DRAFT 3G CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

33.102	**CR**	**070**	Current Version:	3.3.1

3G specification number ↑ *↑ CR number as allocated by 3G support team*

For submission to TSG *list TSG meeting no. here ↑* | for approval **X** | for information | *(only one box should be marked with an X)*

Form: 3G CR cover sheet, version 1.0 *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/3GCRF-xx.rtf*

Proposed change affects: *(at least one should be marked with an X)* USIM **X** ME **X** UTRAN **X** Core Network **X**

Source: Siemens Atea **Date:** 2000-Feb-20

Subject: User identity confidentiality

3G Work item: Security

Category: *(only one category shall be marked with an X)*

F	Correction	
A	Corresponds to a correction in a 2G specification	
B	Addition of feature	
C	Functional modification of feature	**X**
D	Editorial modification	

Reason for change: The mechanisms for user identity confidentiality are presented more clearly. The different scenarios are discussed separately and the procedures that are involved are discussed separately.

Clauses affected: 6.1, 6.2

Other specs affected:

Other 3G core specifications		→ List of CRs:
Other 2G core specifications		→ List of CRs:
MS test specifications		→ List of CRs:
BSS test specifications		→ List of CRs:
O&M specifications		→ List of CRs:

Other comments: The changes proposed by T-Mobil are not included.

help.doc

<--------- double-click here for help and instructions on how to create a CR.

6.1 User identity confidentiality

6.1.1 General

The mechanisms for user identity confidentiality described in 6.1 protect against passive attacks on user identity confidentiality by allowing the identification of a user on the radio access link by means of a temporary user identity (TMSI or P-TMSI).

In the CS service domain, the TMSI is used. A TMSI has local significance only in the location area in which the user is registered. Outside that area it should be a accompanied by an appropriate LAI in order to avoid ambiguities. The association between the permanent and temporary user identities is kept by the VLR in which the user is registered.

Analogously, in the PS service domain, the P-TMSI is used. A P-TMSI has local significance only in the routing area in which the user is registered; outside that area it should be a accompanied by an appropriate RAI. The association between the permanent and temporary user identities is kept by the SGSN database in which the user is registered.

Either the TMSI or P-TMSI, when available, is normally used to identify the user on the radio access path, for instance in paging requests, location update requests, attach requests, service requests, connection re-establishment requests and detach requests.

The implementation and use of temporary identities is mandatory in UMTS.

In the event that no temporary user identity is available or the network side cannot resolve the IMSI from the temporary user identity that is presented, the network can request the user to send the permanent user identity in cleartext. This is a breach in user identity confidentiality. The mechanisms in 6.2 and annex B provide a way around this breach.

6.1.2 Scenarios

6.1.2.1 Network-initiated connection establishment

Network-initiated connection establishment starts with paging the user. The scenario is shown in Figure 6.1.1.

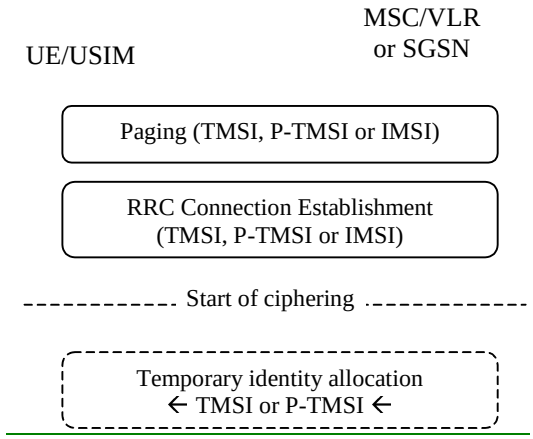

Figure 6.1.1: Network-initiated connection establishment

The VLR shall select the user identity according to the following rules:

- when a (single) TMSI is available in the VLR, the VLR shall use the TMSI;
- otherwise, the VLR shall use the IMSI.

The SGSN shall select the user identity according to the following rules:

- when a (single) P-TMSI is available in the SGSN, the SGSN shall use the P-TMSI;
- otherwise, the SGSN shall use the IMSI.

Upon receipt of a *paging request* that contains either the TMSI, the P-TMSI or the IMSI the user initiates *RRC connection establishment* referencing the forgoing *paging request*. During RRC connection establishment the user is

identified by means of the user identity that was included in the *paging request*.

When the user does not respond to paging requests with the TMSI or P-TMSI, it should be concluded that the user is not reachable. Nevertheless, the VLR or SGSN may attempt to reach the user by means of paging with the IMSI.

