3GPP TSG SA WG3 Security — S3#28 **S3-030225**
6 - 9 May 2003 Berlin, Germany

Source: **Siemens**

Title: **Unciphered IMEISV transfer (Early UE)**

Document for: **Discussion and Decision**

Agenda Item: **7.5**

Abstract

This contribution provides inputs for replying to the LS from S2 (S3-030192(S2-031565)) on unciphered IMEI transfer.

1) Introduction on Early UE handling

TS 23.195 V1.0.0 (2003-03), under SA2 responsibility, describes the provision of UE Specific Behaviour Information to Network Entities. This Stage 2 description describes how UESBI-Iu and UESBI-Uu are sent to the RAN. UESBI may be used by correction mechanisms to overcome some of the issues that have been recognized by 3GPP in TR 25.994 (Measures employed by the UMTS Radio Access Network (UTRAN) to overcome early User Equipment (UE) implementation faults). Below are the definitions copied from the TS:

> ***"UE Specific Behaviour Information - Uu (UESBI-Uu):*** *is information that is sent using Access Stratum signalling from the UE to the RAN. It can be used to derive some specific information about the UE's capabilities.*
>
> ***UE Specific Behaviour Information - Iu (UESBI-Iu****): is information that is sent from the MSC and/or SGSN to the RAN that can be used to derive some specific information about the UE's capabilities."*

In particular UESBI-Iu is derived from the IMEISV. The scenarios on the provision of UESBI to the SRNC have been copied below from TS 23.195 clause 4.3. SA2 in particularly asks whether there are security issues for IMEISV request within procedure 1 (red arrow) in order to be able to plan the timing of procedure 3 (blue arrow).

> *"The IMEISV information is retrieved from the UE and stored in the VLR and SGSN. At subsequent Iu interface connection establishment, the UESBI-Iu [derived from the IMEI-SV] is sent to the SRNC when the Iu signaling link between MSC and SRNC, or SGSN and SRNC, has been established. The UESBI-Iu is normally sent in the same procedure that currently carries the IMSI. This is summarised in figure 4.3-1.*

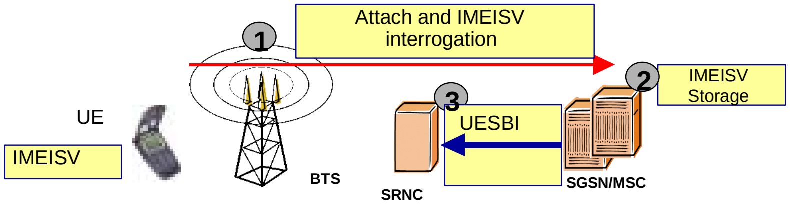

Figure 4.3-1: UESBI–Iu architecture

> *If the UE state is changed from RRC Connected to RRC Idle, all information derived from the received UESBI is released in the RNS. Thus if the UE state is changed afterwards back to RRC Connected the delivery of the UESBI-Iu from MSC or SGSN to SRNC shall be repeated."*

2) Requirements on the start of Iu-mode protection

TS 33.102 Clause 6.4.5 (Security mode set-up procedure) specifies the timing of the start of integrity and ciphering between the RNC and the UE.

/REQ-A/ :

> *" When the integrity protection shall be started, the only procedures between MS and VLR/SGSN that are allowed after the initial connection request (i.e. the initial Layer 3 message sent to VLR/SGSN) and before the security mode set-up procedure are the following:*
>
> - *Identification by a permanent identity (i.e. request for IMSI), and*
> - *Authentication and key agreement."*

For identification of a MS following rule apply: Normally, the mobile station will be identified by an TMSI (or IMSI). However, if none of these identifiers is available in the mobile station, then the mobile station shall use the IMEI for identification purposes. The Identity Request procedure from SN to MS (before authentication) is optional and executed if the provided identity (i.e.TMSI) within the initial layer 3 request could not be found back by the SN. Therefore the IMEI will not be requested before start of ciphering for purposes of authentication.

According to TS 23.060 (stage 2 PS domain), the network can retrieve the IMEI from the MS with the same Identity Request procedure (TS 24.008) as mentioned is previous paragraph. TS 23.060 makes no statements about dependencies between the IMEI retrieval and ciphering).

Conclusion: The procedures are in place to request the IMEISV before start of ciphering, but the cited Stage 2 requirement from TS 33.102 forbids this.

