

- [Home](#)
- [About](#)
- [Contact](#)
- [Jobs](#)
- [Download 3GPP Decoder](#)
- [Privacy Policy](#)

Search

3GLTEinfo

3GPP  Internet of Things

[Home](#) > [3GPP](#) > UMTS Security: User Identity Confidentiality (IMSI, TMSI & P-TMSI)

UMTS Security: User Identity Confidentiality (IMSI, TMSI & P-TMSI)

 Prashant Panigrahi  September 4, 2009  6

UMTS system uses the same old concept used in GSM and GPRS to protect the user identity over the service link. This is achieved by providing temporary identity to mask the true identity. There are two types of temporary identity used:

1. TMSI: Temporary mobile subscriber identity (for CS domain)
2. P-TMSI: Packet – Temporary Mobile Subscriber Identity (for PS Domain)

The IMSI is the permanent identity of the USIM/Subscriber in the UMTS network.

The UMTS network provides the following features in terms of user confidentiality:

1. Subscriber's IMSI should not be compromised on the radio link.
2. The presence or arrival of a subscriber in a specific area can not be determined by eavesdropping on the radio access link.
3. The intruder should not know whether different services are provided to the same user.

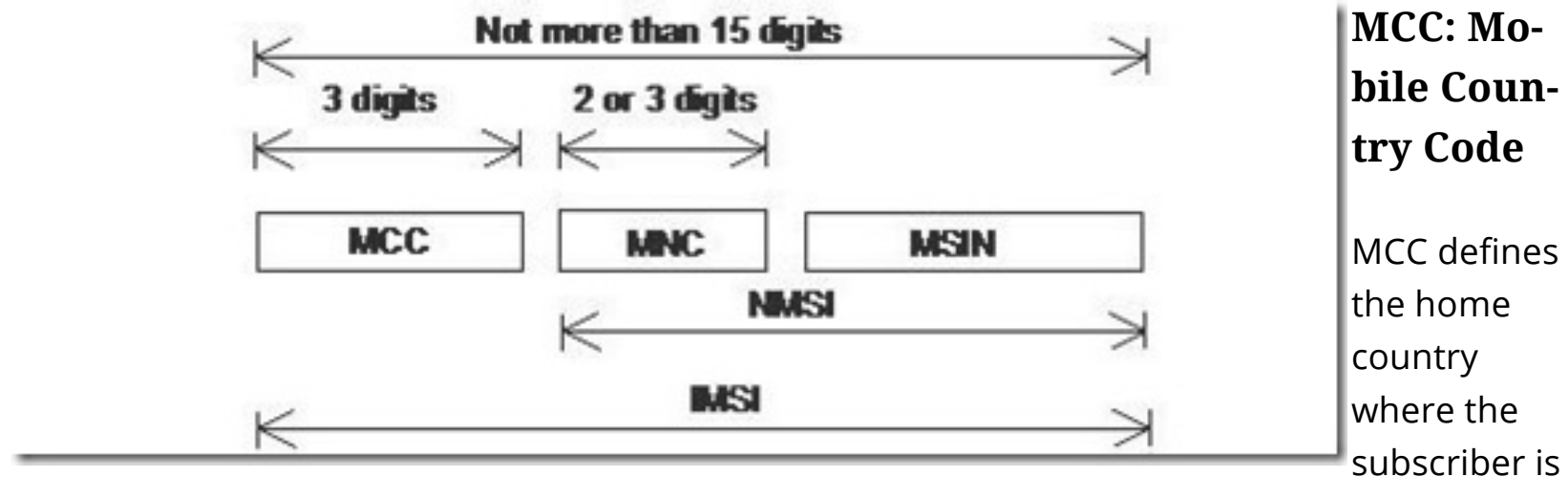
To achieve these:

1. The user is normally identified by temporary identities:
 1. TMSI or
 2. P-TMSI

1. The user should not be identified by the same identity for longer period of time.
2. The signaling and user data that might reveal the user's real identity should always be ciphered.

IMSI: International Mobile Subscriber Identity

The IMSI is defined as follows:



registered.