The VLR or SGSN may now allocate a new temporary identity to the user. This procedure is described in 6.1.3.1. Before allocating a new temporary identity, the VLR or SGSN should start ciphering. When the user was identified by means of an IMSI, the VLR or SGSN shall allocate a new temporary identity to the user.

6.1.2.2 User-initiated connection establishment – temporary identity available

User-initiated connection establishment starts with the user requesting an RRC connection establishment. The scenario is shown in Figure 6.1.2.

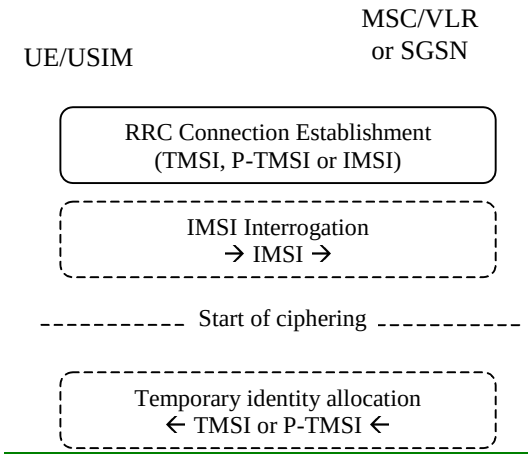

Figure 6.1.2: User-initiated connection establishment

The UE shall select the user identity according to the following rules:

- when it attempts to access CS services and a valid TMSI is available, the UE shall use the TMSI;
- when it attempts to access PS services and a valid P-TMSI is available, the UE shall use the P-TMSI;
- otherwise, the UE shall use the IMSI.

When a TMSI or P-TMSI is used, the VLR or SGSN shall attempt to resolve the user's IMSI from the TMSI or P-TMSI. In case two TMSI or P-TMSI are assigned to a user, the temporary user identity not used is released.

In case the user's IMSI cannot be resolved, the VLR or SGSN shall initiate the IMSI interrogation procedure with the user. In the response, the user (without eUIC) shall include the IMSI in cleartext. This procedure is described in 6.1.3.2.

Note: When the user has eUIC, the procedures described in 6.2 apply.

In case two TMSI (or P-TMSI) were associated to a user, the VLR or SGSN may initiate the IMSI interrogation procedure and possibly authentication and key agreement, in order to verify the user identity.

The VLR or SGSN may allocate a new temporary identity to the user. This procedure is described in 6.1.3.1. It shall allocate a new temporary identity when it had two temporary identities or when the TMSI or P-TMSI could not be resolved or when the user used the IMSI. Before allocating a new temporary identity, the VLR or SGSN should start ciphering.

6.1.2.3 Location update

Location update starts with the user establishing an RRC connection. The scenario is shown in Figure 6.1.3.

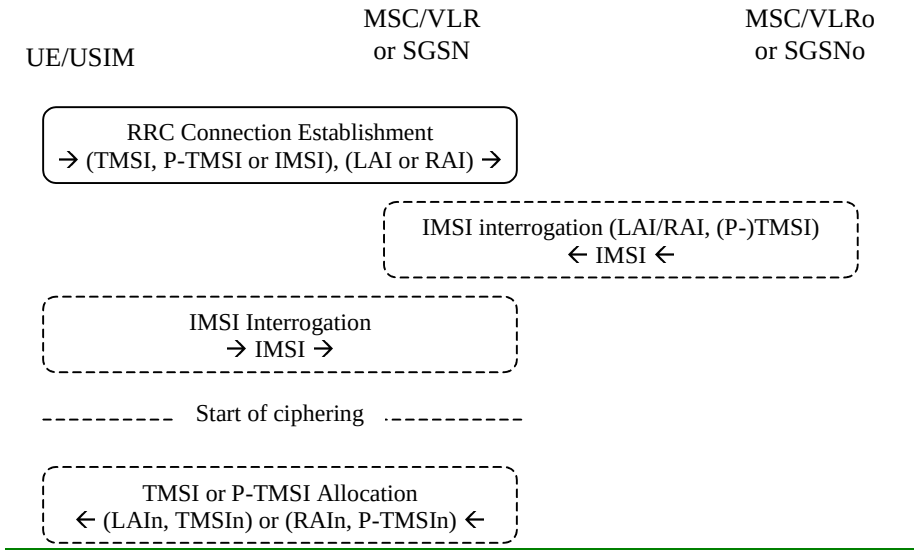

Figure 6.1.5: Location update with a temporary identity

The UE shall select the user identity according to the following rules:

- when it attempts to access CS services and a valid (TMSI, LAI) pair is available, the UE shall use the (TMSI, LAI) pair;
- when it attempts to access PS services and a valid (P-TMSI,RAI) is available, the UE shall use the (P-TMSI, RAI) pair;
- otherwise, the UE shall use the IMSI and the LAI or RAI.

