

EMM Procedure 1. Initial Attach

Part 1. Cases of Initial Attach

Table of Contents

- I. Introduction
- II. Cases of Initial Attach
- III. Simplified Call Flow in Each Case
- IV. Closing

The Initial Attach document discusses procedures for initial attach by a user attaching to an LTE network for the first time, as defined as EMM Case No. 1 in our previous document, “Eleven EMM Cases in an EMM Scenario”. The document consists of two companion documents: this document (Part 1. Cases of Initial Attach) and the subsequent document (Part 2. Call Flow of Initial Attach). In this document, we will distinguish different cases of initial attach (Attach Case 1 ~ Attach Case 5), and different function blocks involved in each case. Then we will explain different procedures required in each case of initial attach. In the subsequent document, detailed initial attach procedures in Attach Case 1 will be described.

December 26, 2013
(Initial Released: September 15, 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 © 2002-2013 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	O
11		LTE EMM Procedure 1. Initial Attach - Part 2. Call Flow of Initial Attach	
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

This document discusses initial attach, as defined as EMM Case 1 in our previous document, “Eleven EMM Cases in an EMM Scenario” [1]. During this phase, a user turns on his device (UE) for the first time after subscribing to an LTE network/service, and attempts to attach to the network, sending an IMSI to the network (The initial procedure will be the same if the user is using an IMSI as his UE ID, even when he has previously attached to the network).

The initial attach procedure may vary depending on circumstances. It can be as in EMM Case 1, to be explained below, or as in EMM Case 11 (Initial Attach in Another City), to be covered in the subsequent document later. Or it can be other types depending on whether or not a user (UE) kept the information used for his last attach to the network (hereinafter referred to as the “Last Attach Information”¹, or whether the network (MME) has information about the user, including UE ID, (hereinafter referred to as the “Last UE Context”²). So, this document (Part 1 of Initial Attach) will describe different initial attach types, and find out their characteristics and differences from one another. The subsequent document (Part 2) will focus on EMM Case 1, providing the related procedures in details.

This document is organized as follows: Chapter II identifies different initial attach cases, and Chapter III briefly discusses different initial attach procedures of each case, by listing the functions to be performed by MME.

II. Cases of Initial Attach

When a UE initially attaches to a network, an MME initiates a different procedure depending on the type of such attach. The procedure begins when a user sends an **Attach Request** message to an MME, and ends when the MME returns an **Attach Accept** message to the UE. When the UE sends the MME the **Attach Request** (UE ID), it includes its UE ID (IMSI or Old GUTI³) in the message to identify itself. When the MME sends the **Attach Accept** (GUTI and TAI list) message, it includes a GUTI, an ID that the UE can use instead of IMSI, and a TAI list⁴ that contains the areas the UE is allowed to enter without TAU updates.

An MME may go through some or all of the following procedures after receiving an **Attach Request** message from a UE and before sending an **Attach Accept** message back to the UE (see Chapter III):

- UE ID acquisition
- Authentication
- NAS security setup
- Location update
- EPS session establishment

¹ A UE's Last Attach Information includes the UE's Old GUTI and NAS security context.

² An MME's Last UE Context includes the UE's ID (IMSI and Old GUTI) and MM Context (NAS security context and UE-AMBR).

³ Refers to the GUTI assigned to a UE before it was detached from the network. If properly detached, the UE keeps its GUTI and NAS security context valid. For more information, see our technical document, “LTE Identification I: UE and ME Identifiers”.

⁴ If a UE moves to a TA that is not on the TAI list, it must update its TA. For more information, see our technical document, “LTE Identification II: NE and Location Identifiers”.

Decisions on which procedure to perform are made based on the types of initial attach attempted by a UE. But, both UE ID acquisition and EPS session establishment procedures are required in all types of initial attach. Other procedures like authentication, NAS security setup and location update are performed selectively depending on the type of initial attach. The procedure selection is affected by i) what UE ID the UE has (IMSI or Old GUTI), ii) whether or not the Last Attach Information is still kept valid in the network (MME), etc. In this document, we will use the following criteria to distinguish different types of initial attach, as seen in Figure 1:

- With which UE ID is the UE making a request for initial attach? (IMSI or Old GUTI)
- To which MME is the UE trying to attach? (the one it has attached last time⁵ or new one it has never attached before?)
- Does the valid Last UE Context exist in the network? (Yes or No?)

