3GPP TSG SA WG3 Security — S3#22 **S3-020038**

25 - 28 February 2002

Bristol, UK

3GPP TSG SA WG1 — UE split SWG **S1-020300**

13 January 2002, Phoenix, USA

From: **SA1**

To: **SA3**

CC: **SA2, T2, CN1, GERAN**

Title: **IMS Security requirements**

Contact: **Mark Watson**
mwatson@nortelnetworks.com

Phone: +44 1628 434456

---

1. Overall Description:

SA1 thanks SA3 for their liaison S3-010703 on UE Functional Split.

SA3's assumptions

SA1 has discussed the SA3 assumptions communicated in that liaison and in particular the assumption that no forms of Call Control will reside in the TE.

SA1 sees no issues with having CS and PS domain call control and mobility management procedures residing in the MT, and therefore all security procedures associated with these terminating in the MT.

Also, in Release 5, the MT has a UICC on which the USIM and/or the ISIM reside.

SA1 has further considered the location of the procedures relating to the IMS with respect to the impact on the user. SA1 sees that the user may be interested in devices where a TE and MT are integrated, based on an open operating system, where potentially malicious software could be wittingly or unwittingly loaded which impacts the operation of the IMS procedures. SA1 also sees that the users may be interested in separate devices where the IMS Client is a user-installable software element, whether running on the TE, or as an application within a standard OS environment on an integrated UE (e.g. PDA).

This possibility raises two distinct areas of study:

- Requirements on the IMS network elements to be secure against attacks resulting from this arrangement, and in particular the possibility of a maliciously modified or faulty IMS Client.
- Security requirements on the TE/MT interface for this arrangement

SA1 has doubts that standardisation of the TE/MT interface for this arrangement will be completed in Release 5, and hence the second area of study is less urgent.

However, SA1 believes that such arrangement may exist in Release 5 timeframes (either on integrated PDAs or with proprietary TE/MT interfaces) and when standardised in Release 6, it should be possible to connect such terminals to Release 5 networks. Therefore SA1 believes that it is important for Release 5 that the first of the above items is understood and mechanisms to meet these requirements completed in Release 5.

We therefore request SA3 to ensure that the security requirements for the IMS network arising from this are completed and met in Release 5

Questions to SA1 regarding S1-011246:

Question from SA3: Is stage 2 and stage 3 work on UE functional split for Rel 5 or Rel 6? (The current 3GPP workplan (version 011011) lists this Feature as Rel 6, but the LS from S1 seems to suggest that it is Rel 5.)

Answer from SA1: It is expected that Stage 2 and Stage 3 work will be included in Release 5 for certain scenarios.

Question from SA3: Section 6.3.2 bullet point 11 (Access services and capabilities provided by the MT is a TE function) created some prolonged discussion. What precisely does it mean?

Answer from SA1: This text has been clarified. It represented only the fact that the TE includes functions, which allow it to request services from the MT. The exact set of services to which the TE has access is ffs.

Question from SA3: To what extent is access independence addressed in S1-011246? Can a MT only access GERAN and UTRAN, or may it also comprise the functionality of a WLAN station?

Answer from SA1: Access Independence for IMS does not imply that the MT should support multiple accesses, however there are benefits to be gained from avoiding that the IMS procedures should make access-specific assumptions.

Plans for SA3 work on UE functional split

SA3 made a number of proposals as to how to proceed based on their assumptions. Given the comments above, SA1 would modify those proposals as follows:

1) No need is seen to modify the security procedures involving network entities specified in TS 33.102 for the CS and PS domains.
2) Security procedures for the IMS (e.g. in TS 33.203) shall ensure that the network is secure against attacks from software IMS clients, which could be maliciously modified.
3) A section “security for the local interface between the TE and the MT in UE functional split scenarios” would be added to TS 33.102. In this section, it would be pointed out what security features are required on this local interface. Security mechanisms would not be specified as they would depend on the particular nature of this interface. The new section would also not attempt to assess security mechanisms available for technologies, which may be used to realise this interface (e.g. Bluetooth, Wireless LAN). Given that the deadline for Rel 5 is very close even that goal is very ambitious, and as there have been no contributions on this subject in SA3 so far, it is not certain that it can be achieved.
4) Any work on the security aspects of UE functional split scenarios which goes beyond the work described in 2) and 3) is considered infeasible for Rel 5.

2. Actions:

SA3 are requested to address the security concerns arising from the possible existence of software IMS clients, which may be subject to malicious modification, independently of whether these clients exist in the TE or the MT or an integrated UE.

SA2 and CN1 should expect to receive requirements from SA3 on this matter.

3. Date of Next SA1 Meetings:

Title	Date	Location	Country
SA1#15	11 – 15 Feb 02	Saalfelden	Austria
SA1 SWGs	8 – 12 Apr 02	Sophia Antipolis	France
SA1#16	13 – 17 May 02	Victoria	Canada
SA1 SWGs	8 – 12 Jul 02		Italy
SA1#17	12 – 16 Aug 02	Durango	United States
SA1 SWGs	14 - 18 Oct 02		Taiwan
SA1#18	11-15 Nov 02		Korea