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

Prashant Panigrahi September 4, 2009 4

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.

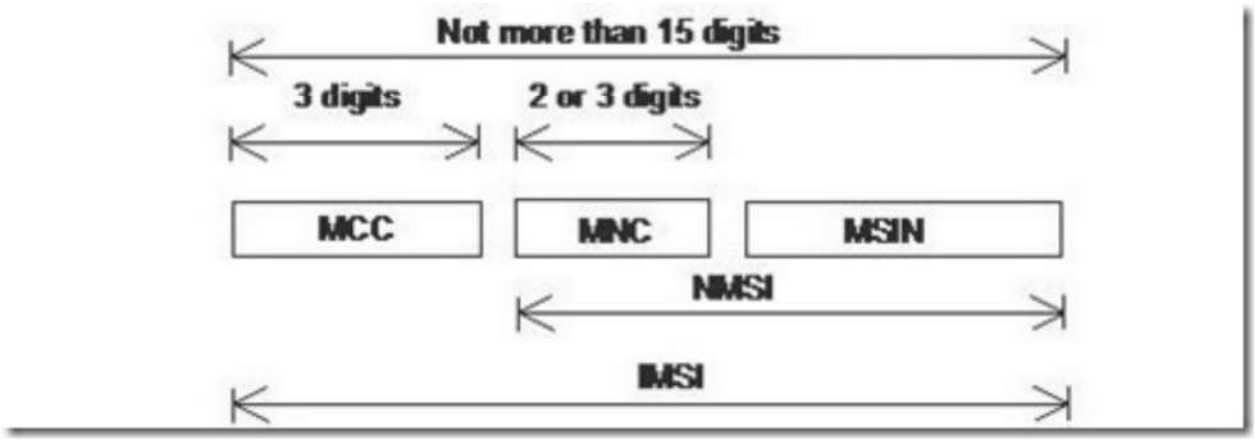
To achieve these:

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.

[SI: International Mobile Subscriber Identity

e IMSI is defined as follows:



MCC: Mobile Country Code

MCC defines the home country where the subscriber is 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

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

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

SIN: Mobile Subscriber Identity Number

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

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

ocedures 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.

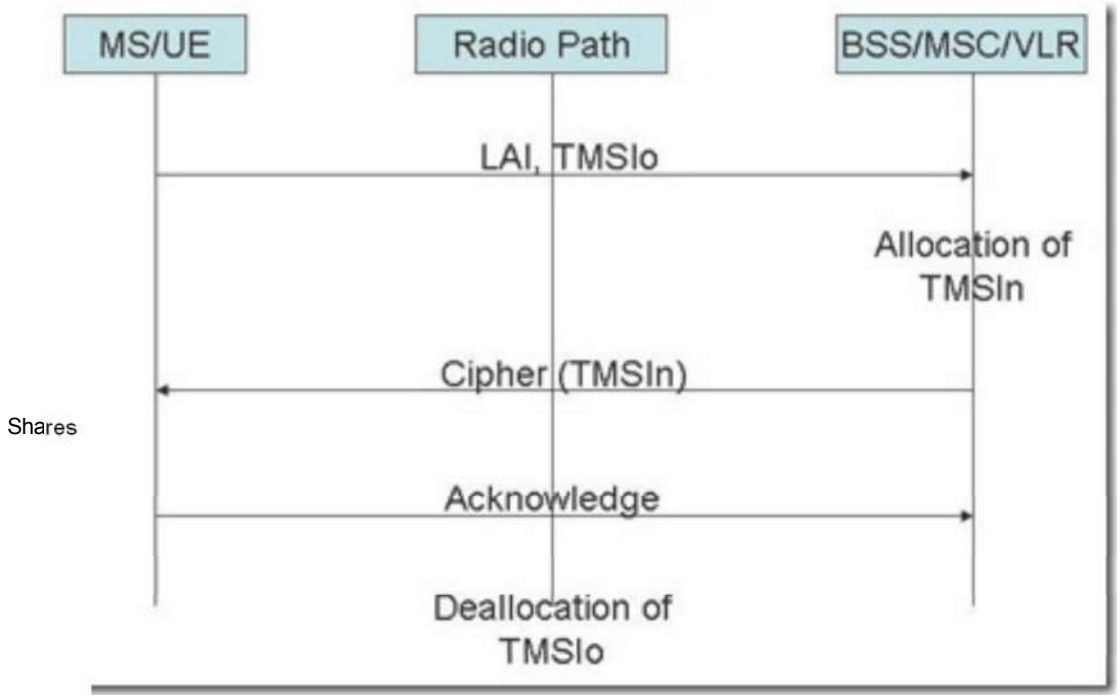
In the core network the VLR keeps the relation between IMSIs and TMSIs in a database. There are number of different instances when TMSI is changed or recalculated.

