3GPP S3 Meeting #17
Gothenberg, Sweden, 27 February – 2 March, 2001

S3-010099

Liaison Statement

From: **S3**

To: **T3, N1, T2**

CC: **S1**

Subject: **TR 31.900 - SIM/USIM Internal and External Interworking Aspects**

Contact: Marc Blommaert, Siemens Atea (Marc.Blommaert@siemens.atea.be)

S3 did receive the T3 liaison Statement (T3-010109), including the technical report TR 31.900 (V0.2.0) on 'SIM/USIM internal and external interworking aspects', and performed an e-mail review on the document.

S3 has spotted following issues where TR 31.900 is inconsistent with the S3 specification TS 33.102 (V3.7.0).

- TR 31.900 describes in section 7.1 the case named 'Shared IMSI & Shared Secret Key'. T3 assumes that the USIM-subscription can be kept in a 2G HLR/AuC. Although technically possible (the so-called 'fixed virtual 2G mode' of the 3G algorithm with input and output characteristics of a 2G algorithm), this has never been the assumption of S3. The TS 33.102 does currently not include interworking descriptions for USIM subscription kept in a 2G HLR/AuC.

- Keeping a USIM-subscription in a 2G HLR/AuC, and executing the scenario "F" as described in case 5 of section 6.1 (3G ME and UICC), leads to executing 2G AKA over a UTRAN for a UMTS subscriber. But this is explicitly forbidden in TS 33.102.

  > Section 6.8.1.1 of TS 33.102: '*For UMTS subscribers, authentication and key agreement will be performed as follows: UMTS AKA shall be applied when the user is attached to a UTRAN.*'
  >
  > Section 6.8.1.4 of TS 33.102: '*R99+ ME with a USIM inserted and attached to a UTRAN shall only participate in UMTS AKA and shall not participate in GSM AKA.*'

  This means that 3G ME, which are implemented according to the 3GPP Technical Specifications, can not execute this scenario. Allowing this scenario opens the door for false base station attacks. S3 is not willing to remove current security requirements for permitting scenario "F". S3 asks T2, N1 to check that the 3G ME forbids this scenario: 3G ME accepts only (RAND,AUTN) from UTRAN in case USIM-application is active and not RAND alone.

- Keeping a USIM-subscription in a 2G HLR/AuC, and executing the scenario "E" as described in case 4 of section 6.1 (3G ME and UICC), leads to executing 2G AKA over a GSM BSS for a UMTS subscriber. TS 33.102 has following requirement (Section 6.8.1.1): '*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.'*

- From the Mobile Equipment seen (TS 33.102 section 6.8.1.4) this scenario is possible: *'R99+ ME with a USIM inserted and attached to a GSM BSS shall participate in UMTS AKA and may participate in GSM AKA . Participation in GSM AKA is required to allow registration in a R98- VLR/SGSN'.*
- From the VLR/SGSN seen (TS 33.102 section 6.8.1.3) this scenario can not be prevented: '*When the user has R99+ ME, UMTS AKA shall be performed using a quintet….* '. The problem is here that the VLR/SGSN has obtained triplets from the 2G HLR/AuC.

Conclusion: 3G VLR/SGSN and 3G ME cannot prevent scenario "E" from being executed, S3 points out that any scenario due to keeping a USIM-subscription in a 2G HLR/AuC implies that this particular 2G HLR/AuC has implemented a new A3/A8 algorithm based on 3G algorithms + conversion functions.

Also it is difficult to see any business requirements for having a USIM subscription in a 2G HLR/AuC, at least S3 did not receive any service requirement for it in the past, and therefore it is not part of the security architecture, although S3 sees no additional security risks in it compared to scenario 'C'.