Upon receipt of the location update request in which a TMSI or P-TMSI was used, the VLR or SGSN verifies the LAI or RAI and determines whether the user performs a location update in the same or in a new VLR or SGSN area:

- When the user performs a location update in the same VLR or SGSN area, the VLR or SGSN shall attempt to resolve the user's IMSI from the TMSI or P-TMSI. In case two TMSI or P-TMSI are assigned to a user, the temporary identity not used is released.
- When the user performs a location update in a new VLR or SGSN area, and the new VLR or SGSN and the old VLR or SGSN exchange identification data (i.e., belong to the same serving network), the new VLR or SGSN shall interrogate the old VLR or SGSN. The old VLR or SGSN shall then attempt to resolve the user's IMSI from the LAI and TMSI or RAI and P-TMSI and if successful send the IMSI to the new VLR or SGSN. This procedure is described in 6.3.3.3.

In case the user's IMSI cannot be resolved, the VLR or SGSN shall initiate the *IMSI interrogation* procedure with the user. In the response, the user (without eUIC) shall include the IMSI in cleartext. This procedure is described in 6.1.3.2.

Note: When the user has eUIC, the procedures described in 6.2 apply.

The VLR or SGSN may now allocate a new temporary identity to the user. This procedure is described in 6.1.3.1. It should allocate a new temporary identity when it had two temporary identities. Before allocating a new temporary identity, the VLR or SGSN should start ciphering.

Note: In the event the user has performed a location update in a new VLR or SGSN, the VLR shall inform the HLR. The HLR may in its turn inform the previously visited VLR or SGSN. These procedures however are not related to user identity confidentiality.

6.1.3 Procedures

6.1.3.1 Temporary identity allocation

The purpose of the temporary identity allocation procedure is to allocate a new (LAI, TMSI) or (RAI, P-TMSI) pair to a user.

The procedure should be ran at least after each location update in a new location area or after each routing area update

in a new routing area.

The procedure can be initiated by the serving domain at any time whilst a radio connection exists. The procedure should be performed after the initiation of ciphering. The ciphering of communication over the radio path is specified in clause 6.6. The allocation of a temporary identity is illustrated in Figure 6.1.7. Details on the procedure for the CS service domain can be found in TS 24.008, 4.3.1.

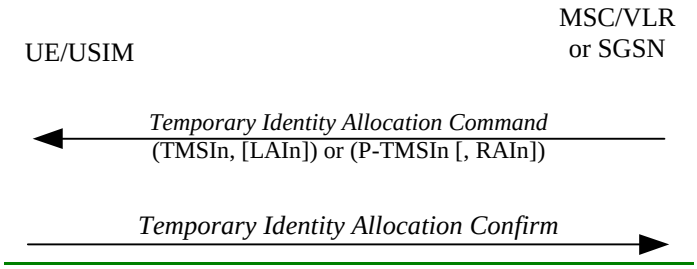

Figure 6.1.7: Temporary identity allocation procedure

The allocation of a temporary identity is initiated by the VLR or SGSN.

The VLR or SGSN generates a new temporary user identity (TMSIn or P-TMSIn) and stores the association with the permanent user identity IMSI. The TMSI or P-TMSI should be unpredictable.

The VLR or SGSN then sends a *temporary identity allocation command* to the user that

- shall include the new temporary identity TMSIn or P-TMSI and
- after a location update in a new location area or routing area, shall include the new location area identity LAIn or new routing area identifier RAIn.

Upon receipt the user stores the new temporary identity and new location information and automatically removes the association with the previously stored temporary identity and location information (of the service domain that is updated). The user sends an acknowledgement back to the VLR or SGSN.

Upon receipt of the acknowledgement the VLR or SGSN removes the association with the old temporary identity TMSIo or P-TMSIo and the IMSI (if there was any) from its database. If the VLR or SGSN does not receive an acknowledgement, it maintains both the new and the old TMSI in its database.

