3GPP TSG SA WG3 (Security) meeting #28 **S3-030277**

6-9 May 2003, Berlin, Germany

Title: **Draft** Reply LS on unciphered IMEISV transfer
Response to: **S2-031565 (S3-030192)**
Release: --
Work Item: Early UE

Source: SA3
To: SA2, CN1
Cc: --

Contact Person:

Name: Marc Blommaert
Tel. Number: +32 14 25 3411
E-mail Address: Marc.Blommaert@siemens.com

Attachments: None

---

1. Overall Description:

SA3 thanks SA2 for their liaison on unciphered IMEISV transfer.

SA3 understands that it is desirable to request the IMEISV before the security mode command. One of the reasons is to be able to handle faulty ciphering behaviour of non fully ciphering tested early UE's. Early availability of UE's and RNC's with ciphering capabilities would help a lot here.

Security Requirements:

The stage-2 specification TS 33.102 contains following statement in clause 6.4.5 (Security mode set-up procedure) that is relevant for the timing of procedures (e.g. IMEISV request) after the initial contact message sent to VLR/SGSN:

> *" 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."*

According to the above requirement the VLR/SGSN shall not request the IMEISV before the security mode set-up procedure has been completed.

However, it was also indicated that

A) Stage-3 specification TS 24.008 seems not to include any timing restrictions in VLR/SGSN or UE on handling an IMEISV request.

B) During GSM coverage, the unciphered authentication and ciphering response may include an IMEISV.

Privacy implications:

Whenever the request for IMEISV 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), 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 (TMSI), 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.

The conclusion of this are:

- It would be desirable from a privacy point of view to use the IMEISV stored from within the network, whenever possible.
- SA3 sees no privacy issue in sending the IMEISV together with the IMSI (i.e. a frequency less then a IMSI request would be in any case allowable).

Also following remarks seem to be useful for the privacy discussion.

1) Does the Serving Network need the full IMEI ?
2) If the Early-UE handling would rely on certain IMEISV's to disable the ciphering then an attacker could use this knowledge to substitute the unciphered IMEISV during transfer to the serving network.

Based on the current discussions, SA3 did decide to wait for more information before relaxing the TS 33.102 requirement in clause 6.4.5.

2. Actions

To [SA2] group:

SA3 asks SA2 to consider the above comments and to provide SA3 with any useful information such that a decision can be made.

To [CN1] group:

SA3 asks CN1 to check if Stage-3 specification TS 24.008 do not include any timing restrictions (in accordance with the mentioned clause 6.4.5 in TS 33.102) in VLR/SGSN or UE on handling an IMEISV request.

3. Date of Next TSG SA WG3 Meetings:

Meeting	Date	Location
SA3#29	15-18 July 2003	San Francisco, USA
SA3#30	7-10 Oct 2003	NN