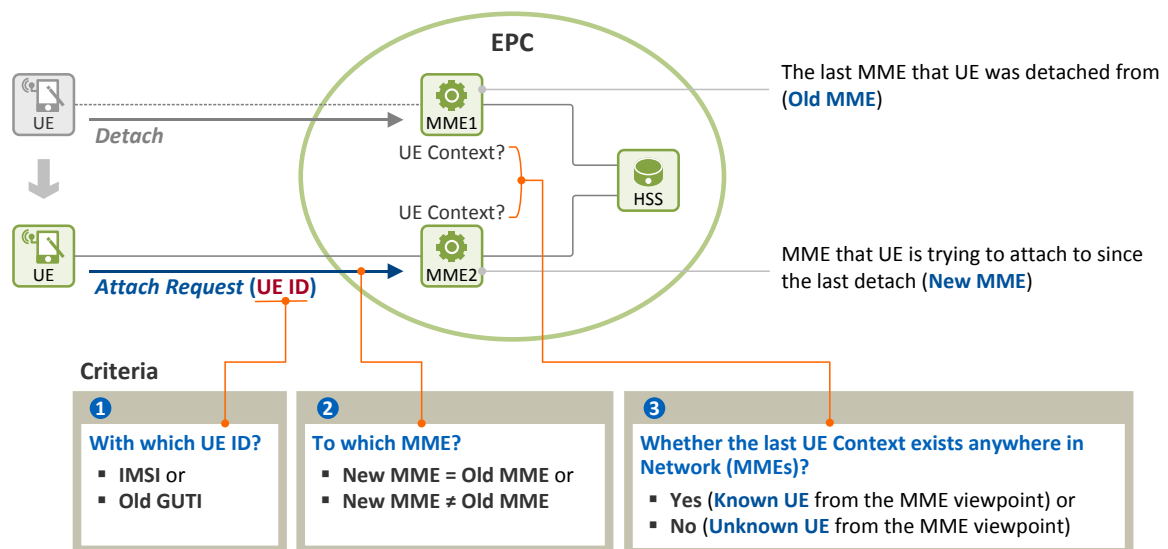


Figure 1. Criteria for Classification of Initial Attach

In the document, UEs are defined as “unknown UEs” if their Last UE Context, including UE IDs, does not exist in the network (MME), and others are defined as “known UEs”. Section 2.1 describes initial attach by unknown UEs while Section 2.2 explains one by known UEs. Below, we will assume **Attach Request** messages are sent integrity-protected if the UE has the Last Attach Information.

2.1 Unknown UE

Figure 2 illustrates the cases of initial attach where a user (UE) sends an **Attach Request** message to a network, and the network (MME) does not have any valid UE context about the user (UE). We will distinguish the types of initial attach, and explain the characteristics of each type for comparison (EPS session establishment procedure is common, and thus will not be discussed here). An MME to which the UE is trying to attach now will be called “New MME” and the one the UE has attached to last time will be called “Old MME”.

⁵ The last MME that a UE was detached from.