Repeated failure of temporary identity allocation procedures (passing a limit set by the operator) may be reported for O&M action.

6.1.3.2 IMSI interrogation of the user

The purpose of the IMSI interrogation procedure is to obtain the IMSI from the user. The procedures is shown in Figure 6.1.8. Details on the procedure for the CS service domain can be found in TS 24.008, 4.3.3.

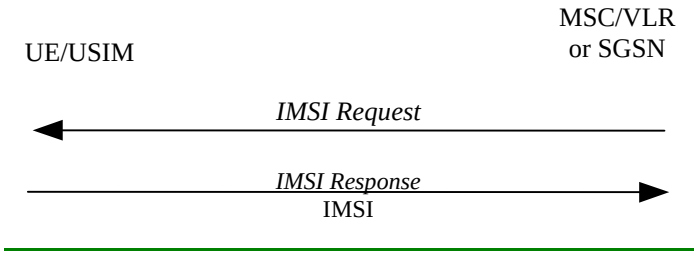

Figure 6.1.8: IMSI interrogation of the user

The VLR or SGSN sends the user an *IMSI request*. If the user has no eUIC, it responds with the *IMSI response* message and includes the IMSI in cleartext and deletes the TMSI or P-TMSI. If the user has eUIC, the procedures described in 6.2 apply.

6.1.3.3 Paging

The purpose of paging is to entice the user to initiate an RRC connection establishment. The procedure is shown in Figure 6.1.9.

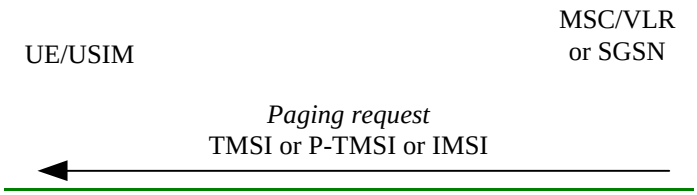

Figure 6.1.9: Paging

The VLR shall page with the TMSI when one is available. When no TMSI is available or when two TMSI are available, the VLR shall page with the IMSI.

The SGSN shall page with the P-TMSI when one is available. When no P-TMSI is available or when two P-TMSI are available, the SGSN shall page with IMSI.

6.1.3.4 IMSI interrogation to a VLR or SGSN

The purpose of IMSI interrogation to a VLR or SGSN is to resolve the IMSI from a (LAI, TMSI) pair or (RAI, P-TMSI) pair. The procedure is described in 6.3.3.3.

6.1 Identification by temporary identities

6.1.1 General

This mechanism allows the identification of a user on the radio access link by means of a temporary mobile user identity (TMUI). A TMUI has local significance only in the location area in which the user is registered. Outside that area it should be a accompanied by an appropriate Location Area Identification (LAI) in order to avoid ambiguities. The association between the permanent and temporary user identities is kept by the Visited Location Register (VLR) in which the user is registered.

The TMUI, when available, is normally used to identify the user on the radio access path, for instance in paging requests, location update requests, attach requests, service requests, connection re-establishment requests and detach requests.

6.1.2 TMUI reallocation procedure

The purpose of the mechanism described in this subsection is to allocate a new TMUI/LAI pair to a user by which he may subsequently be identified on the radio access link.

The procedure should be performed after the initiation of ciphering. The ciphering of communication over the radio path is specified in clause 6.6. The allocation of a temporary identity is illustrated in Figure 3.

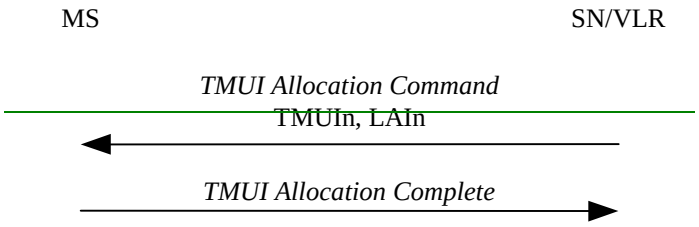

Figure 3: TMSI allocation

The allocation of a temporary identity is initiated by the VLR.

The VLR generates a new temporary identity (TMUIn) and stores the association of TMUIn and the permanent identity IMUI in its database. The TMUI should be unpredictable. The VLR then sends the TMUIn and (if necessary) the new location area identity LAIn to the user.

Upon receipt the user stores TMUIn and automatically removes the association with any previously allocated TMUI. The user sends an acknowledgement back to the VLR.