Example: 240 is MCC for Sweden

Complete list of MCC can be found here:

http://en.wikipedia.org/wiki/List_of_mobile_country_codes

MNC: Mobile Network Code

MNC code defines the home GSM PLMN of the mobile subscriber.

Example: 01 is the MNC for Telia Sweden

The complete list of MNC for all countries can be found here:

http://en.wikipedia.org/wiki/Mobile_Network_Code

MSIN: Mobile Subscriber Identity Number

This number is used to identify a subscriber within the PLMN.

The NMSI (National Mobile Subscriber Identity Code) = MNC + MSIN

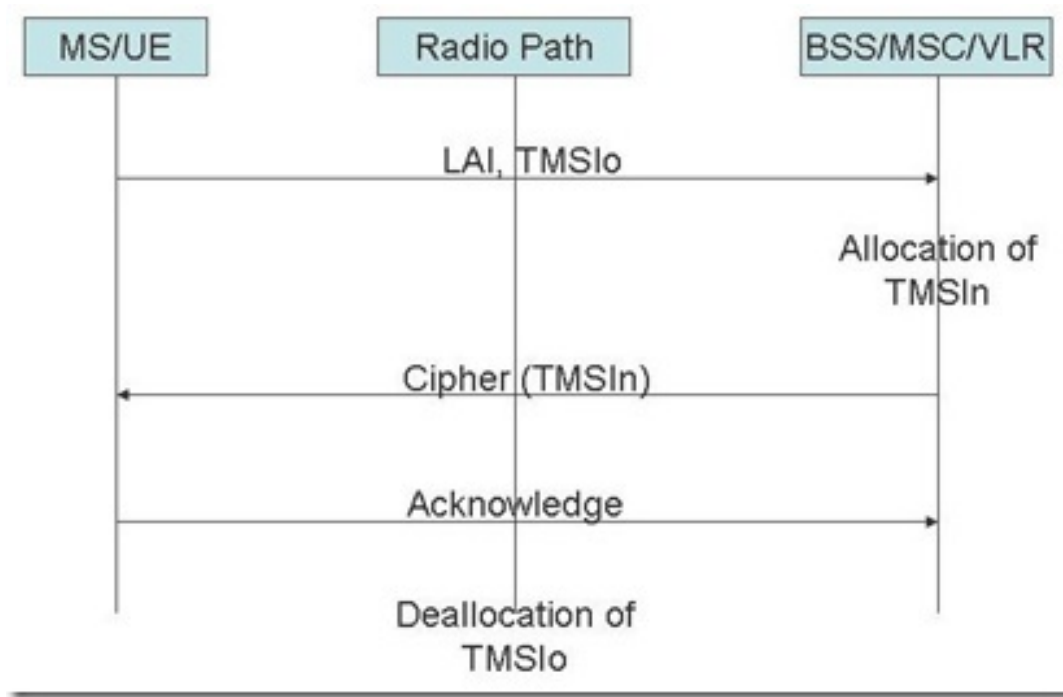
Procedures for management of TMSIs

TMSI changes when user changes the location area. TMSI is a local number and has a meaning only in a certain location area. TMSI is always accompanied by a LAI (Location area Identity) to avoid ambiguities.

Location updating in the same MSC area

TMSIo: Old TMSI

TMSIn: New TMSI



Step 1: UE starts the location area procedure with content set for LAI and old TMSI (TMSIo).

Step 2: MSC/VLR calculates the new TMSI (TMSIn).

