TSG-RAN Meeting #16 *RP-020274*
Marco Island, FL, USA, 4 - 7 June 2002

(S2-021503, to TSG-RAN) LS on Handling Early R'99 Mobiles

3GPP TSG-SA WG2 meeting #24 Tdoc S2-021503
Madrid, Spain, 22nd – 26th April 2002

Title: **LS on Handling Early R'99 Mobiles**
Source: SA 2
To: RAN, RAN 2
Cc: GERAN
Response to: **n/a**
Release: R'99

Contact Person:
Name: Chris Pudney
E-mail Address: Chris.Pudney@vf.vodafone.co.uk

Attachments: S2-021221

---

1. Overall Description:

SA 2 understand that at the last RAN plenary there was considerable debate over a change request proposing to introduce an "interim tested marker" into the UE capability information that is sent to the network, and that, in the end, the CR was withdrawn.

The stimulus for the debate seems to have been a concern that mobiles are unable to be fully tested against all of the mandatory features in the R'99 standard. Hence when one of the un-tested features is "switched on" in a network, there is a risk that some mobiles will not work with this feature. Some SA 2 delegates fear that this may happen and that important functionality may be impossible to use with any mobile.

An alternative proposal is that networks adapt their functionality so that they handle different types of mobiles differently. Although it is undoubtedly undesirable that RNCs handle different mobiles differently, it should be noted that typical GSM BSCs handle many mobile variations (eg most combinations of codecs (HR, FR, EFR, AMR) and frequency bands (GSM, EGSM, DCS, UMTS)).

As a consequence of this fear, SA 2 has briefly considered (but not concluded) the architectural impacts of the use of the IMEISV to influence the network's behaviour (either as a complement, or as an alternative, to the "interim tested marker"). The brief discussion of the attached S2-021221 is summarised in section 2 below, but its provisional conclusions are that:

a) the provision of the IMEISV to the RNC appears to impact several network entities and/or the UE. All these may well be supplied by different vendors;
b) the timescales involved in obtaining network functionality are frequently long (especially for functionality that relies upon support in multiple nodes from different vendors); and
c) there are several detailed questions that require the expertise of other WGs;

and therefore, **in the case that IMEISV dependent functionality might be needed, some more detailed feasibility studies should be considered**.

2 Handling IMEISV in the network

The following suggestions were made as different possible means of obtaining and using the IMEISV within the network:

2.1 Use of GMM/MM signalling to obtain IMEISV at Attach and use RANAP to carry it to the RNC

This raised a couple of issues:

a) Would this provide the IMEISV to the RNC early enough?

b) When using the Gs interface, the IMEI is not normally provided to the MSC as part of the attach procedure: hence changes to 29.018 and/or changes to MSC functionality may be needed.

c) Although most debate has focussed on RAN functionality, it should be noted that the mobile's functionality towards the 3G-SGSN is markedly different to that towards the 2G-SGSN. What method would the SGSN use to determine the mobile's capabilities from the IMEISV?

d) At inter-SGSN SRNS relocation, would the 'source' 3G-SGSN need to pass the IMEISV to the new 3G-SGSN?

2.2 Use of new RRC signalling to pass IMEISV from UE to RNC

Several delegates felt that it would be natural "to leave the RAN to sort out its own issues", for example, by adding the IMEISV (or just the TAC/FAC/SVN parts) to messages which carry the UE Capability information to the RAN. This raised the following issues:

a) This seems to require changes to be made NOW to the R'99 mobiles and has interesting consequences for mobiles which have already been built/designed.

b) How should the IMEI be handled at relocation/GSM to UMTS handover? Would this require changes to the GERAN radio and A interface standards, and, what impact would it have on Call Setup times in GSM?

2.3 How does the RNC use the IMEISV to derive the mobile's capabilities?

This was felt to be an internal RAN matter, however, similar problems might occur with, for example, the GSM Iu mode and so common solutions with GERAN might be interesting.

2.4 Allocation of SVN

The current rules for allocation of SVN seem to be unclear. For example, while the "Manufacturers shall allocate individual serial numbers (SNR) in a sequential order" there are almost no rules on the use of the SVN.

a) Is it worth specifying within 3GPP a format for the allocation and update of SVN? (eg that SVN starts at 0 and is increased by 1 for each update?)