Upon receipt of the acknowledgement the VLR removes the association with the old temporary identity TMUIo and the IMUI (if there was any) from its database.

6.1.3 Unacknowledged allocation of a temporary identity

If the serving network does not receive an acknowledgement of the successful allocation of a temporary identity from the user, the network shall maintain the association between the new temporary identity TMUIn and the IMUI and between the old temporary identity TMUIo (if there is any) and the IMUI.

For a user-originated transaction, the network shall allow the user to identify itself by either the old temporary identity TMUIo or the new temporary identity TMUIn. This allows the network to determine the temporary identity stored in the mobile station. The network shall subsequently delete the association between the other temporary identity and the IMUI, to allow the temporary identity to be allocated to another user.

~~For a network-originated transaction, the network shall identify the user by its permanent identity (IMUI). When radio contact has been established, the network shall instruct the user to delete any stored TMUI. When the network receives an acknowledgement from the user, the network shall delete the association between the IMUI and any TMUI to allow the released temporary identities to be allocated to other users.~~

~~Subsequently, in either of the cases above, the network may initiate the normal TMUI reallocation procedure.~~

~~Repeated failure of TMUI reallocation (passing a limit set by the operator) may be reported for O&M action.~~

~~6.1.4 Location update~~

~~In case a user identifies itself using a TMUIo/LAIo pair that was assigned by the visited VLRn the IMUI can normally be retrieved from the database. If this is not the case, the visited VLRn should request the user to identify itself by means of its permanent user identity. This mechanism is described in 6.2.~~

~~In case a user identifies itself using a TMUIo/LAIo pair that was not assigned by the visited VLRn and the visited VLRn and the previously visited VLRo exchange authentication data, the visited VLRn should request the previously visited VLRo to send the permanent user identity. This mechanism is described in 6.3.4, it is integrated in the mechanism for distribution of authentication data between VLRs. If the previously visited VLRo cannot be contacted or cannot retrieve the user identity, the visited VLRn should request the user to identify itself by means of its permanent user identity. This mechanism is described in 6.2.~~

6.2 Enhanced user identity confidentiality

6.2.1 General

The mechanisms for enhanced user identity confidentiality described in 6.2 protect against active attacks on user identity confidentiality by allowing the identification of a user on the radio access link by means of the encryption of the permanent user identity and provision of a user identity for paging the user.

The mechanism is triggered by the identification request message sent by the VLR or SGSN and should only be used when no valid temporary user identity is available in the VLR and in the UE/USIM.

For the purpose of the eUIC a new logical network node UIDN is introduced. The serving VLR or SGSN shall be able to request decryption of the user identity by this home network node.

The UIDN is in charge of decrypting the encrypted IMSI provided by the mobile station in the UIDN-message. The UIDN is a home network operator specific logical network node and may be co-located with the HLR.

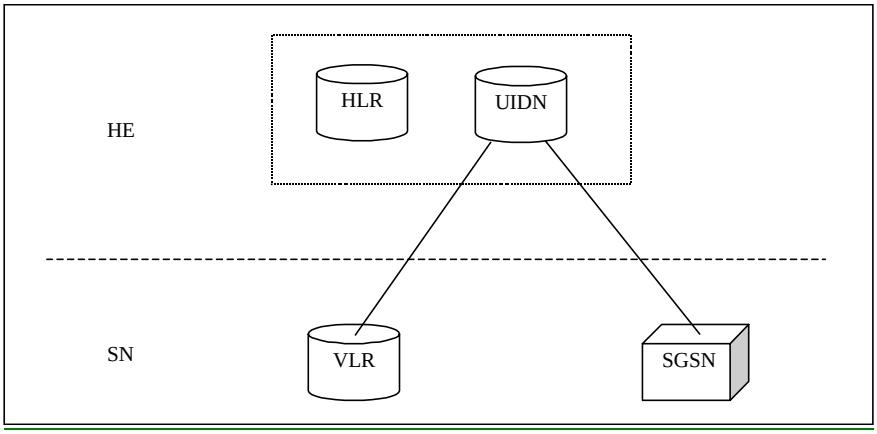

Figure 6.2.1: Core Network Architecture for Enhanced User Identity Confidentiality

The interface between the VLR and the UIDN is used by the VLR to request the decryption of the EIMSI contained in the UIDN-message from the UIDN for the CS service domain.