Location updating in the same MSC area

In this case both the old location area and the new location area are part of the same MSC.

TMSIo: Old TMSI

TMSIn: New TMSI



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

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

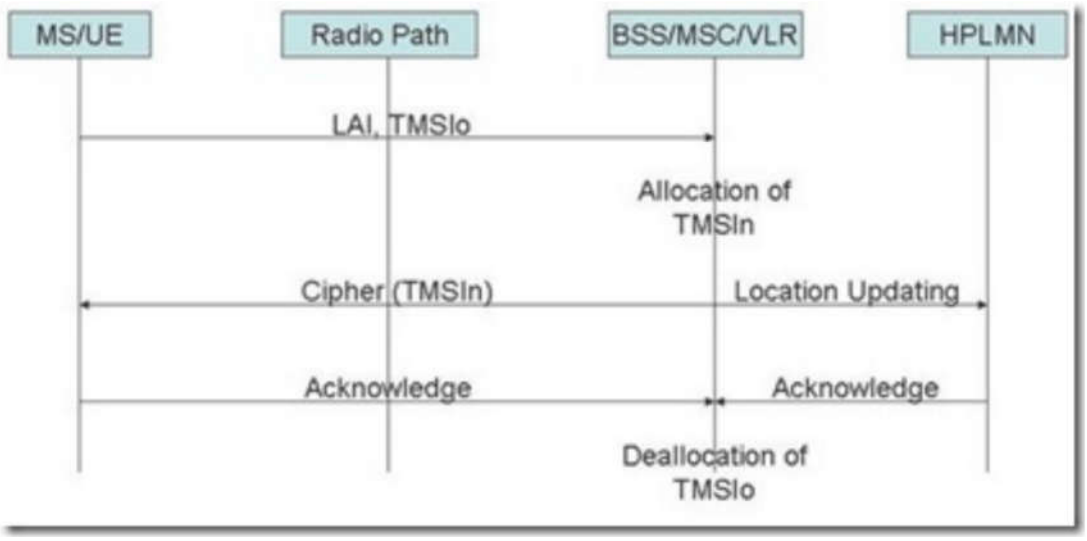
p 3: TMSIn is transferred to UE in ciphered text to maintain the confidentiality.

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.



