC policies are applied to each SDF, the P-GW sets up mapping between SDFs and the EPS bearer, and prepares a QoS profile to be applied to the default EPS bearer (see our technical document, "LTE QoS: SDF and EPS Bearer QoS"[5] for more information).

13) ~ 15) EPS Session Creation Response

The P-GW informs the MME of the QoS information applied to the established EPS sessions and default EPS bearer, by sending it in a **Create Session Response** message. The PCRF may decide to keep the value the MME received from the HSS, or select a new value.

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

The P-GW allocates an uplink S5 TEID (S5 P-GW TEID) for establishing S5 GTP to the S-GW. It then includes the S5 P-GW TEID and the QoS profile to be applied to the default EPS bearer (S5 bearer) in the **Create Session Response** message, and sends it to the S-GW as a response to the **Create Session Request** message received in Step 4).

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

Completing Step 13) establishes the uplink S5 GTP-U tunnel, allowing the S-GW to exchange uplink/downlink traffic with the P-GW.

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

When receiving the **Create Session Response** message from the P-GW, the S-GW keeps the uplink S5 TEID (S5 P-GW TEID) to be used for uplink traffic, and allocates an uplink S1 TEID (S1 S-GW TEID) of S1 GTP tunnel to be used for S1 bearer. After processing the message, the S-GW adds the newly allocated S1 S-GW TEID to the processed message, and sends it to the MME as a response to the **Create Session Request** message it received in Step 3).

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

Once attached to a network, if a UE performs a TAU or handover, its S-GW may be changed. For this reason, the MME informs the UE's new S-GW of the uplink S5 TEID so that the new S-GW can deliver uplink traffic to the P-GW.

17) [S1 Bearer: Uplink]

Completing Step 15) establishes the uplink S1 GTP-U tunnel. However, since the eNB does not have this value (S1 S-GW TEID) yet, it cannot deliver uplink traffic to the S-GW at this time.

18) [MME] Calculating UE-AMBR

Now, the MME returns an **Attach Accept** message to the UE as a response to the **Attach Request** message, and prepares for E-RAB setup (i.e. for allocating resources to radio link and S1 bearer) by controlling the eNB. For this, the MME calculates the UE-AMBR value to send to the eNB. The MME has already received the UE-AMBR value, as included in subscription information, from the HSS in Section 2.4 above. However, it can adjust the value to the extent not exceeding the total APN-AMBR of each APN, and allocates it instead.