The interface between the SGSN and the UIDN is used by the SGSN to request the decryption of the EIMSI contained in the UIDN-message from the UIDN for the PS service domain.

6.2.2 Scenarios

6.2.2.1 Network-initiated connection establishment

Network-initiated connection establishment is identical for all users.

6.2.2.2 User-initiated connection establishment

When a user with eUIC attempts to establish a connection with a service domain and uses an unresolvable temporary user identity, the VLR or SGSN shall initiate IMSI interrogation and the user (with eUIC) shall respond with the EMSI and the UIDN address. The VLR or SGSN shall interrogate the UIDN to obtain the user's IMSI. The mechanism is shown in Figure 6.2.2.

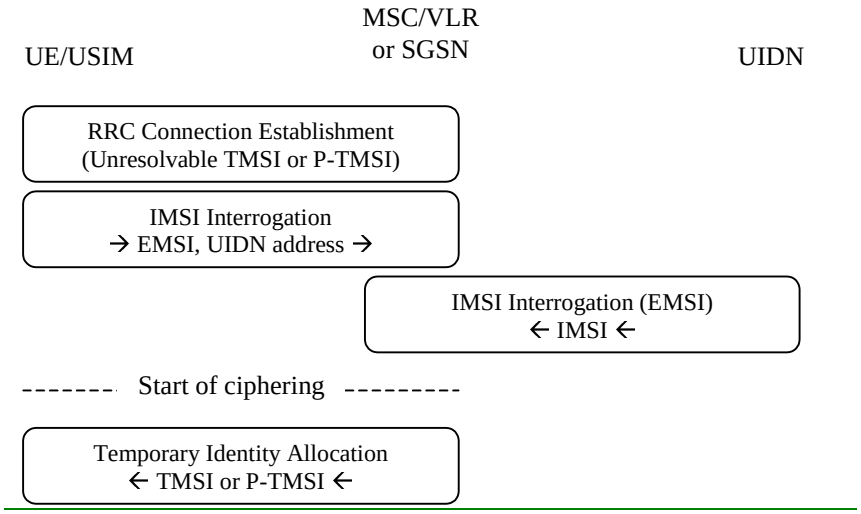

Figure 6.2.2: User-initiated connection establishment for users with eUIC

The user's TMSI or P-TMSI cannot be resolved the VLR or SGSN initiates the IMSI interrogation procedure with the user. In the response, the user (with eUIC) includes the EMSI and the UIDN address.

Subsequently, the VLR or SGSN shall interrogate the user's UIDN in order to obtain the user's IMSI. The user's IMSI is included in the response from the UIDN. This procedure is described in 6.2.3.2.

The VLR or SGSN should now allocate a new temporary identity to the user. This procedure is described in 6.1.3.1. Before allocating a new temporary identity, the VLR or SGSN should start ciphering.

6.2.2.3 Location update

This mechanism describes the case whereby a user with eUIC attempts a location update (resp. routing area update) and uses an unresolvable TMSI (resp. P-TMSI). The mechanism is shown in Figure 6.2.3.