2.5 Impact on the network due to security

The IMEI is a one time programmable field but SVN cannot be one time programmable. Hence there needs to be a means to change the SVN when the software is changed in the mobile. Therefore SVN cannot be as secure as the IMEI field. What is the impact on the network if a mobile indicates an IMEISV that does not align with actual software in the mobile?

3. Actions:

To RAN and RAN 2

SA2 are aware that RAN is investigating several other mechanisms for handling the above concerns. SA2 invite RAN and/or RAN 2 to consider 'sponsoring' a feasibility study that involves the impacted groups (eg SA 2, SA 3, GERAN 2, GERAN 5, RAN 2, RAN 3, CN 1, CN 4, T1).

4. Date of Next SA 2 Meetings:

SA 2 #25	24-28 June 2002	Finland.
SA 2 #26	19-23 August 2002	Toronto, Canada.

3GPP TSG-SA2 Meeting #24 ***Tdoc S2-021221***
Madrid, Spain, April 22-26, 2002

Source: Vodafone
Agenda item: R'99

Handling Early R'99 UMTS Mobiles

1 Introduction

At the last RAN plenary there was considerable debate over a change request proposing to introduce an "interim tested marker" into the mobile capabilities/classmark information that is sent to the network. In the end, the CR was rejected.

The stimulus for the debate was the concern that mobiles are unable to fully test all of the mandatory features in the R'99 standard. Hence when one of the un-tested features is "switched on" in a network, there is a risk that some mobiles will not work with this feature.

Vodafone believe that it is the responsibility of the mobile manufacturer to ensure that their products are fully compliant to the R'99 standard.

However, the experience of GSM has shown that different subsets of mobiles are likely to have different, as yet undetected, faults. As a consequence it seem sensible to consider some contingency plans, and, some proposals are outlined in this document.

The intention is to find potential R'5/R'6 network solutions rather than to change the R'99 mobile specifications.

2 "Tested" marker in Classmark

This was not accepted at the last RAN plenary.

One basic problem with it is that, even with the "strong type approval" used in GSM phase 1 Full Type Approval, faulty mobiles still appear on the market. Once one type of mobile has a detected fault then, that feature cannot be used with ANY TYPE of mobile. This gives no incentive to mobile makers to develop quality products!

So, this appears to be an unacceptable route forward.

3 Network functionality dependent upon IMEISV

With this concept, the network knows from the TAC, FAC and SVN fields of the IMEISV the features which are faulty in the UE, and, the network adapts its functionality to these faults. (Section 6.2.2 of 23.003 describes the structure of the IMEISV and this is copied into Annex A of this document.)

Although this appears to be a horrible concept, in some regards it might not be many times worse than a GSM BSC being supplied with Half Rate/Full Rate/EFR information by the

GSM MSC. Undoubtedly, the use of this function will reduce RNC performance and so **this shall be regarded as "an escape route" rather than "normal network behaviour".**

In addition, this functionality cannot solve all issues (eg I think that my radio colleagues suggested that the use of Transmit Diversity requires support from ALL mobiles).

Although there has been publicity about the ability to change IMEIs after manufacture, this must not apply to UMTS mobiles because they have to comply to the requirements of 22.016. Regardless of this, modifying TAC and FAC would only lead to the network treating the mobile in a sub-optimal manner, potentially leading to dropped calls etc.

The main issues are (a) how to obtain the IMEISV and (b) how to derive the mobile's capabilities from the IMEISV.

4 Obtaining the IMEISV

4.1 Use Identity Request at IMSI attach and LA/RA update and store IMEISV in VLR and SGSN

For subsequent connections/relocations, the MSC and SGSN send the IMEISV to the RNC in the RANAP Common ID message.

To handle the case of Gs interface and combined attaches, the IMEISV could be added to the BSSAP+-LOCATION-UPDATE-REQUEST message

This procedure assumes that the mobile has sufficient functionality to initiate IMSI Attaches satisfactorily on whatever radio channels the RNC chooses to use!

4.2 USIM reads IMEISV and sends it in an SMS to the HLR

Changes to MAP permit the HLR to sends IMEISV to the VLR/SGSN. SIM/USIM tool kit functionality needs to be checked. The RANAP Common ID message is then reused to send it to the RNC.

However, the coordination of HLR development (in the HPLMN) with RNC/MSC/SGSN development (in the VPLMN) will be problematic.

This appears to be an unnecessarily complex way of doing things.