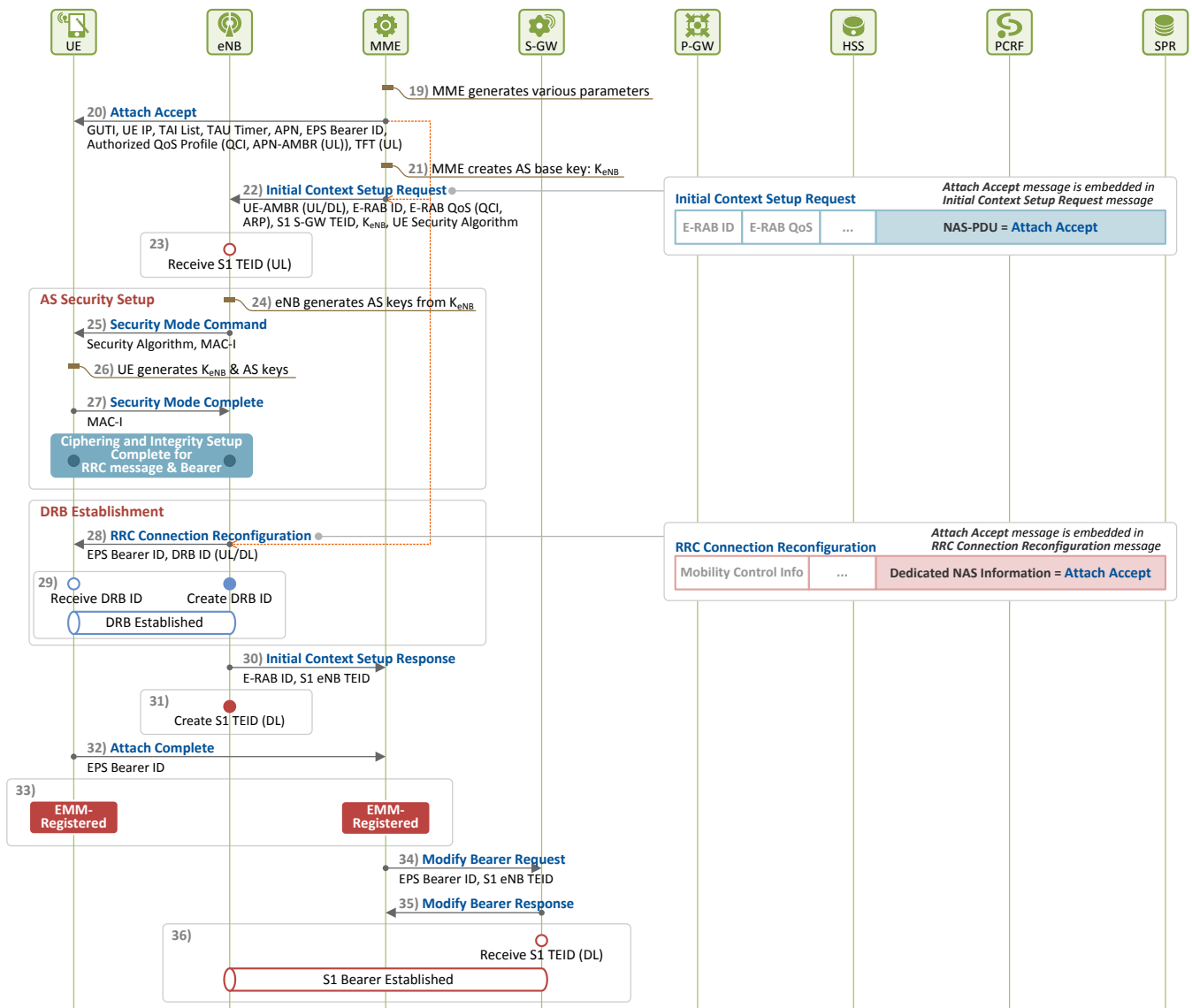


Figure 8. Procedure for EPS Session Establishment (2)

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

By receiving the **Create Session Response** message from the P-GW, the MME learns resources have been approved and allocated to the user. Then, it becomes in charge of E-RAB (DRB+S1 bearer) setup, and controls the eNB and the S-GW. To this end, it determines the resources required for E-RAB setup and the information needed for NAS signaling (**Attach Accept**) as follows:

- Allocating a GUTI that the UE can use instead of the IMSI
- Determining parameters related to controlling TAU (TAI list allocation, TAU Timer value)
- Determining UE-AMBR for the eNB's use
- Allocating an E-RAB ID

20) [UE ← MME] Attach Accept

The MME includes information, such as the 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, in

the **Attach Accept** message⁸, and sends it to the UE as a response to the **Attach Request** message received in Section 2.1.

This message is delivered as included in the **Initial Context Setup Request** message through the S1 signaling connection, and then in the **RRC Connection Reconfiguration** message through the RRC connection.

21) [MME] Creating K_{eNB}

The MME creates K_{eNB} , the AS security base key, from K_{ASME} . This is to ensure the eNB can generate AS security keys to be used for secured communication between the eNB and the UE over radio link (i.e. for AS security setup).

22) [eNB ← MME] Requesting E-RAB Setup

The MME sends an **Initial Context Setup Request** message so that the eNB can establish S1 bearer with the S-GW, and DRB with the UE. The **Initial Context Setup Request** message consists of the following information elements:

Initial Context Setup Request (UE-AMBR (UL/DL), E-RAB ID, E-RAB QoS (QCI, ARP), S1 S-GW TEID, K_{eNB} , 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
- **K_{eNB}** : generated by MME from K_{ASME} , 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 K_{eNB} for AS security setup.
- **NAS-PDU**: NAS message (**Attach Accept**)

23) [S1 Bearer: Uplink]

Once Step 22) is completed, and the S1 S-GW TEID is obtained, the eNB can deliver uplink traffic to the S-GW.

