3GPP TSG SA WG3 Security — S3#29 **S3-030312**
15 - 18 July 2003
San Francisco, USA

3GPP TSG-SA WG2 meeting #32 **Tdoc S2-032156**
San Diego, USA 12th – 16th April 2003 **rev of S2-031946**

Title:	**LS on** unciphered IMEISV transfer
Release:	Release 99
Source:	SA WG2
To:	SA WG3
Cc:	CN WG1, RAN WG2

Contact Person:

Name: Ravi Kuchibhotla, Motorola
E-mail Address: Ravi.Kuchibhotla@motorola.com

SA WG2 thanks SA3 for their reply on the issue of unciphered IMEISV transfer. Additional information on the issues raised by SA3 is provided below.

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

1) *Does the Serving Network need the full IMEI ?*
The Serving Node does not need the full IMEI and it is sufficient for it to be provided the TAC + SV information for the terminal. However, given the late stage of R99 it is considered very unlikely that CN WG1 would be able to make the necessary changes to their specifications to enable this change in behaviour.

2) *A network that disables ciphering for certain IMEISV may be vulnerable to a man-in-the-middle attack whereby the attacker substitutes the mobile's genuine IMEI with one that forces the network to disable encryption. SA3 has just started studying overcoming the potential attack.*
SA2 understands that one way forward on this issue is for the network to re-request the IMEISV after completion of the security mode set-up procedure. The necessary text related to this behaviour, or any other approach SA3 reach agreement on, is best captured in TS 33.102 where additional actions for the network have been specified.

Actions

To SA WG3

ACTION: To note the above and make the necessary changes to R99 TS 33.102 to align with the CN1 specifications and to address the man-in-the-middle attack.

Date of Next TSG SA WG2 Meetings

TSG SA WG2 Meeting #33	7th – 11th July 2003	France
TSG SA WG2 Meeting #34	18th – 22nd August, 2003	Brussels, Belgium

3GPP TSG-SA WG2 meeting #32 **Tdoc S2-031742**

San Diego, U.S.A. , 12th – 16th May 2003

____

3GPP TSG SA WG3 (Security) meeting #28 **S3-030294**

6-9 May 2003, Berlin, Germany

Title:	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: S3-030192 (S2-031565)

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 to avoid interoperability problems when ciphering is enabled in the network.

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 for 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 in clear together with the IMSI, when the mobile needs to identify itself by sending its IMSI in clear (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) A network that disables ciphering for certain IMEISV may be vulnerable to a man-in-the-middle attack whereby the attacker substitutes the mobile's genuine IMEI with one that forces the network to disable encryption.
   SA3 has just started studying overcoming the potential attack.

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 does not include any timing restrictions (in mis-alignment 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

3GPP TSG-SA WG2 meeting #31 **Tdoc S2-031565**
Seoul, Korea, 7th – 11th April 2003 **rev of S2-031334**

Title:	LS on unciphered IMEISV transfer
Response to:	n/a
Release:	Release 5
Work Item:	Late UE (Early UE)
Source:	SA WG2
To:	SA WG3
Cc:	

Contact Person:
Name: Frank Mademann
Tel. Number: +49 30 386 29079
E-mail Address: frank.mademann@siemens.com

Attachments: none

1. Overall Description:

SA2 evaluate mechanism to provide UE specific behaviour information to network entities. This information may be used by correcting mechanisms to overcome issues that have been recognised by 3GPP in TR 25.994 (Measures employed by the UMTS Radio Access Network (UTRAN) to overcome early User Equipment (UE) implementation faults), and other such documents.

The UE specifics are determined by means of the IMEISV. The network will retreive the IMEISV from the UE at each PS or CS Attach and in addition at each Location Area Updating when the MSC/VLR changes. The IMEISV is retrieved at these times in order to discover changes of the equipment (terminal type / software version). When a Iu interface connection is established for the UE, the UE specific behaviour information shall be sent as early as possible to the RAN, i.e. before the Security Mode Command is sent to the RAN. Because the IMEISV has to be obtained before the Security Mode Command, it will be transferred unciphered from the UE to the network.

SA2 ask SA3 to comment on any potential security issues caused by this transfer of the unciphered IMEISV within UE to network signalling.

2. Actions:

Evaluation of any potential security issues caused by the transfer of the unciphered IMEISV.

3. Date of Next TSG-SA WG2 Meetings:

SA2#32	12th – 16th May 2003	San Diego, USA
SA2#33	7th – 11th July 2003	Sophia-Antipolis, France