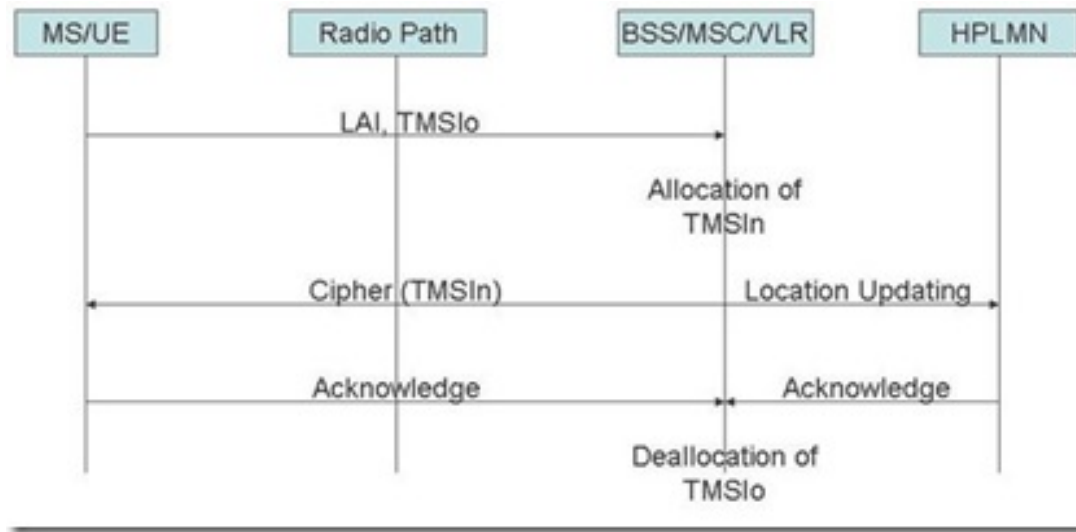
Step 3: TMSIn is transferred to UE in ciphered text to maintain the confidentiality.

Step 4: UE acknowledges the change of TMSI.

Step 5: Old TMSI (TMSIo) will be de-allocated from the VLR database.

Location Updating to a new MSC but the VLR is same

In this case the VLR of the old location area is same as that of the old location area but the MSC changes.



Step 1: UE starts the location area procedure with content set for LAI and old TMSI (TMSIo).

Step 2: MSC/VLR calculates the new TMSI (TMSIn).

Step 3: TMSIn is transferred to UE in ciphered text to maintain the confidentiality. HPLMN is also informed about the change of location area.

Step 5: Old TMSI (TMSIo) will be de-allocated from the VLR database.

```

sequenceDiagram
    participant MSUE as MS/UE
    participant RadioPath as Radio Path
    participant BSSMSCVLRn as BSS/MSC/VLRn
    participant BSSMSCVLRo as BSS/MSC/VLRo
    participant HPLMN as HPLMN

    MSUE->>RadioPath: LAI, TMSIo
    RadioPath->>BSSMSCVLRn: 
    BSSMSCVLRn->>BSSMSCVLRo: TMSIo
    BSSMSCVLRo->>BSSMSCVLRn: IMSI
    BSSMSCVLRn->>RadioPath: Allocation of TMSIn
    RadioPath->>MSUE: Cipher (TMSIn)
    BSSMSCVLRn->>HPLMN: Location Updating
    HPLMN->>BSSMSCVLRn: Acknowledge
    BSSMSCVLRn->>RadioPath: Deallocation of TMSIo
    RadioPath->>MSUE: Acknowledge
  
```

The diagram illustrates the sequence of messages for TMSI Allocation and Deallocation. The participants involved are MS/UE, Radio Path, BSS/MSC/VLRn, BSS/MSC/VLRo, and HPLMN. The process begins with MS/UE sending LAI and TMSIo to the Radio Path, which then forwards it to BSS/MSC/VLRn. BSS/MSC/VLRn sends TMSIo to BSS/MSC/VLRo, which responds with IMSI. BSS/MSC/VLRn then sends Allocation of TMSIn to the Radio Path, which forwards it to MS/UE as Cipher (TMSIn). BSS/MSC/VLRn sends Location Updating to HPLMN, which responds with Acknowledge. Finally, BSS/MSC/VLRn sends Deallocation of TMSIo to the Radio Path, which forwards it to MS/UE as Acknowledge.

Step 2: The new MSC/VLR send the TMSI to the old MSC/VLR.

Step 3: Old MSC/VLR responds with sending back IMSI of the UE.

Step 4: The new MSC/VLRn calculates the new TMSI (TMSIn).