When the eNB receives the MME's **Initial Context Setup Request** message that requests E-RAB setup, it sets up DRB by sending an **Attach Accept** message to the UE. Then, it completes S1 bearer setup by including a downlink S1 TEID in the **Initial Context Setup Response** message, and sending the message as a response to the **Initial Context Setup Request** message to the MME, so that the MME can forward it to the S-GW.

24) ~ 27) AS Security Setup

Upon receiving the MME's **Initial Context Setup Request** message, the eNB attempts to communicate with the UE to set up DRB. To ensure secured communication over the radio link, the eNB performs the procedure for AS security setup before sending messages to the UE (see our technical document, "LTE Security II: NAS and AS Security"[3] for more information).

⁸ This Attach Accept message is an EMM message, and includes Activate Default EPS Bearer Context Request message, an ESM message, when being sent.

24) [eNB] Generating AS Security Keys

The eNB generates AS security keys from K_{eNB} received from the MME for safe delivery of RRC messages and user traffic to/from the UE. The eNB selects ciphering and integrity algorithms for RRC messages from the security algorithms that the MME forwarded for the UE, and ciphering algorithms for user traffic. Next, from K_{eNB} , it derives K_{RRInt}/K_{RRCenc} , RRC integrity/ciphering keys, and K_{UPenc} , a key for ciphering user traffic.

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

The eNB helps the UE to generate AS security keys (K_{RRInt} , K_{RRCenc} and K_{UPenc}) by informing the UE of the AS security algorithms it selected (i.e. control plane RRC integrity/ciphering algorithm and user plane ciphering algorithm) through a **Security Mode Command (AS Security Algorithm, MAC-I)** message. The eNB sends this RRC message with its integrity-protected (by including MAC-I).

26) [UE] Generating AS Security Keys

Upon receiving the **Security Mode Command** message from the eNB, the UE generates AS security keys using the AS security algorithm that the eNB selected, and performs integrity check on the **Security Mode Command** message.

27) [UE → eNB] AS Keys Generation Complete

Once the integrity check on the **Security Mode Command** message is completed, AS security keys are successfully set up and ready to work between the UE and the eNB. The UE then indicates to the eNB that AS security keys are generated by sending a **Security Mode Complete (MAC-I)** message. The UE sends the message with its integrity-protected by using the RRC integrity key.

As the AS security setup over the radio link is ended, RRC messages exchanged over the radio link thereafter are sent as encrypted and integrity-protected, and user traffic is delivered as encrypted. Now, the eNB begins DRB establishment.

28) ~ 29) DRB Establishment**28) [UE ← eNB] Reconfiguring RRC Connection**

The eNB allocates uplink/downlink DRB IDs, and configures DRB QoS parameters from E-RAB QoS in order to establish DRB, an EPS bearer over the radio link. Thereafter, it sends a **RRC Connection Reconfiguration** message to the UE through the secured RRC connection. The RRC connection was already established when the UE sent the **Attach Request** message. However, it must be reconfigured now that the UE needs to configure parameters according to the resources allocated by the network as a result of permission to access the network. The RRC layer of the UE allocates radio resources based on the configuration parameters gathered from the **RRC Connection Reconfiguration** message. Next, it extracts an **Attach Accept** message from the **RRC Connection Reconfiguration** message, and sends it to the NAS layer.

When the NAS layer of the UE receives the message, it obtains the UE IP address and GUTI from the message, and uses them for future communication.

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

Once Step 28) is completed, and the UE can deliver uplink/downlink traffic from/to the eNB.

30) [eNB → S-GW] E-RAB Setup Response

The eNB allocates a downlink S1 TEID (S1 eNB TEID) for S1 bearer. Then it includes the allocated ID in an **Initial Context Setup Response** message, and sends it to the MME as a response to the **Initial Context Setup Request** message received in Step 22), so that the MME can forwards it to the S-GW.