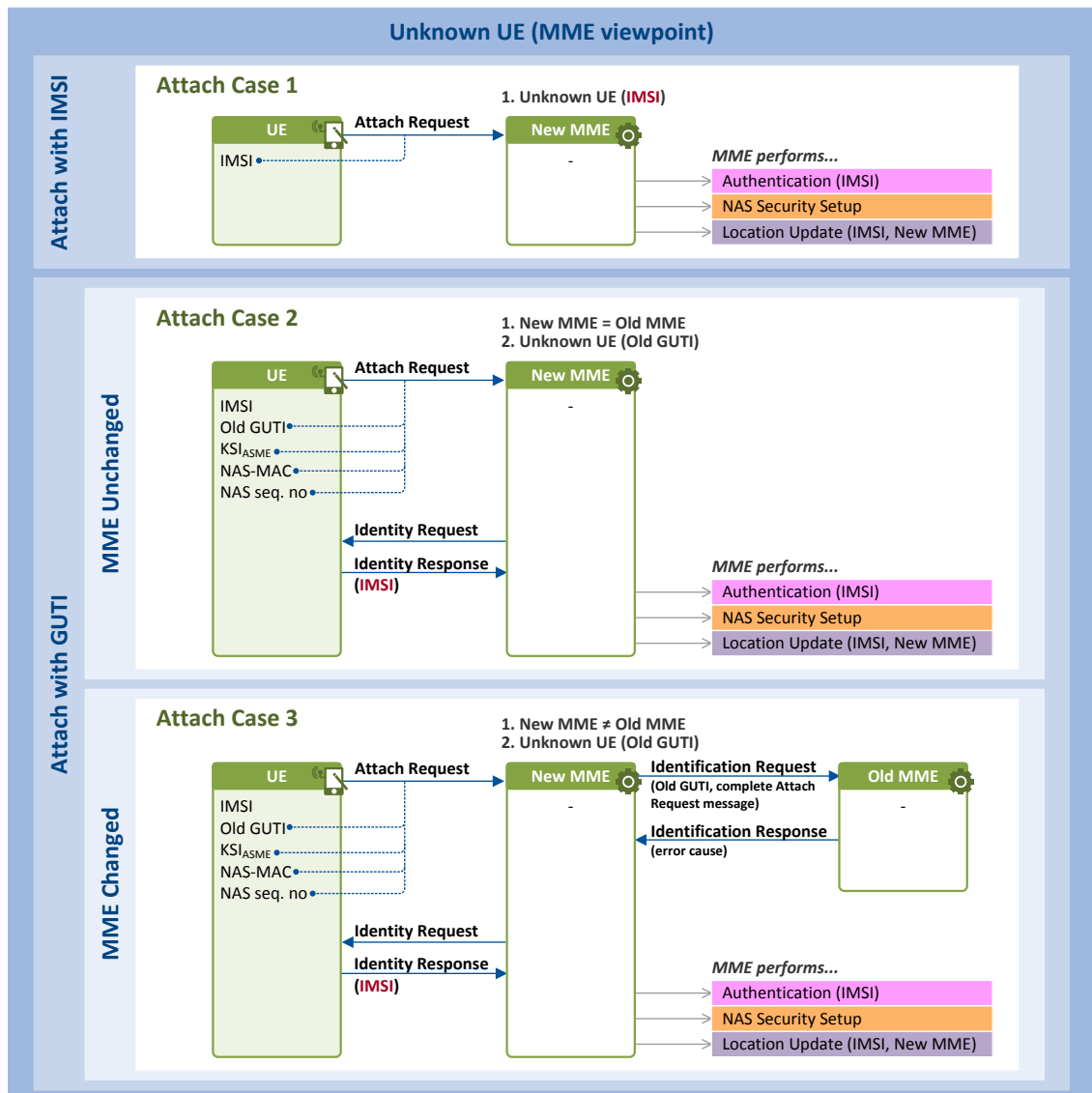


Figure 2. Initial Attach Cases by Unknown UE

Attach Case 1: When a UE is attaching using an IMSI

This is when neither user (UE) nor network (MME) has the Last UE Context, as in EMM Case 1 to be explained in Part 2. A scenario required for this case is as follows:

- 1) A UE sends an MME an **Attach Request** message using its IMSI as a UE ID. The MME obtains the IMSI from the message.
- 2) The MME, assuming it doesn't know the UE (because an IMSI was sent), initiates procedures for authentication and NAS security setup.
- 3) The MME sends a location update message to HSS, informing the HSS that the UE is registered with it, and downloads the subscription information of the user from the HSS.