3) Requirements on IMEI transfer

TS 33.102 clause 5.1.5 specifies:

"5.1.5 Mobile equipment identification

> *In certain cases, SN may request the MS to send it the mobile equipment identity of the terminal. The mobile equipment identity shall only be sent after authentication of SN with exception of emergency calls. The IMEI should be securely stored in the terminal. However, the presentation of this identity to the network is not a security feature and the transmission of the IMEI is not protected. Although it is not a security feature, it should not be deleted from UMTS however, as it is useful for other purposes. "*

What follows is an analysis of the above sentences:

> */REQ-B/ "The mobile equipment identity shall only be sent after authentication of SN with exception of emergency calls".*

The Serving Network is the requestor of the IMEI, therefore the sentence reads as a requirement to the UE. The UE shall not answer to any IMEI request (except the emergency call) sent before the Serving Network has been authenticated. From the viewpoint of the UE, the Serving Network is only authenticated successfully if AUTN could be validated. But that requires that AUTN has reached the mobile and that the

Serving Network runs an explicit authentication. The first pre-requisite is always fulfilled for an Iu-mode connection attempt. The second pre-requisite is more not valid than valid. In most cases an implicit authentication is performed by using directly the available key set (referenced by KSI within initial layer 3 message : I.e. attach, location update, ...) at UE and SN. The SN authentication from UE point view can therefore only be validated at the start of integrity protection (I.e. when the UE verifies the MAC-I within of the Security mode command). When the Serving Network receives the security mode complete, it can be sure that the integrity and confidentiality (if applied) protection was started. This interpretation is much inline with /REQ-A/ that does not allow any other NAS procedure other than IMSI request before ciphering is started. A strict interpretation makes the /REQ-B/ superfluous as that case is not allowed.

> */REQ-C/ "The IMEI should be securely stored in the terminal. However, the presentation of this identity to the network is not a security feature and the transmission of the IMEI is not protected".*

It is not so clear what this 'protected' means within the context of the above sentence. Does it mean a) integrity protected on the air interface, or b) confidentiality protected on the air interface or c) both former interpretations. If interpretation 'b)' is the right one, then this implies that are no issues in sending the IMEI unprotected (I.e. in cleartext) over the air, being in contradiction with the /REQ-B/ in certain scenarios.

3) Handling of IMEI during GSM coverage

The early UE feature is applicable to UMTS terminals and GSM/UMTS dual system terminals. Therefore, it is possible that a UE starts with a GSM access and afterwards performs an inter-system handover to UMTS. For the inter-system handover, the MSC will have to send UESBI-Iu to the target RNC, i.e. it needs the IMEI-SV at the beginning of the inter-system handover. In this case, the MSC needs to retrieve the IMEI-SV from the UE while it is in GSM coverage: either during a previous location update procedure (and the IMEI-SV is stored in the VLR) or during the current GSM access itself. The security stage 2 requirements are covered within TS 42.009. Section 3.5.3 states (italic text):

"The signalling information elements included in the message used to establish the connection (protocol discriminator, connection reference, message type and MS identity (IMSI, TMSI or IMEI according to the circumstance)) are not protected.

The following signalling information elements related to the user are protected whenever used <u>after connection establishment:</u>

- *International Mobile Equipment Identity (IMEI).*
- *International Mobile Subscriber Identity (IMSI).*
- *Calling subscriber directory number (mobile terminating calls).*
- *Called subscriber directory number (mobile originated calls)."*

This above requirements in TS 42.009 seem not to rule out the possibility of requesting the IMEI of the user, before ciphering has been started. Indeed, when looking in TS 24.008 (Stage 3 description) it is specified that the network can request IMEISV within the authentication and ciphering request. The response of this procedure is not ciphered, therefore <u>GSM-procedures allow to request IMEI over an unciphered connection (no IMEI privacy is provided).</u>

4) Threats when exposing the IMEI on the air interface

/REQ-B/ serves in denying Serving Networks that have no roaming agreements with the Home Networks requesting the IMEI of subscribers. This alone seems not to be a privacy problem as any unauthenticated SN is able to request the IMSI of the subscriber too. But as soon as the Security mode command response was received by the SN, every NAS-signalling message is protected. The temporary identifier (P-)TMSI serves in providing user identity confidentiality and is transferred to the user over a ciphered connection. Further identity exchanges (IMEI, IMEISV,IMSI) are protected too. Whenever the request for IMEI would be allowed before ciphering is started, it would weaken the privacy of the subscriber at the air interface. Given the fact that users don’t change their mobile very often (the relation IMSI-IMEI is *de facto* fixed some years), and passive observation could record the relation between IMSI and IMEI. Seeing IMEI travelling the air-interface in clear-text provides some means for an attacker to go around the user identity confidentiality feature, and as such weakens the location privacy of the user proportional to the frequency of the IMEISV-request. This however needs only be done when a new MM-context needs to be build up at the network side.