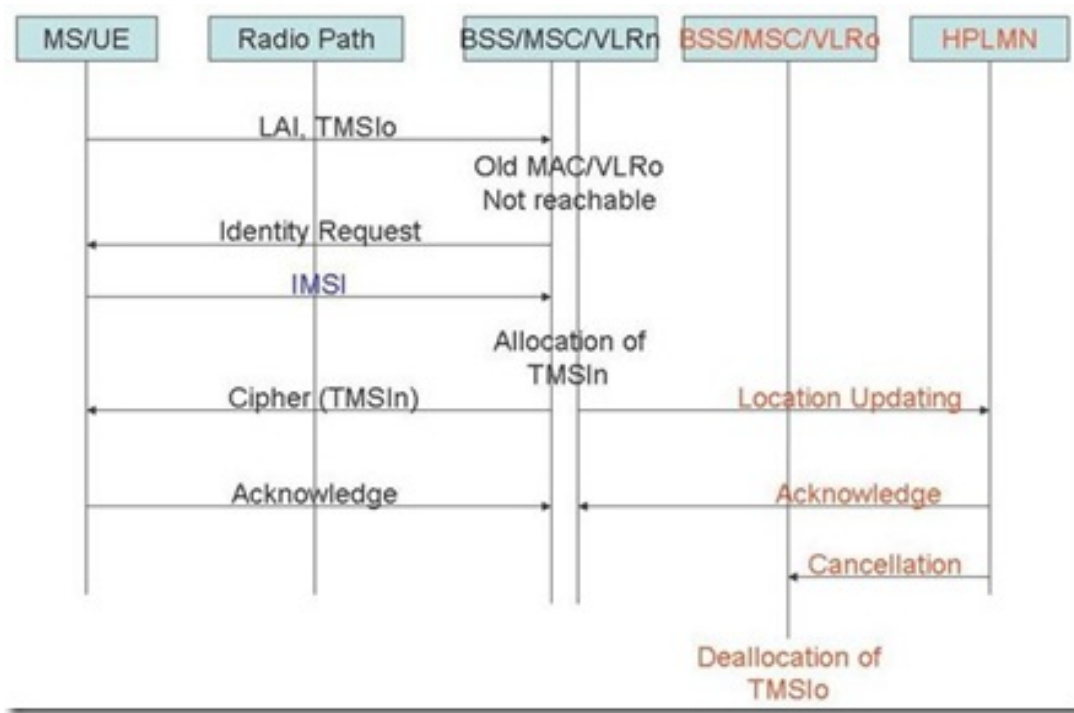
Step 5: MSC/VLRn sends TMSIn to UE in ciphered text and inform the HPLMN of the UE.

Step 6: Both UE and HPLMN acknowledges the new MSC/VLRn.

Step 7: The old MSC/VLRo deallocates the TMSIo from its database.

Location updating in a new VLR; old VLR not reachable

This is the case when the old VLR of the UE is not reachable by the new VLR.



Step 1: UE request location update request with old TMSI (TMSIo) and old LAI set.

Step 2: The new MSC/VLRn can not reach the old MSC/VLRo.

Step 3: New MSC/VLRn request UE for identity with **Identity Request** message.