Attach Case 2: When a UE is attaching to the MME that it has attached to last time (New MME = Old MME), but the MME doesn't have the valid Last UE Context of the UE

This is when a UE, still having the Last Attach Information (Old GUTI and NAS security context⁶) even after its last detach, is trying to attach to the same MME, but the MME doesn't have any valid UE context of the UE. An exemplary scenario can be as follows:

- 1) A UE sends New MME an **Attach Request** message, using its Old GUTI. At this time, the **Attach Request** message is sent integrity-protected by a NAS integrity key (K_{NASint}) (i.e. by including NAS-MAC).
- 2) As a GUTI includes a GUMMEI, an MME ID, the New MME knows from the Old GUTI that the Old GUTI was assigned by itself. The New MME looks up the Last UE Context, but fails to find any (e.g. due to failed integrity validation or no Old GUTI).
- 3) The MME sends the UE an **Identity Request** message, requesting an IMSI.
- 4) The UE sends the MME an **Identity Response** message, providing the requested IMSI.
- 5) Now, the MME performs the procedures for authentication and NAS security setup by using the obtained IMSI as in **Attach Case 1**, then sends the UE's location update message to HSS.

Attach Case 3: When a UE is attaching to a new MME that it has never attached to before (New MME ≠ Old MME), and the MME doesn't have the valid Last UE Context of the UE

This is when a UE, still having the Last Attach Information even after its last detach, is attaching to a new MME (New MME), not to the Old MME, but the Old MME doesn't have the valid UE context relating to the UE, either. An exemplary scenario can be as follows:

- 1) A UE sends New MME an **Attach Request** message using its Old GUTI as a UE ID. At this time, the **Attach Request** message is sent integrity-protected.
- 2) When the New MME receives the message, it knows from the Old GUTI that it was assigned by other MME (Old MME).
- 3) Then, the New MME sends the Old MME an **Identification Request** (Old GUTI, Complete **Attach Request** Message), forwarding the Old GUTI and **Attach Request** message it received from the UE. By doing so, the New MME requests the Last UE Context related to the Old GUTI.
- 4) Upon receiving the message, the Old MME looks up the UE context, but fails to find any (e.g. due to failed integrity validation or no Old GUTI).
- 5) The Old MME then sends the New MME an **Identification Response** (error cause) message, informing that no UE context was found.

From here, things are the same as in **Attach Case 2**, and thus Steps 3), 4) and 5) in **Attach Case 2** are performed. The New MME sends the UE an **Identity Request** message, requesting an IMSI. The UE then sends its IMSI to the MME through an **Identity Response** message. With the received IMSI, the MME performs procedures for authentication and NAS security setup, and has the UE's location updated.

⁶ See our technical document, "LTE Security II: NAS and AS Security" [2].

2.2 Known UE

Figure 3 shows a case of initial attach where a user (UE) attaches to a network by sending an **Attach Request** message, and the network (MME) has the valid UE context for the user. Unlike unknown UEs, all known UEs are assumed to use a GUTI, not IMSI, for their initial attach. In Figure 3, both the UE and the MME have the Last UE Context relating to the user, and the UE sends an **Attach Request** message with its integrity protected.