5) Conclusions

- Stage 2 specification TS 33.102 is dubious about the possibility of requesting the IMEI over an unciphered connection. On one hand, it disallows requesting the IMEI before ciphering has been started, on the other hand it is stated that the transmission of the IMEI is not protected. The cited TS 33.102 requirements shall be aligned to avoid misunderstanding.
- Mobile behaving conforming TS 33.102 /REQ-B/ will not answer the IMEI(-SV) request before authentication (or even start of integrity protection depending on the scenario). According /REQ-A/ it is even not allowed to request the IMEI before ciphering has been started. However, since /REQ-B/ has not been implemented explicitly in the stage 3, TS 24.008, the behaviour of actual mobile implementations is not clear. Furthermore, there is a certain danger that refusal by the MS to send the IMEI(-SV) will result in an abort of the ongoing (G)MM procedure by the network, or problems if the network implementation insists on retrieving it before it initiates the security mode procedure. Probably, SA3 needs to ask the manufacturers in CN1 whether any MS manufacturer has implemented requirement /REQ-B/.
- It is possible to request the IMEI-SV before start of ciphering as the procedures are in place. If the MS answers, this will weaken the location privacy of the subscriber proportional to the frequency of the request.

6) Annex 1: Excerpt of TS 24.008

According to Siemens interpretation /REQ-B/ has not been implemented in the stage 3, TS 24.008. E.g. in section 4.1.1.1.1, Integrity Checking of Signalling Messages in the Mobile Station (UMTS only), it is stated:

***** start of excerpt ******

"…

Except the messages listed below, no layer 3 signalling messages shall be processed by the receiving MM and GMM entities or forwarded to the CM entities, unless the security mode control procedure is activated for that domain.

- *MM messages:*
  - *AUTHENTICATION REQUEST*
  - *AUTHENTICATION REJECT*
  - *IDENTITY REQUEST*
  - *LOCATION UPDATING ACCEPT (at periodic location update with no change of location area or temporary identity)*

  …

- *GMM messages:*
  - *AUTHENTICATION & CIPHERING REQUEST*
  - *AUTHENTICATION & CIPHERING REJECT*
  - *IDENTITY REQUEST*

…"

***** End of excerpt ******

and for the (GMM) Identification procedure it is stated:

***** start of excerpt ******

"4.7.8 Identification procedure

The identification procedure is used by the network to request an MS to provide specific identification parameters to the network e.g. International Mobile Subscriber Identity, International Mobile Equipment Identity (see 3GPP TS 23.003). For the presentation of the IMEI, the requirements of 3GPP TS 42.009 apply.

4.7.8.1 Identification initiation by the network

The network initiates the identification procedure by transferring an IDENTITY REQUEST message to the MS and starts the timer T3370. The IDENTITY REQUEST message specifies the requested identification parameters in the identity type information element.

4.7.8.2 Identification response by the MS

An MS that has been attached to GPRS shall be ready to respond to an IDENTITY REQUEST message at any time.

Upon receipt of the IDENTITY REQUEST message the MS sends back an IDENTITY RESPONSE message. The IDENTITY RESPONSE message shall contain the identification parameters as requested by the network. "

4.7.8.3 Identification completion by the network

Upon receipt of the IDENTITY RESPONSE the network shall stop timer T3370.

4.7.8.4 Abnormal cases on the network side

The following abnormal cases can be identified:

…

b) *Expiry of timer T3370*

> *The identification procedure is supervised by the network by the timer T3370. The network shall, on the first expiry of the timer T3370, retransmit the IDENTITY REQUEST message and reset and restart the timer T3370. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3370, the network shall abort the identification procedure and any ongoing GMM procedure.*

***** End of excerpt ******