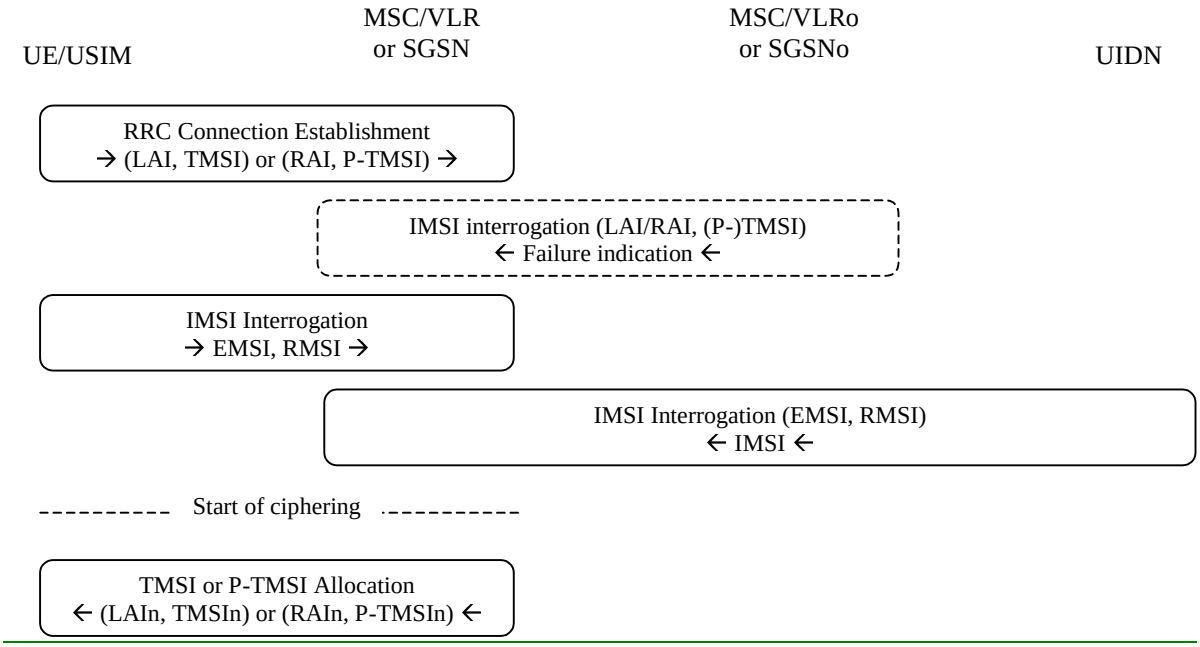

Figure 6.2.3: Location update for users with eUIC

Upon receipt of the location update request, the VLR or SGSN verifies the LAI or RAI and determines whether the user performs a location update in the same or in a new VLR or SGSN area. We assume here that the user's IMSI cannot be resolved. This is the case when:

– The user performs a location update in the same VLR or SGSN area, and the VLR or SGSN cannot resolve the IMSI from the TMSI or P-TMSI;

- The user performs a location update in a new VLR or SGSN area, and the new VLR or SGSN and the old VLR or SGSN do not exchange identification data (e.g., they may not belong to the same serving network);
- The user performs a location update in a new VLR or SGSN area, the new VLR or SGSN and the old VLR or SGSN exchange identification data (i.e., they belong to the same serving network), but the old VLR or SGSN cannot resolve the IMSI from the TMSI or P-TMSI.

The VLR or SGSN initiates the *IMSI interrogation* procedure with the user. In the response, the user (with eUIC) shall include the EMSI and the UIDN address.

Subsequently, the VLR or SGSN shall interrogate the user's UIDN in order to obtain the user's IMSI. The user's IMSI is included in the response from the UIDN. This procedure is described in 6.2.3.2.

The VLR or SGSN should now allocate a new temporary identity to the user. This procedure is described in 6.1.3.1. Before allocating a new temporary identity, the VLR or SGSN should start ciphering.

Note: In the event the user has performed a location update in a new VLR or SGSN, the VLR shall inform the HLR. The HLR may in its turn inform the previously visited VLR or SGSN. These procedures however are not related to user identity confidentiality.

6.2.3 Procedures

6.2.3.1 IMSI interrogation to the user

The purpose of the IMSI interrogation procedure to the user is to obtain the IMSI from the user. Users with eUIC however, respond to an *IMSI request* by means of an *IMSI response* that includes an EMSI and a UIDN address. The procedures is shown in Figure 6.2.4.

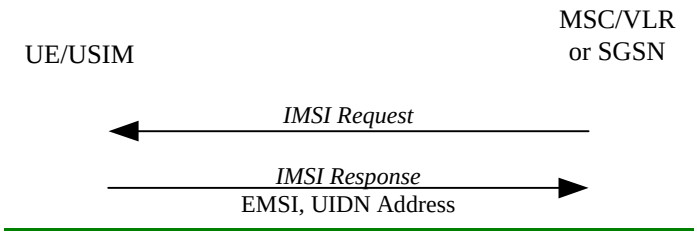

Figure 6.2.4: IMSI interrogation of the user (with eUIC)

The VLR or SGSN sends the user an *IMSI request*. In this case the user has eUIC. Upon receipt of an *IMSI request*, the UE passes the request to the USIM which returns the UIDN address and an encrypted user identity EMSI. The UDIN address allows the VLR or SGSN to address the user's UIDN. The EMSI allows the user's UIDN to retrieve the IMSI. The UE includes the EMSI and the UIDN address in its response to the VLR or SGSN.

The encryption/decryption mechanism is not specified. An example mechanism using group keys is described in annex B.

6.2.3.2 IMSI interrogation to the UIDN

The purpose of the IMSI interrogation to the UIDN procedure is to obtain the IMSI from UIDN, from the EMSI provided by the user. The procedures is shown in Figure 6.2.7.