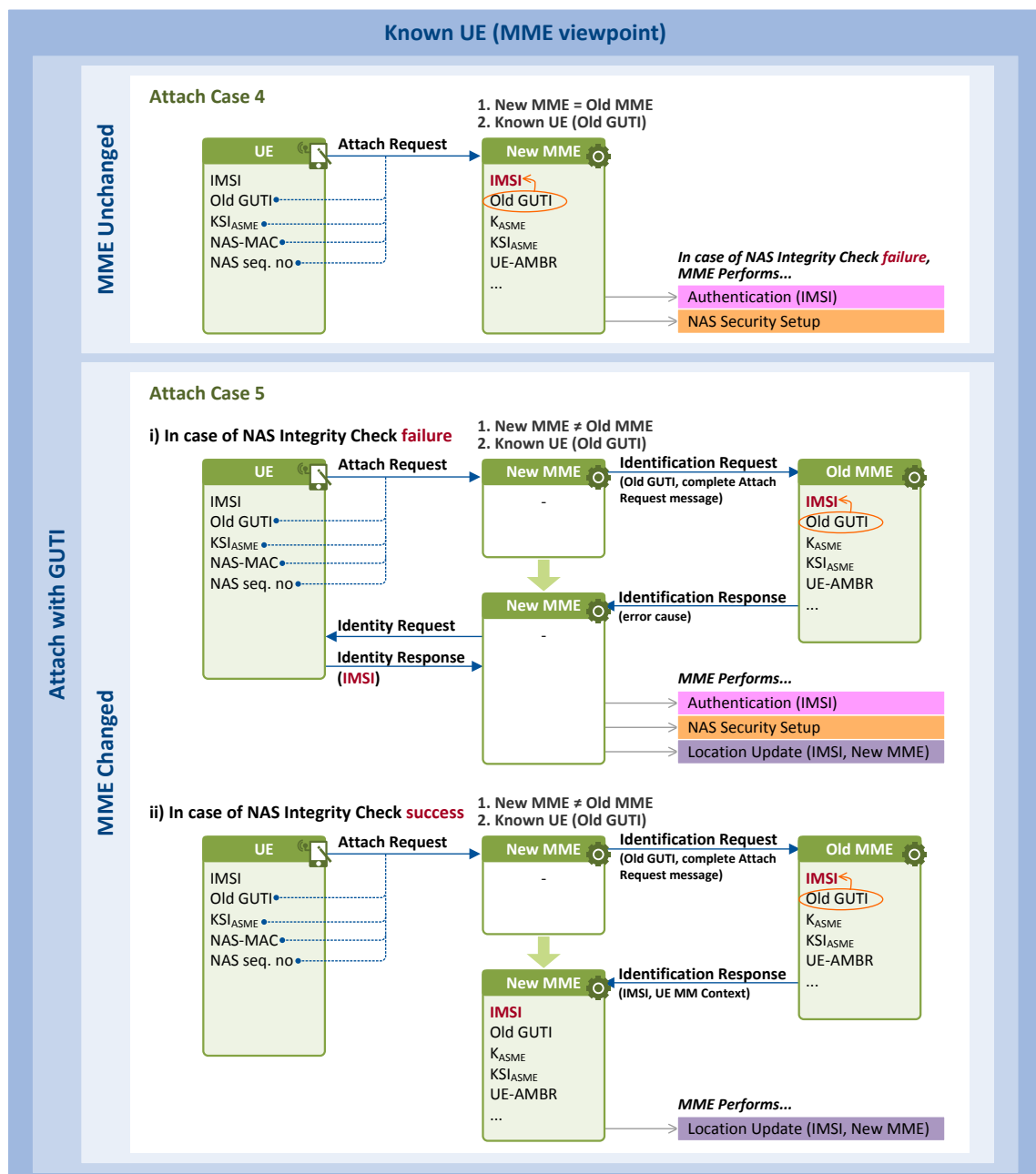


Figure 3. Initial Attach Cases by Known UE

Attach Case 4: When a UE is attaching to the MME that it has attached last time (New MME = Old MME), and the MME has the valid Last UE Context of the UE

This is when a UE, still having the Last Attach Information (Old GUTI, NAS security context), attaches to the MME that it has attached to last time, and the MME has the valid UE context for the UE. An exemplary scenario can be as follows:

- 1) A UE sends New MME an **Attach Request** message using its Old GUTI as a UE ID. At this time, the **Attach Request** message is sent integrity-protected with a NAS integrity key (K_{NASint}) (i.e. by including NAS-MAC).
- 2) The New MME knows from the received Old GUTI that it was assigned by itself. Then, it looks up the Old GUTI, and finds the valid UE context of the UE (IMSI, MM Context (NAS security context, UE-AMBR)).
- 3) The MME conducts an integrity check on the **Attach Request** message.
 - i) If the integrity check on NAS-MAC fails, the MME must authenticate the user by using an IMSI instead, and perform NAS security setup procedure for the user.
 - ii) If it passes, the MME may skip the procedures for authentication and NAS security setup.