31) [eNB] Allocating a Downlink TEID for S1 Bearer

Once Step 29) is completed, a downlink TEID is allocated by the eNB to S1 bearer, establishing the downlink S1 GTP-U tunnel. However, since the S-GW does not know about the establishment yet, it cannot delivery downlink traffic to the eNB at this time.

32) [UE → MME] Sending Attach Complete Message

The UE sends an **Attach Complete** message⁹ to the MME, as a response to the message in Step 20). The **Attach Complete** message is delivered through an **UL Information Transfer** message over the RRC connection, and then through an **Uplink NAS Transport** message over the S1 signaling connection.

33) [UE][MME] EMM State

Now the UE and the MME stay in EMM-Registered state. If an **Attach Reject** message is sent from the MME to the UE in Step 20), the UE must release the ECM/RRC connection and transit to EMM-Deregistered state.

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

The MME forwards the downlink S1 TEID (S1 eNB TEID) received from the eNB to the S-GW through a **Modify Bearer Request** message.

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

The S-GW sends the MME a **Modify Bearer Response** as a response to the **Modify Bearer Request** message. Now, the S-GW is ready to deliver downlink S1 traffic.

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

Step 35) completes the setup procedure for S1 bearer. With the establishment of S1 bearer, the eNB and the S-GW can exchange traffic with each other. Now, the default EPS bearer from the UE all the way to the P-GW is finally established, allowing uplink/downlink EPS bearer communication between the UE and the P-GW.

⁹ The Attach Complete message is an EMM message, and includes Activate Default EPS Bearer Context Accept message, an ESM message, when being sent.

III. EPS Entity Information: Before/After Initial Attach

In this chapter, we will look into changes in EMM information¹⁰ stored in EPS entities before and after the “EMM Case 1: Initial Attach by Unknown UE” procedure. For the purpose of description, all the information stored in each EPS entity will be grouped as UE ID information, UE Location information, Security Context information, and EPS Session/Bearer information as seen in Figure 9.

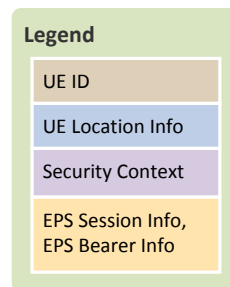
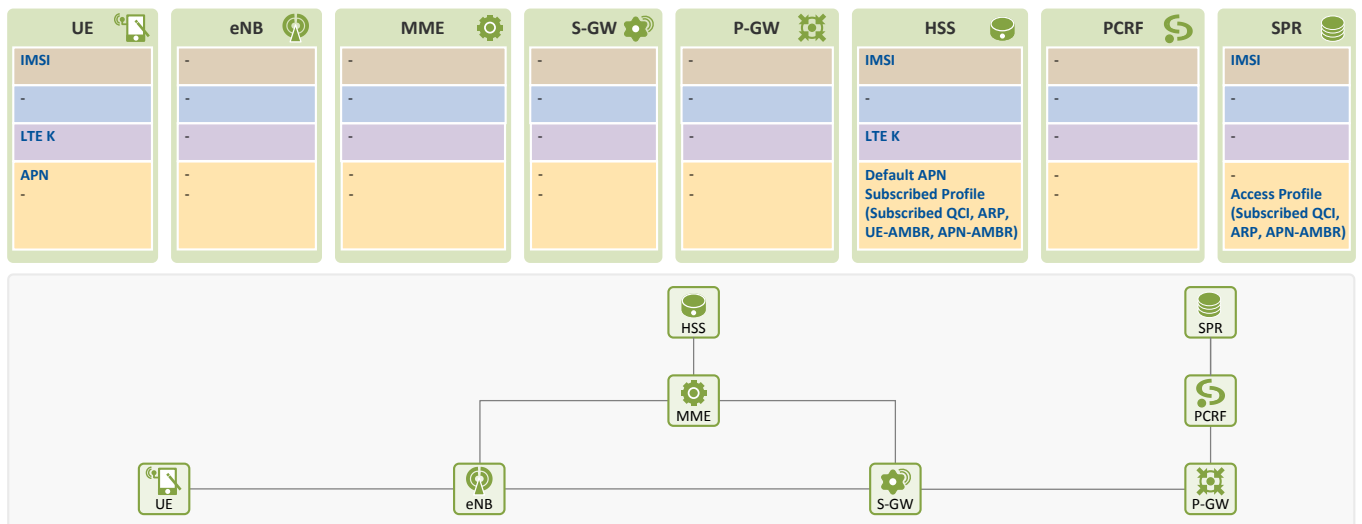