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

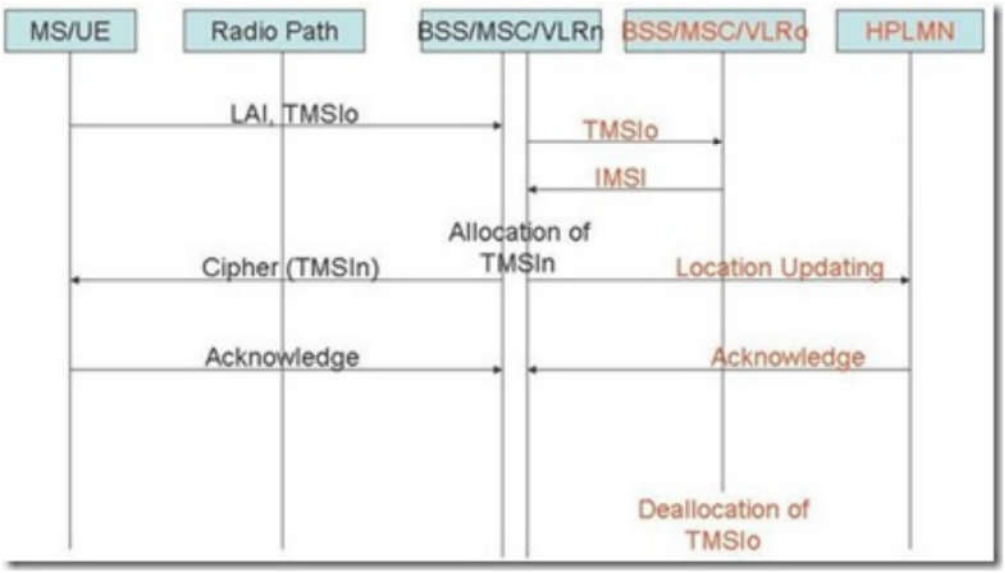
p 2: MSC/VLR calculates the new TMSI (TMSIn).

p 3: TMSIn is transferred to UE in ciphered text to maintain the confi-ntiality. HPLMN is also informed about the change of location area.

p 4: UE acknowledges the change of TMSI. HPLMN also acknowledges changes.

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

Location updating in new VLR, old VLR reachable



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

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

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

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

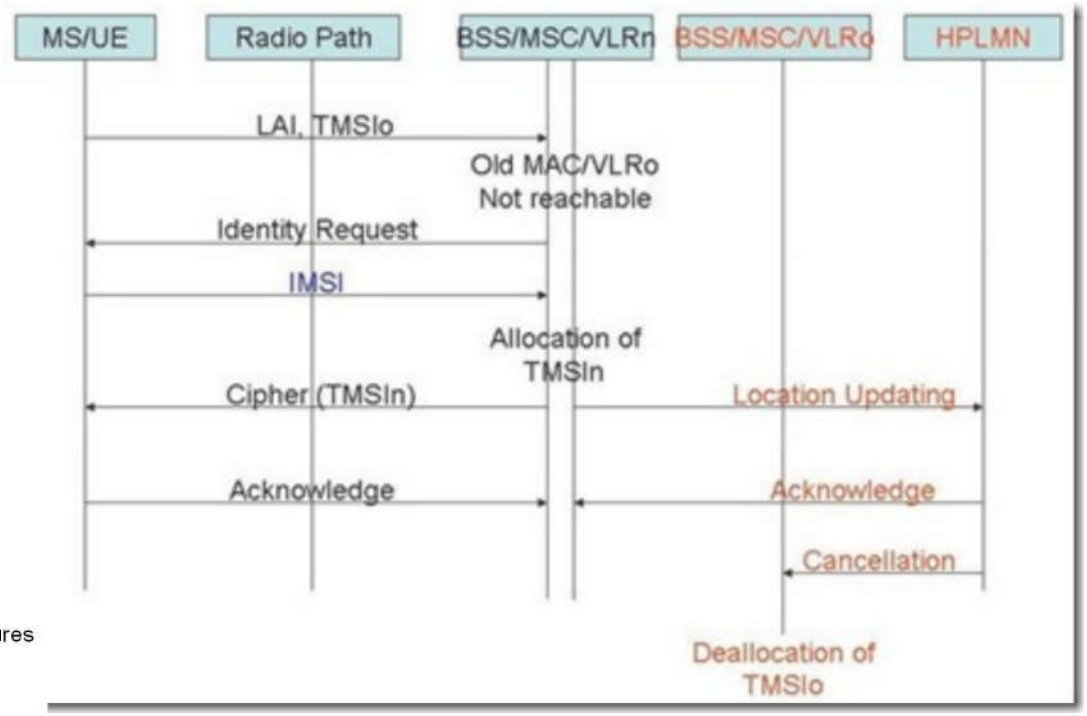
ep 5: MSC/VLRn sends TMSIn to UE in ciphered text and inform the LMN of the UE.