Attach Case 5: When a UE is attaching to a new MME that it has not attached to before (New MME \neq Old MME), and the Old MME has the valid Last UE Context of the UE

This is when a UE, still having the Last Attach Information, attaches to a new MME (New MME), and the Old MME has the valid UE context of the UE. An exemplary scenario can be as follows:

- 1) A UE sends New MME an **Attach Request** message using its Old GUTI as a UE ID. At this time, the **Attach Request** message is sent integrity-protected.
- 2) The New MME knows from the received Old GUTI that it was assigned other MME (Old MME).
- 3) Then, the New MME sends the Old MME an **Identification Request** (Old GUTI, complete **Attach Request** message), forwarding the Old GUTI and **Attach Request** message it received from the UE. By doing so, the New MME requests the Last UE Context related to the Old GUTI.
- 4) Upon receiving the message, the Old MME looks up the UE context, and finds the IMSI and MM context (NAS security context, UE-AMBR) related to the UE.
- 5) The Old MME conducts an integrity check on the **Attach Request** message.
- 6) Then, it delivers the check result to the New MME through an **Identification Response** message.
 - i) If the integrity check fails, the Old MME delivers the message with error causes.
 - ii) If it passes, the UE context (IMSI, Old GUTI and MM context) is delivered.

If the integrity check fails, things are the same as in **Attach Case 3**, and hence the same procedures of IMSI acquisition, authentication and NAS security setup are performed as in **Attach Case 3**. If the check passes, the New MME receives the IMSI and MM context from the Old MME, and the procedures for authentication and NAS security setup may be skipped, as in **Attach Case 4**. The only difference from **Attach Case 4** is that since the UE is attached to a new MME, the New MME communicates with the HSS to have the UE's location updated.

III. Simplified Call Flow in Each Case

Chapter II has explained the different cases of initial attach. Now Chapter III describes simplified call flows during the initial attach procedure in each case, with main focus on function blocks involved in each case. Figure 4 illustrates the different call flows that each initial attach procedure would have depending on which UE ID is used when a UE is attempting to attach. In case of initial attach by a known UE, we discuss the case where the NAS-MAC integrity check is passed only. The function blocks that can be performed during initial attach procedure are as follows:

- **UE ID Acquisition**

The network (MME) acquires a UE ID for user identification and authentication. Here, the UE ID can be an IMSI or Old GUTI. An IMSI can be acquired from a UE through **Attach Request** or **Identity Response** messages while an Old GUTI can be obtained from a UE through an **Attach Request** message.

- **Authentication**

If the network (MME) has acquired i) an IMSI or ii) Old GUTI as the UE's ID through an **Attach Request** message, but the integrity check on the message fails, the network checks whether the user is permitted to attach or not by performing the EPS-AKA procedure. The HSS derives K_{ASME} , the MME base key, by generating authentication vectors and sending them to the MME, which then performs mutual authentication with the UE, on behalf of the HSS.⁷

- **NAS Security Setup**

Once user authentication is completed, NAS security keys for secured delivery of NAS messages between the UE and MME are generated.⁸

- **Location Update**

The MME downloads user information from the HSS, and the HSS updates the information about the UE's current location (MME).

The MME will perform location updates only when i) the UE sends an IMSI as its UE ID, ii) the MME doesn't have the valid Last UE Context of the UE, iii) the MME doesn't have any valid subscription information about the user, or iv) the UE was detached from other MME last time.

- **EPS Session Establishment**

An EPS session and a default EPS bearer are established.

⁷ See our technical document, "LTE Security I: LTE Security Concept and LTE Authentication" [3].

⁸ See our technical document, "LTE Security II: NAS and AS Security" [2].