Figure 9. Legend

3.1 Before Initial Attach

Figure 10 shows what information is stored in each entity before the “EMM Case 1: Initial Attach by Unknown UE” procedure. As EMM Case 1 involves initial attach by an unknown user, all the network has is commissioning and provisioning information only.



- UE ID information: A user’s IMSI is provisioned at UE, HSS and SPR.
- UE Location information: No information about UE location is registered at UE or anywhere in the network.
- Security Context information: An LTE master key to be used for user authentication is commissioned at UE and HSS.

¹⁰ Although ESM messages are not discussed in the document, ESM information elements are included here because procedures for establishing an EPS session/default EPS bearer are presented in the EMM procedures anyway.

- EPS Session/Bearer information: User subscription information (Default APN, Subscribed QCI, ARP, UE-AMBR, APN-AMBR, etc.) and user access profile (Subscribed QCI, ARP, APN-AMBR, etc.) are provisioned at HSS and SPR, respectively.

3.2 After Initial Attach

Figure 11 shows what kinds of information are stored in EPS entities after the “EMM Case 1: Initial Attach by Unknown UE” procedures described in Chapter II. As the user is registered in the network, and all the necessary resources have been allocated, information (allocated identifiers or parameters) required for the UE to securely receive user traffic and to use services at the desired quality level at any location is set in each EPS entity. We will study what changes have been made in the information after initial attach.