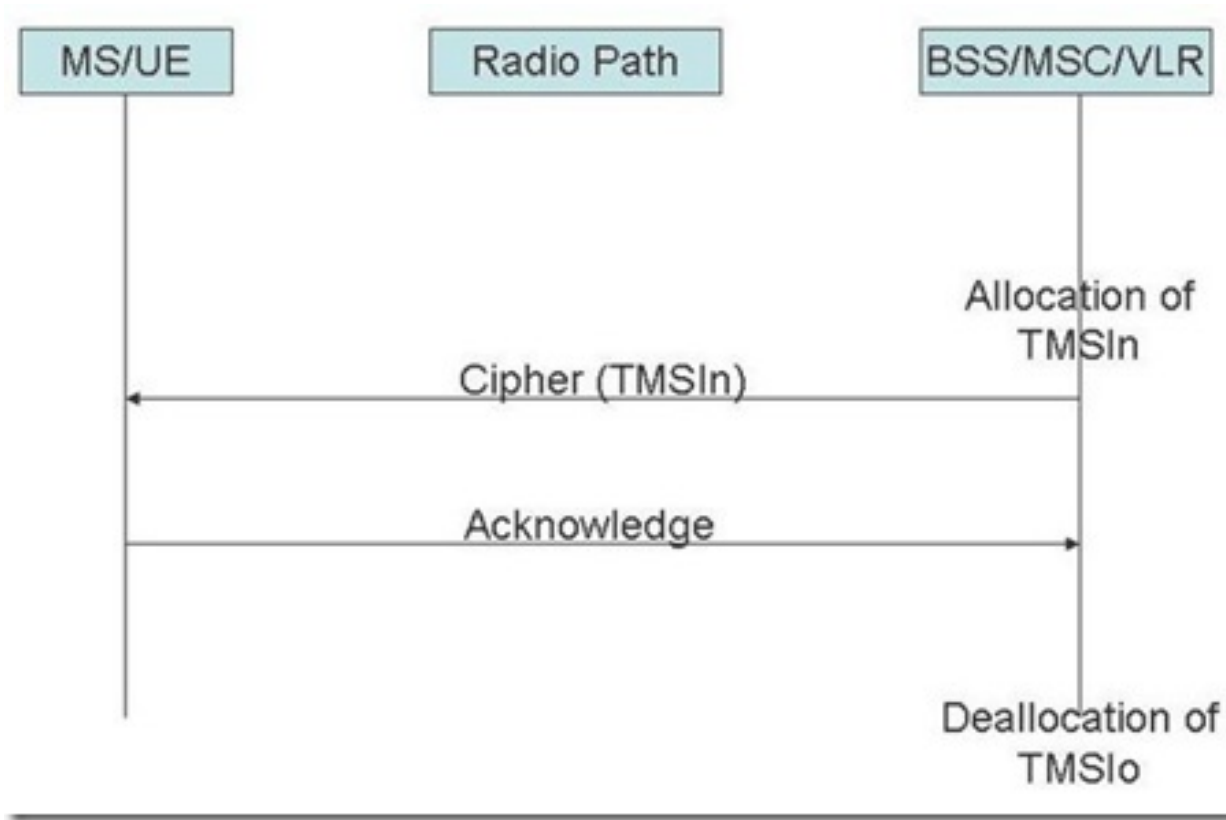
Step 4: UE sends IMSI to the new MSC/VLR in **clear text**.

Step 5: The new MSC/VLRn calculates the new TMSI (TMSIn).

Step 7: Both UE and HPLMN acknowledges the new MSC/VLRn.