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.



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

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

p 3: New MSC/VLRn request UE for identity with **Identity Request** ssage.

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

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

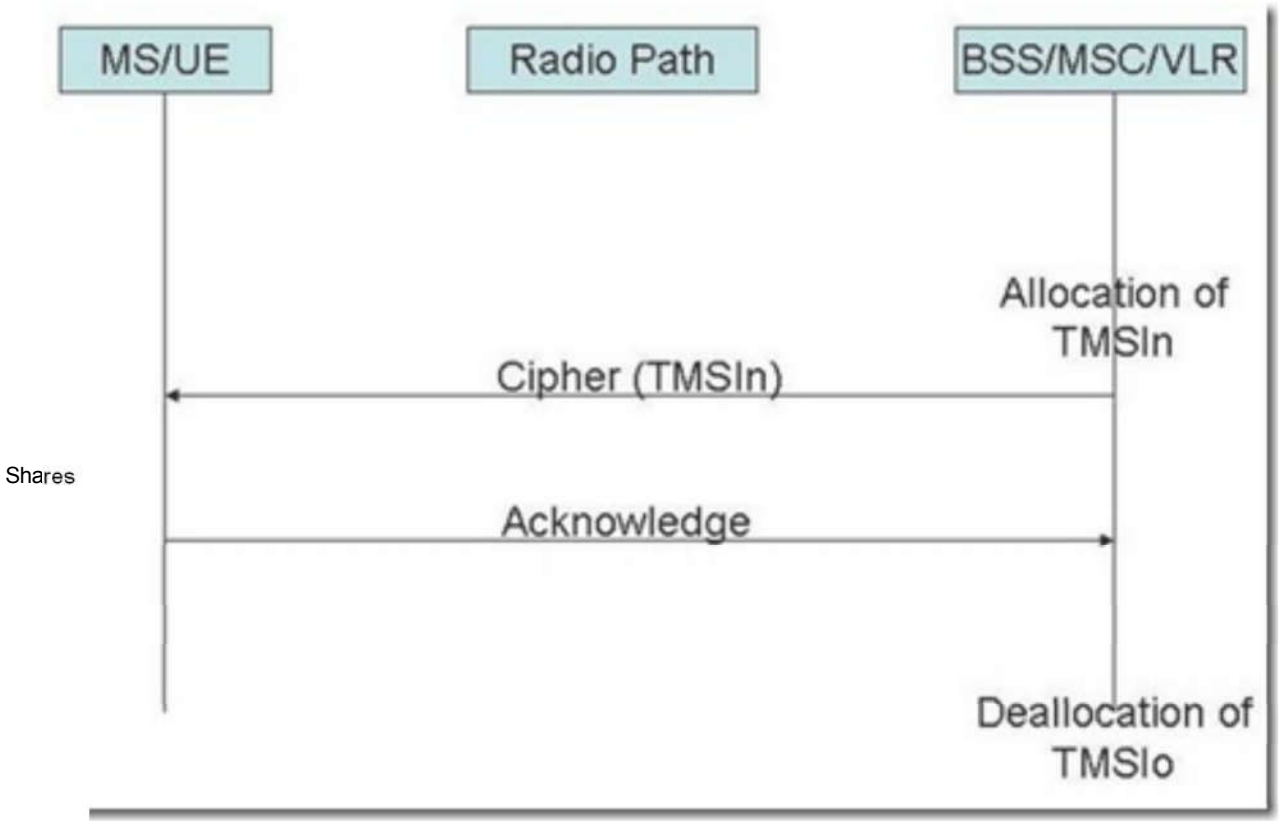
Step 6: MSC/VLRn sends TMSIn to UE in ciphered text and inform the HPLMN of the UE.

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

Step 8: The old MSC/VLRo deallocates the TMSIo from its database.

