3GPP TSG SA WG3 — SA 3 #17 **S3-010044**
Gothenberg, Sweden. 27 Februar-2 March 2001.

Source: **Siemens Atea**

Title: **Problem with no USIM-ME interface in GSM-only ME**

Document for: **Discussion and decision**

Agenda item:

1. Problem setting (Unchanged S3-000682-SA#16)

From various other working groups we have to provide interoperation for a USIM inserted in the following type of ME:

Release 99 ME capable of the UTRAN radio interface
shall support the USIM-ME interface, hence UMTS AKA is executed

Release 99 ME not capable of the UTRAN radio interface
may support the USIM-ME interface, hence GSM AKA is executed

Pre-release 99 ME (not capable of the UTRAN radio interface)
shall not support the USIM-ME interface, hence GSM AKA is executed

The Release 99 VLR/SGSN will initiate UMTS AKA for UMTS subscribers and GSM AKA for GSM subscribers.

When the ME is Release 99 two things may now happen:

The Release 99 ME support UMTS AKA, RAND and AUTN are passed to the USIM, the USIM computes RES (max. 128 bits) and the ME sends **RES (max. 128 bits)** to the VLR/SGSN.

The Release 99 ME does not support UMTS AKA, AUTN is ignored, RAND is passed to the USIM, the USIM computes SRES (32 bits) and the ME sends **SRES (32 bits)** to the VLR/SGSN. This may be the case for R99+ GSM only ME with USIM inserted.

One could have following concern to this (In following paragraph always R99+ VLR/SGSN is meant):

A man-in-the-middle between USIM and VLR/SGSN could take RES and convert SRES by using the conversion function c2 (c2: $SRES_{[GSM]} = XRES^*_1 \text{ xor } XRES^*_2 \text{ xor } XRES^*_3 \text{ xor } XRES^*_4$)

Answer: This is no security threat as will be explained in the following text.

The VLR/SGSN executes following logic for a UMTS-subscriber.

A) SRES-length unequal RES-length: If received RES-length equals to expected UMTS-RES length than compare to UMTS-AV stored value. If received-RES-length equals to expected GSM-SRES length than compare to SRES obtained by executing the conversion function c2 on the stored UMTS-AV. Conclusion: A man-in-the-middle can force that only 32-bits are compared at the VLR/SGSN by using the c2-function. Any other substitute action leads to a failed AKA.

B) RES-length equal to RES-length (32-bit): A man-in-the-middle could not shorten the RES. Executing the conversion-function c2 on SRES gives a RES, which equals SRES.

For both case A and B:

The VLR/SGSN cannot decide upon receiving the RES if UMTS-AKA or GSM-AKA was intended from the USIM. The VLR/SGSN has no means on protocol level to verify this (Initial L3 message content is not appropriate) although the TS 33.102 states that (Clause 6.8.1):

- UMTS AKA shall be applied when the user is attached to a UTRAN.

- UMTS AKA shall be applied when the user is attached to a GSM BSS, in case the user has R99+ ME and also the VLR/SGSN is R99+. In this case, the GSM cipher key Kc is derived from the UMTS cipher/integrity keys CK and IK, by the VLR/SGSN on the network side and by the USIM on the user side.

Avoiding that a man-in-the middle can shorten the RES to 32-bit can only be countered for the UTRAN-Interfaces by forcing on the VLR/SGSN that only UMTS-length RES is allowed for MS connected via UTRAN. For interfaces towards GSM-BSS, both GSM-AKA and UMTS-AKA are allowed, which definitely means that when UMTS subscribers connect via a GSM-RAN, the authentication is as secure as 32-bit authentication which still seems to be acceptable.

---

2. Proposal

It is acceptable that 'In response to a UMTS challenge (i.e., RAND and AUTN) that possibly went over a UTRAN, the VLR/SGSN accepts both RES (max. 128 bits) and SRES (32 bits).'

The following requirement shall be included in TS 33.102 to describe that the VLR/SGSN may receive SRES in stead of expected RES:

"The R99+ VLR/SGSN shall accept authentication if a valid SRES is received in response of a UMTS challenge (RAND, AUTN) over a A or Gb-Interface. This will happen in case a UICC is inserted in a '*R99 GSM only ME that does NOT support USIM-ME interface'* and is attached to a GSM BSS. In this case the R99+ VLR/SGSN uses function c2 to convert RES (from the quintet) to SRES to verify the received SRES".

The following requirement shall be included in TS 33.102 to protect the AKA-procedure from a man-in-middle substituting the RES into SRES over a UTRAN:

"The R99+ VLR/SGSN shall reject authentication if a SRES is received in stead of RES in response of a UMTS challenge (RAND, AUTN) over a Iu-Interface.