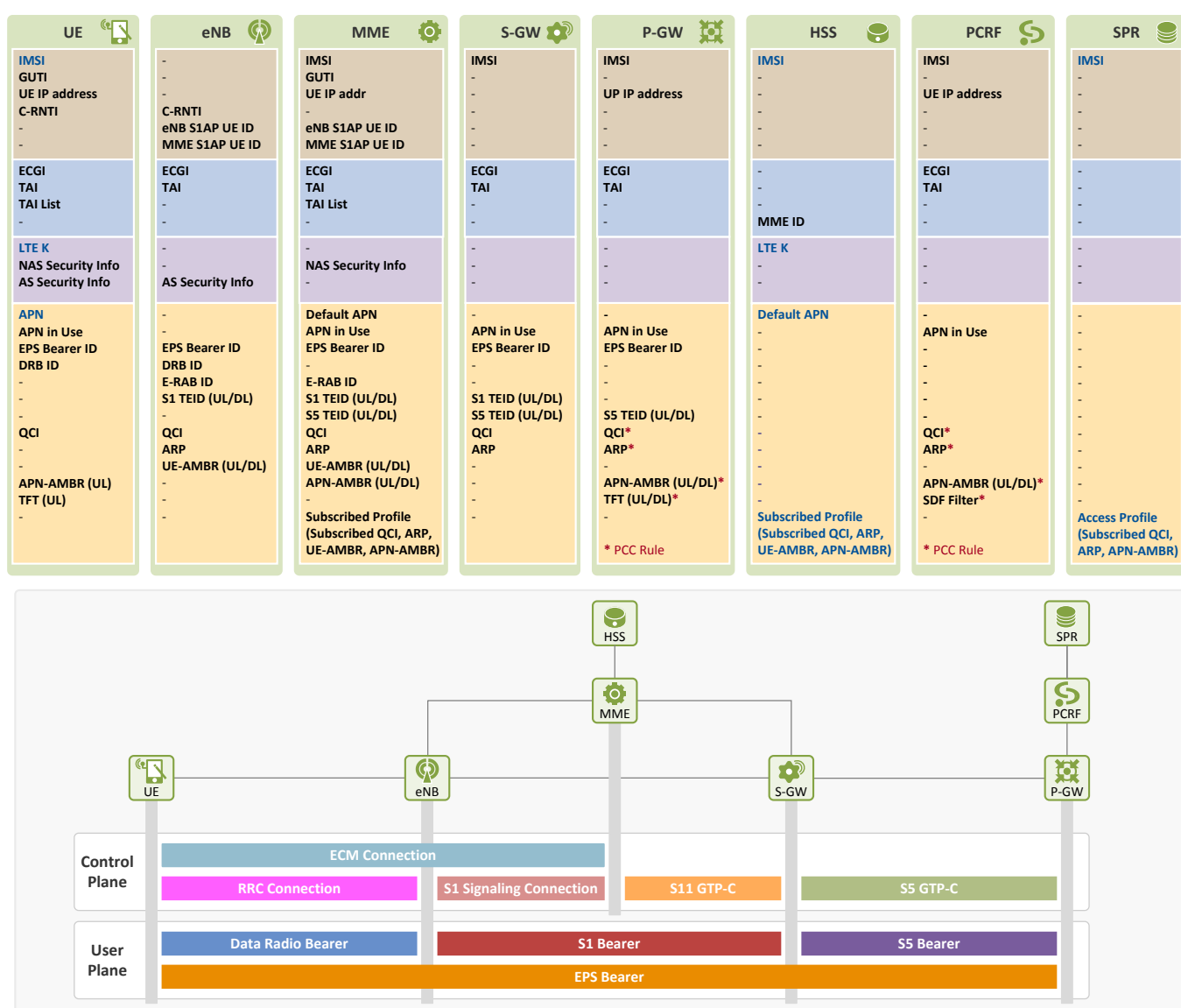


Figure 11. Information in EPS entity after Initial Attach

Changes in UE ID Information

- **IMSI:** The IMSI that the UE delivered through the **Attach Request** message is added to the MME, S-GW, P-GW and PCRF after establishment of the EPS session/bearer.
- **GUTI:** The GUTI that the MME allocated to use instead of IMSI in NAS messages is added to the MME and the UE.
- **UE IP address:** The UE IP address that the P-GW allocated is added to the P-GW, PCRF, MME and UE.
- **C-RNTI:** The C-RNTI that eNB allocated to identify UEs in physical layer over the radio link is added to the eNB and the UE.
- **UE S1AP ID:** The eNB UE S1AP ID and the MME UE S1AP ID are added to the eNB and the MME for user identification in S1AP messages delivered over S1-MME interface.

Changes in UE Location Information

- **ECGI:** Information on the cell in which the user is located is added to the UE, eNB, MME, S-GW, P-GW and PCRF. Every time the user moves to a new cell, the MME notifies the P-GW, which then notifies the PCRF, of the new cell in accordance with the Change Reporting Action policies set by the PCRF.
- **TAI:** Information on the TA in which the user is located is added to the UE, eNB, MME, S-GW, P-GW and PCRF. Every time the user moves to a new TA, the MME notifies the P-GW, which then notifies the PCRF, of the new TA in accordance with the Change Reporting Action policies set by the PCRF.
- **TAI list:** The TAI list that lists the areas the UE is allowed to enter without TAU updates is added to the MME and UE.
- **MME ID:** Information about the MME that the user is attached to (MME ID) is added to the HSS.

Changes in Security Context Information

- **NAS Security Info:** The NAS security context (see our technical document [3]) is added to the UE and MME.
- **AS Security Info:** The AS security context (see our technical document [3]) is added to the UE and eNB.