Reallocation of TMSI

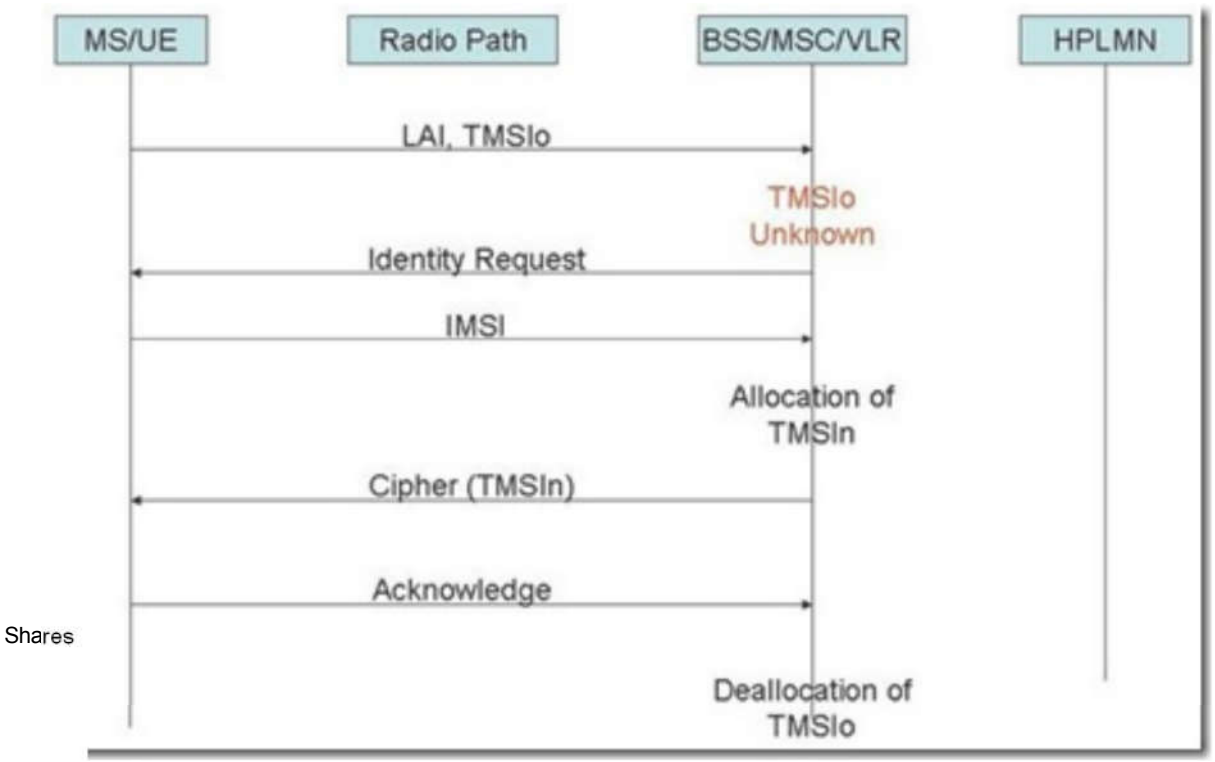
This procedure is initiated by the NW to change the TMSI of the UE. The initiation of the procedure depends on operator.