Reallocation of TMSI

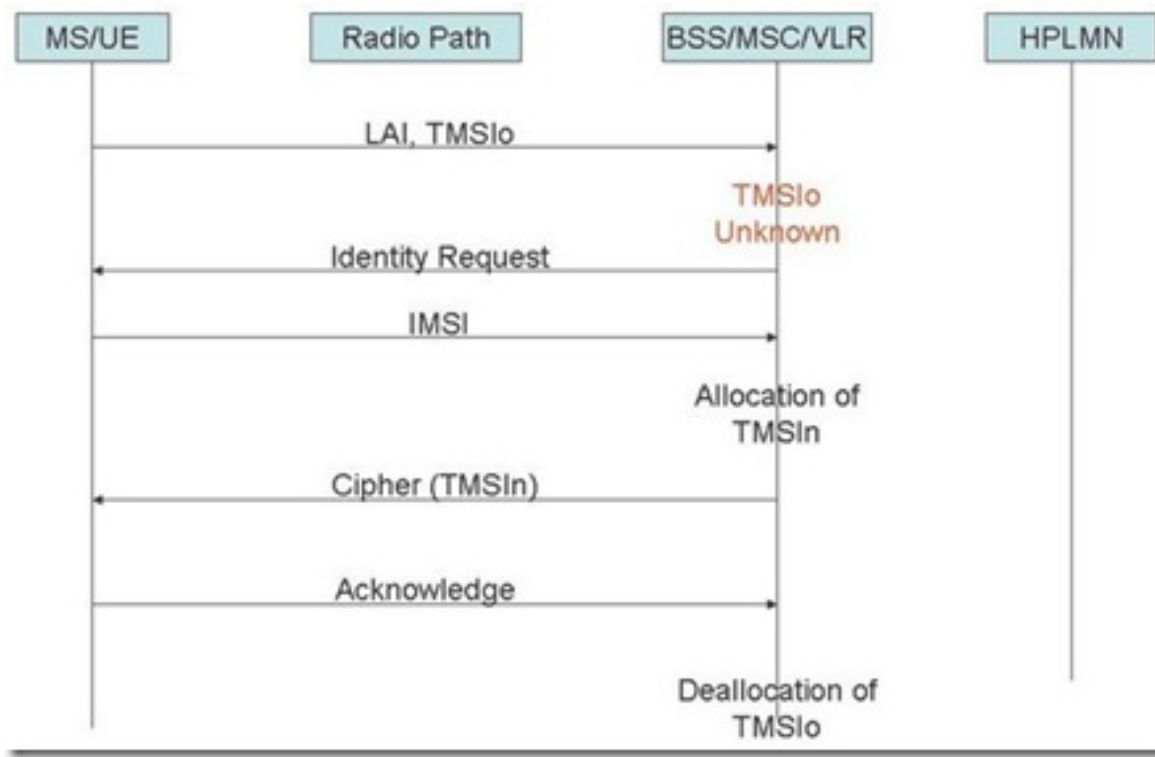
4/25/19, 9:47 PM



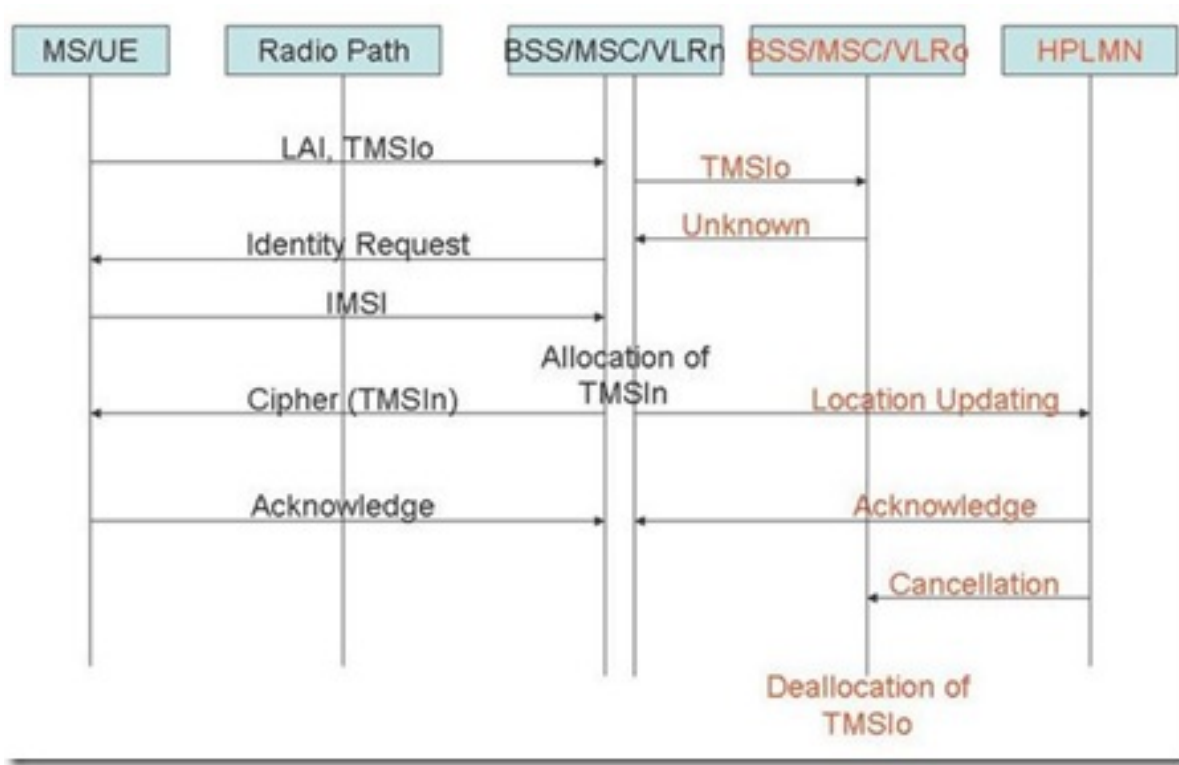
The de-allocation of the old TMSI (TMSIo) only happens when UE acknowledges that the new TMSI (TMSIn) is allocated.