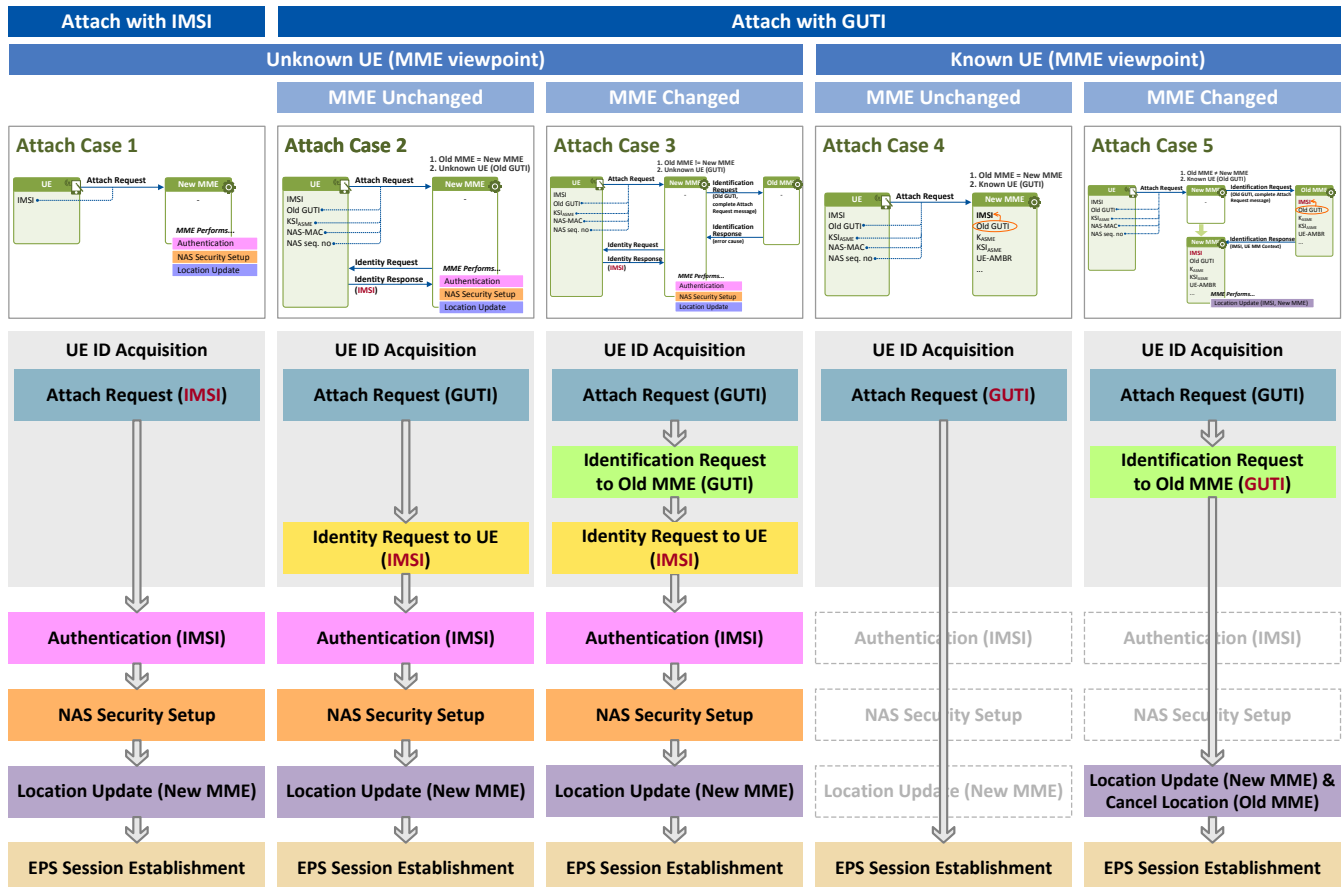


Figure 4. Simplified Call Flow in Different Initial Attach Cases

3.1 Initial Attach with IMSI

Attach Case 1: Unknown UE

The UE requests for initial attach using its IMSI, and the MME acquires the user's IMSI from the **Attach Request** message.

- [UE → MME] **Attach Request (IMSI)**

If the UE uses its IMSI when requesting for initial attach, the MME performs procedures for authentication, NAS security setup and location update, and establishes an EPS session/default EPS bearer.