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

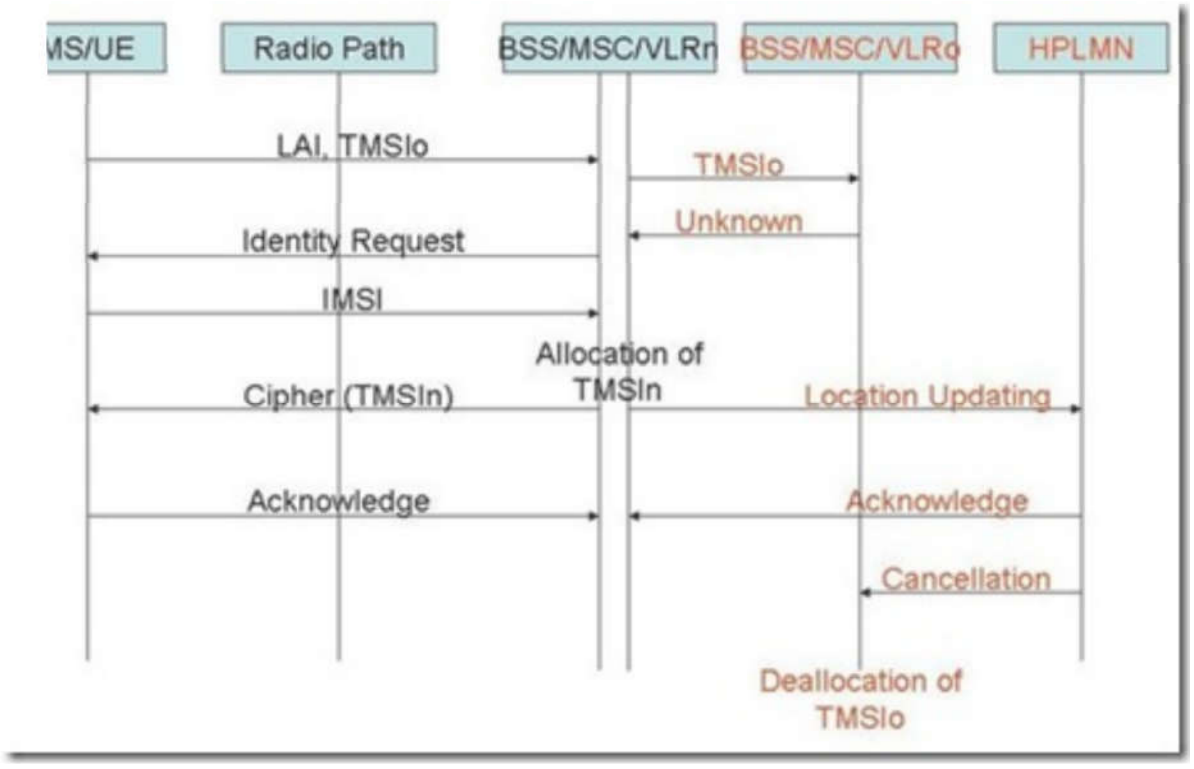
cal TMSI Unknown

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



Shares

cation updating in a new VLR in case of loss of informa-n



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 5: UE responds with sending the IMSI in clear text.

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

:p 7: MSC/VLRn sends TMSIn to UE in ciphered text and inform the LMN of the UE.

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

:p 9: The old MSC/VLRo deallocates the TMSIo from its database.

ısuccessful TMSI allocation

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

Example: Signalling from UE point of view

Location updating in a new VLR; old VLR not reachable

RRC CONNECTION REQUEST (UE –> NW)

———-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

)WNLINK DIRECT TRANSFER (UE <– NW)
——IDENTITY REQUEST

LINK DIRECT TRANSFER (UE –> NW)
——IDENTITY RESPONSE
————IMSI (In Clear Text)

CURITY MODE COMMAND (UE <– NW)

CURITY MODE COMPLETE (UE –> NW)

DOWNLINK DIRECT TRANSFER (UE <– NW)
————LOCATION AREA UPDATE COMPLETE
————————TMSI

Posted in 3GPP

4 COMMENTS

chung nguyen

7 years ago Permalink

it is great tutorial !

chung nguyen
7 years ago Permalink

it is great tutorial !

Prakash Sahoo
6 years ago Permalink

Shares It is a nice article.

Prakash Sahoo
6 years ago Permalink

It is a nice article.

LEAVE A REPLY

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

Comment

Shares

Name *

Email *

Website

Post Comment

Previous Post: MAC (Medium Access Control) Architecture (25.321)

Next Post: UMTS: RLC Length Indicator (RLC LI)

More on 3GLTEinfo

Connect

Shares