Local TMSI Unknown

This procedure happens when there is data loss in the VLR after location update request.



Location updating in a new VLR in case of loss of information



Step 1: UE request location update request with old TMSI (TMSIo) and old LAI set.

Step 2: The new MSC/VLR send the TMSIo to the old MSC/VLR.

Step 3: Old MSC/VLR does not have the TMSI. It responds that the TMSIo is unknown to it.

Step 4: New MSC/VLRn sends Identity request to the UE.

Step 6: The new MSC/VLRn calculates the new TMSI (TMSIn).

Step 8: Both UE and HPLMN acknowledges the new MSC/VLRn.

Step 9: The old MSC/VLRo deallocates the TMSI from its database.

If due to some problem the MS/UE does not acknowledge the allocation of new TMSI then the network will maintain the relationship between the old TMSI and IMSI and between the new TMSI and IMSI.

Location updating in a new VLR; old VLR not reachable

———TMSI & LAI
———TMSI (32 bit)

-----LAI (Location Area Identity)
-----PLMN -ID
-----MCC
-----MNC
-----LAC (16bits)

RRC CONNECTION SETUP (UE ←NW)

RRC CONNECTION SETUP COMPLETE (UE → NW)

INITIAL DIRECT TRANSFER (UE → NW)

-----LOCATION AREA UPDATE REQUEST
-----Location Area Identity
-----TMSI

DOWNLINK DIRECT TRANSFER (UE ← NW)

-----IDENTITY REQUEST

UPLINK DIRECT TRANSFER (UE → NW)

-----IDENTITY RESPONSE
-----IMSI (In Clear Text)

SECURITY MODE COMMAND (UE ← NW)

SECURITY MODE COMPLETE (UE -> NW)

DOWNLINK DIRECT TRANSFER (UE <- NW)

———LOCATION AREA UPDATE COMPLETE

—————TMSI

📁 Posted in [3GPP](#)

💬 6 COMMENTS



👤 chung nguyen

🕒 9 years ago 🔗 [Permalink](#)

it is great tutorial !



👤 chung nguyen

🕒 9 years ago 🔗 [Permalink](#)

it is great tutorial !



 **Prakash Sahoo**

 9 years ago  [Permalink](#)

It is a nice article.



 **Prakash Sahoo**

 9 years ago  [Permalink](#)

It is a nice article.



 **khalifa elreyani**

 2 years ago  [Permalink](#)

Thank you




 **khalifa elreyani**


 2 years ago  [Permalink](#)


could you give us the references of this article, thanks


 **LEAVE A REPLY**

Your email address will not be published. Required fields are marked *

 Comment

 Name *

 Email *

 Website

☐ Save my name, email, and website in this browser for the next time I comment.

Post Comment

Previous Post: [MAC \(Medium Access Control\) Architecture \(25.321\)](#)

Next Post: [UMTS: RLC Length Indicator \(RLC LI\)](#)



Subscribe to our email newsletter for jobs, useful tips and valuable resources.

Enter your email

Subscribe

More on 3GLTEinfo



Connect



Copyright © 2019 3GLTEInfo. Powered by WordPress and Stargazer.