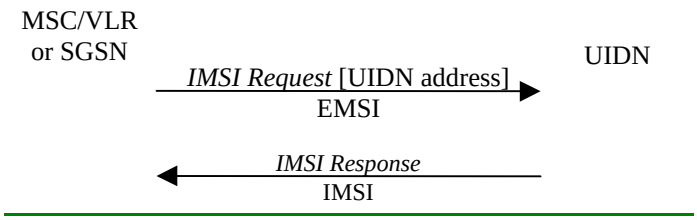

Figure 6.2.7: IMSI interrogation to the UIDN

The VLR or SGSN sends the UIDN an *IMSI request* with the EMSI. The UIDN address is included for routing purposes

only.

Upon receipt, the UIDN resolves the IMSI from the EMSI. The encryption/decryption mechanism is not specified. An example mechanism using group keys is described in annex B.

The UIDN includes the EMSI in its response to the VLR or SGSN.

6.2 Identification by a permanent identity

The mechanism described in here allows the identification of a user on the radio path by means of the permanent user identity (IMUI).

The mechanism should be invoked by the serving network whenever the user cannot be identified by means of a temporary identity. In particular, it should be used when the user registers for the first time in a serving network, or when the serving network cannot retrieve the IMUI from the TMUI by which the user identifies itself on the radio path.

The mechanism is illustrated in Figure 4.

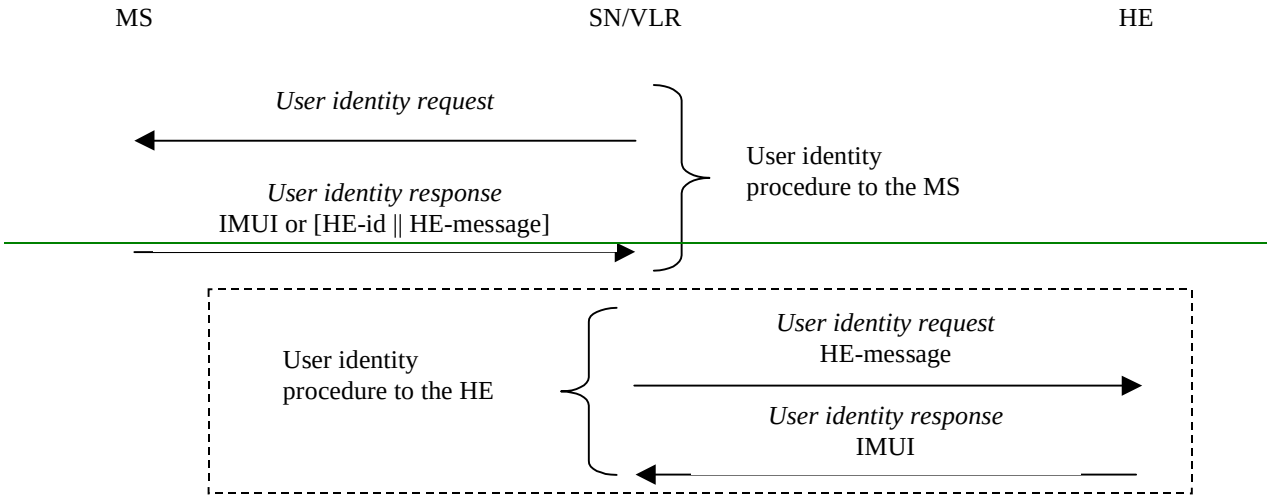

Figure 4: Identification by the permanent identity

The mechanism is initiated by the visited SN/VLR that requests the user to send its permanent identity. According to the user's preferences, his response may contain either 1) the IMUI in cleartext, or 2) the user's HE-identity in cleartext and an HE-message that contains an encrypted IMUI.

The term HE-id denotes an expression which is sufficient to route the user identity request message to an appropriate network element in the HE. Annex B contains a proposal to use MCC, MNC and the first three digits of the user's MSIN as routing information to address an HE/HLR.

In case the response contains the IMUI in cleartext, the procedure is ended successfully. This variant represents a breach in the provision of user identity confidentiality.

In case the response contains an encrypted IMUI, the visited SN/VLR forwards the HE-message to the user's HE in a request to send the user's IMUI. The user's HE then derives the IMUI from the HE-message and sends the IMUI back to the SN/VLR. Annex B describes an example mechanism that makes use of group keys to encrypt the IMUI.