

**3GPP TSG-SA WG2 Meeting #43**  
**Seoul, Korea, 15<sup>th</sup> – 19<sup>th</sup> November 2004.**

**S2-043846**

**Title:** LS on Security Aspects of Early IMS Systems  
**Response to:** LS (S3-040880) on Security Aspects of Early IMS systems  
**Release:** Rel-6

**Source:** SA2  
**To:** SA3  
**Cc:** CN1, CN3, CN4

**Contact Person:**

**Name:** Krister Boman  
**Tel. Number:** +4631 747 4055  
**E-mail Address:** krister.boman@ericsson.com

**Attachments:**

---

**1. Overall Description:**

SA2 would like to thank SA3 for sending the draft TR 33.878 on security aspects for early IMS.

SA2 expects that the issues related to early IMS Security can be resolved without affecting SA2 specifications although it is not possible to give such a confirmation at this stage.

SA2 has reviewed the TR 33.878 and would like SA3 to take the following aspects into consideration.

- SA2 is not aware of a definition of an authenticated PDP context and how such a definition can be used for differentiating different PDP contexts from each other
- It is mentioned that a GGSN shall send information to the HSS. SA2 understands that SA3 envision that the GGSN shall send information to a Radius Server over Gi interface. Note that TS 23.060 do define a MAP based interface between a GGSN and the HLR. SA2 asks SA3 to make the specification clear on this topic assuming that SA3 has no intention to use the interface defined in TS 23.060.
- SA2 noted that the TR is using the term IMS PDP context. It was not clear from the TR if SA3 assumes the use of a signalling PDP context or the use of a specific IMS APN. However SA2 is of the opinion that the architecture needs to allow for the case where a PDP context may be used for both IMS as well as non-IMS based services. It is also noted that the use of a signalling flag is optional both from a network as well as a UE point of view as described in TS 23.228v670.
- SA2 would like to note that in a general context a UE might have multiple IP Addresses even for the case when only one APN is used. The TR 33.878v030 seems to only consider the case when the UE has only one IP Address
- SA2 notes that SA3 refers to an idle timer in the GGSN such that the GGSN sends an Accounting Stop Request towards the Radius server when a PDP context is deleted and after the timer has expired (order of hours). SA2 were uncertain about the purpose of this idle timer and suggest that this timer is removed from the TR.
- SA2 asks SA3 to avoid a requirement that the GGSN under certain situations shall log certain events. SA2 suggests that it is more feasible to require that it shall be possible to log certain events e.g. based on operator configuration.
- The TR suggests that the HSS shall be able to control that a PDP context is not activated for certain events. However this may lead to that a PDP context that could be used for non-IMS based services is terminated. SA2 failed to identify why this is needed from a security point of view for Early IMS Security.

**2. Actions:**

**To SA3 group.**

**ACTION:** SA2 asks SA3 to consider the aspects above when further progressing the TR in SA3. SA2 would also like to know what the security reasons are to introduce a requirement that HSS shall be able to control the PDP context activation procedure in the GGSN.

**3. Date of Next TSG-SA2 Meetings:**

<u>3GPPSA2#44</u>	26 Jan - 2 Feb 2005	tbd	EU
<u>3GPPSA2#45</u>	4 - 8 Apr 2005	tbd	China