Changes in EPS Session/Bearer Information

- **APN in Use:** Added to the MME, S-GW, P-GW, PCRF and UE at the time of EPS session creation.
- **EPS Bearer ID:** Added to the MME and the entities where the default EPS bearer is created (thus, user traffic is delivered through) like the UE, eNB, S-GW and P-GW.
- **DRB ID:** Added to the UE and eNB in charge of communication over the radio link.
- **E-RAB ID:** Added to the eNB and MME at the time of E-RAB creation.
- **S1 TEID (UL/DL):** Added to the eNB, S-GW and MME at the time of S1 bearer creation.
- **S5 TEID (UL/DL):** Added to the S-GW, P-GW and MME at the time of S5 bearer creation.
- **QCI:** Allocated to all types of SDF and EPS bearers, and added to the UE, eNB, MME, S-GW, P-GW and PCRF. This QCI value is approved by the PCRF.
- **ARP:** Allocated to all types of SDF and EPS bearers, and added to the eNB, MME, S-GW, P-GW and PCRF, but not to the UE (unlike QCI). This ARP value is approved by the PCRF.
- **UE-AMBR (UL/DL):** Added to the MME and eNB at the time of EPS session and bearer creation. Calculated by the MME.
- **APN-AMBR (UL/DL):** Added to the MME, P-GW, PCRF and UE at the time of EPS session and bearer creation. This value is approved by the PCRF. UEs have APN-AMBR (UL) only.

- **TFT (UL/DL):** Added to the P-GW and UE at the time of EPS bearer creation. P-GWs have this value for both UL and DL, but UEs have it for UL only.
- **SDF Filter:** Added to the PCRF at the time of EPS session creation.
- **Subscribed Profile:** Added to the MME when subscription information is downloaded from the HSS during the user location update procedure.

IV. Closing

We have discussed the initial attach procedures for a user who attaches to the LTE network for the first time after his subscription to the services provided by the LTE network operator (“EMM Case 1” in [1], “Attach Case 1” in [2]). In addition to the initial attach case discussed above, four other cases were discussed in the previous document, Part 1 of Initial Attach. Among the four, one that involves initial attach to a new MME (“EMM Case 11” in [1], “Attach Case 5” in [2]) will be covered later in the last document of our EMM procedure series. In the subsequent document, we will learn how a user detaches/is detached from a network after using services in the network.

References

- [1] Netmanias Technical Document, “Eleven EMM Cases in an EMM Scenario”, October 2013, <http://www.netmanias.com/en/?m=view&id=techdocs&no=6002>
- [2] Netmanias Technical Document, “EMM Procedure 1. Initial Attach – Part 1. Cases of Initial Attach”, <http://www.netmanias.com/en/?m=view&id=techdocs&no=6098>
- [3] Netmanias Technical Document, “LTE Security II: NAS and AS Security”, August 2013, <http://www.netmanias.com/en/?m=view&id=techdocs&no=5903>
- [4] Netmanias Technical Document, “LTE Security I: LTE Security Concept and LTE Authentication”, July <http://www.netmanias.com/en/?m=view&id=techdocs&no=5902>
- [5] Netmanias Technical Document, “LTE QoS: SDF and EPS Bearer QoS”, September 2013, <http://www.netmanias.com/en/?m=view&id=techdocs&no=5908>
- [6] NMC Consulting Group Confidential Internal Report, “E2E LTE Network Design”, August 2010.

Netmanias Research and Consulting Scope

		99	00	01	02	03	04	05	06	07	08	09	10	11	12	13
Services	eMBMS/Mobile IPTV															
	CDN/Mobile CDN															
	Transparent Caching															
	BSS/OSS															
	Cable TPS															
	Voice/Video Quality															
	IMS															
	Policy Control/PCRF															
	IPTV/TPS															
Mobile Network	LTE															
	Mobile WiMAX															
	Carrier WiFi															
	LTE Backhaul															
Wireline Network	Data Center Migration															
	Carrier Ethernet															
	FTTH															
	Data Center															
	Metro Ethernet															
	MPLS															
	IP Routing															

Visit <http://www.netmanias.com> to view and download more technical documents.

About NMC Consulting Group

NMC Consulting Group is an advanced and professional network consulting company, specializing in IP network areas (e.g., FTTH, Metro Ethernet and IP/MPLS), service areas (e.g., IPTV, IMS and CDN), and wireless network areas (e.g., Mobile WiMAX, LTE and Wi-Fi) since 2002.

Copyright © 2002-2014 NMC Consulting Group. All rights reserved.