3.2 Initial Attach with GUTI

Attach Case 2: Unknown UE, MME Unchanged

The UE requests for initial attach using its Old GUTI, but the MME doesn't have the Old GUTI. So, the MME requests the UE for a UE ID, and acquires an IMSI.

- [UE → MME] **Attach Request (Old GUTI)**
- [MME] **No IMSI**
- [UE ← MME] **Identity Request (UE ID = IMSI)**
- [UE → MME] **Identity Response (IMSI)**

The rest of the procedure is the same as in **Attach Case 1**. That is, the MME performs procedures for authentication, NAS security setup and location update, and establishes an EPS session/default EPS bear.

Attach Case 3: Unknown UE, MME Changed

The UE requests for initial attach using its Old GUTI. So, the MME (New MME) asks the Old MME for the Last UE Context relating to the UE, but fails to receive any. So, the MME requests the UE for a UE ID, and acquires an IMSI.

- [UE → New MME] **Attach Request** (Old GUTI)
- [New MME → Old MME] **Identification Request** (Old GUTI)
- [Old MME] No IMSI
- [New MME ← Old MME] **Identification Response** (error cause)
- [UE ← New MME] **Identity Request** (UE ID = IMSI)
- [UE → New MME] **Identity Response** (IMSI)

The rest of the procedure is the same as in **Attach Case 1**. That is, the MME performs procedures for authentication, NAS security setup and location update, and establishes an EPS session/default EPS bear.

Attach Case 4: Known UE, MME Unchanged

The UE requests for initial attach using its Old GUTI, and the MME has the Last UE Context relating to the Old GUTI. So, no further step for acquiring an IMSI is required.

- [UE → MME] **Attach Request** (Old GUTI)
- [MME] **IMSI**, Old GUTI, MM Context

If the integrity check on NAS-MAC passes, the MME may immediately establish an EPS session/default EPS bearer without performing the procedures for authentication, NAS security setup and location update.⁹

Attach Case 5: Known UE, MME Changed

The UE requests for initial attach using its Old GUTI. So, the MME (New MME) asks the Old MME for the Last UE Context relating to the UE, and acquires the UE's IMSI and MM context.

- [UE → New MME] **Attach Request** (Old GUTI)
- [New MME → Old MME] **Identification Request** (Old GUTI)
- [Old MME] **IMSI**, Old GUTI, MM Context
- [New MME ← Old MME] **Identification Response** (IMSI, Old GUTI, MM Context)

If the Old MME's integrity check on NAS-MAC passes, the New MME receives the IMSI and MM context, and thus doesn't perform procedures for authentication and NAS security setup. However, since the MME is changed, the New MME communicates with the HSS to have the UE's location updated, and then establishes an EPS session/default EPS bearer.¹⁰ The HSS updates the UE's location from the Old MME to the New MME,

⁹ If the integrity check on NAS-MAC fails, the MME performs the procedures for authentication and NAS security setup, and then establishes an EPS session/default EPS bearer.

¹⁰ If the Old MME's integrity check on NAS-MAC fails (i.e. if the New MME receives an error message), the New MME acquires an IMSI from the UE, performs the procedures for authentication and NAS security setup, has the UE's location updated, and finally establishes an EPS session/default EPS bearer.

and sends a **Cancel Location** message to the Old MME so that the MM context of the UE is deleted from the Old MME.

IV. Closing

So far, we have discussed different cases of initial attach, and different initial attach procedures required for each case. In the subsequent document (Part 2 of the Initial Attach document), we will focus on the detailed initial attach procedures in Attach Case 1 (Initial Attach with IMSI), and find out what kinds of information are set in the EPS entities after the procedures.

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, “LTE Security II: NAS and AS Security”, August 2013, <http://www.netmanias.com/en/?m=view&id=techdocs&no=5903>
- [3] Netmanias Technical Document, “LTE Security I: LTE Security Concept and LTE Authentication”, July 2013, <http://www.netmanias.com/en/?m=view&id=techdocs&no=5902>
- [4] 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 © 2002-2013 NMC Consulting Group. All rights reserved.