Despite this, if the SMS was sent across a GSM network, it would remove the dependency on the mobile being able to Attach properly via UMTS. Alternatively O+M could also be used to enter the IMEISV into the HLR: however, this obviously does not support USIMs being transferred into other terminals.

4.3 RRC signalling modified to carry IMEISV directly from UE to RNC

This appears to require changes to R'99 mobiles.

5 How to derive Mobile Capabilities from IMEISV

5.1 Statically Configured O+M information in the RNC

When a relevant fault is found in a particular type of mobile, the RNC's software will need to be patched. As part of this software development, O+M is included so that the impacted TAC/FAC/SVN combination can be loaded into the RNC.

This would appear to be an adequate technique for the short term.

5.2 DNS style lookup from RNC

This would allow the RNC to cache information on the different TAC/FAC/SV combinations. This might require a new interface to the RNC, however, existing O+M interface hardware or Iu-BC or Iu-ps hardware might be reusable.

If 'mobile problems' are expected to exist for the long term, then this solution becomes more attractive.

5.3 Use EIR to convert IMEISV into 'list of known faults'

The existing MAP interface between MSC/SGSN and EIR could be extended so that the EIR returns fault information to the MSC/SGSN. This information would then be both sent to the RNC in a new RANAP message and stored in the VLR/SGSN.

This technique appears to add extra delay and has dependencies on more nodes than 5.1/5.2.

5.4 Use EIR white list to decide to Reject the Attach

This is not really a solution. However it is a technically feasible way to limit network problem caused by faulty mobiles

6 Preferred Solution and Impact on Specifications

Our initial preference (besides requiring correctly functioning mobiles!) is to work on contingency plans based around points 4.1 and 5.1/5.2.

This would require updates to 23.060, 29.018, 25.413 and possibly other RAN specifications.

7 R'99 or R'4 or R'5 or R'6

Network changes such as these appear to be 'phase irrelevant'. However, solely in order to limit the administrative load on MCC, it might be best to incorporate these changes into R'5.

8 Proposal

SA 2 are invited to consider these issues and the preferred solution.

Depending upon the outcome of the discussion, it is suggested that we liaise this concept to RAN 2 and RAN and SA plenaries (with a copy to CN 1). It may also be beneficial to attach a draft work item description.

Annex A
Extract from 23.003 v3.9.0

6.2.2 Composition of IMEISV

The International Mobile station Equipment Identity and Software Version Number (IMEISV) is composed as shown in figure 11.

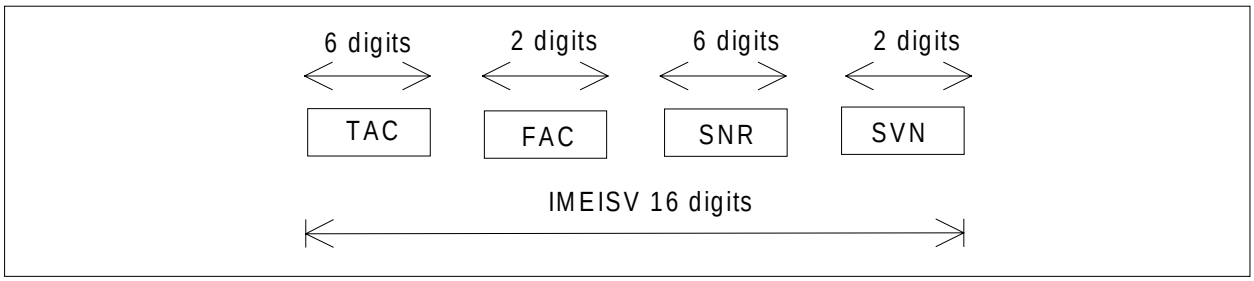

Figure 11: Structure of IMEISV

The IMEISV is composed of the following elements (each element shall consist of decimal digits only):

- Type Approval Code (TAC). Its length is 6 digits;
- Final Assembly Code (FAC) identifies the place of manufacture/final assembly. Its length is 2 digits;
- Serial Number (SNR) is an individual serial number uniquely identifying each equipment within each TAC and FAC. Its length is 6 digits;
- Software Version Number (SVN) identifies the software version number of the mobile equipment. Its length is 2 digits.

Regarding updates of the IMEISV: The security requirements of 3GPP TS GSM 22.016 apply only to the TAC, FAC and SNR, but not to the SVN part of the IMEISV.