3GPP TSG-SA WG3 Meeting #36 **Tdoc S3-041068**
Shenzhen, China, 23-26 November 2004.

Title:	**[DRAFT]** LS on impacts of early IMS security mechanisms
Response to:	LS (S2-043846) on Security Aspects of Early IMS Systems from SA2
Release:	Rel-6
Work Item:	early IMS security
Source:	SA3
To:	SA2
Cc:	CN1, CN3, CN4

Contact Person:
Name: Peter Howard
Tel. Number: +44 1635 676206
E-mail Address: peter.howard@vodafone.com

Attachments: S3-041091 [Draft TS 33.878 v0.0.4].

---

1. Overall Description:

SA3 thanks SA2 for its LS on early IMS security and informs SA2 that all the points raised in the LS have been taken into consideration when creating TR 33.878v0.0.4, which SA3 has agreed to send to SA plenary for approval. The points have been addressed by SA3 as follows:

- *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*

SA3 response: It has been clarified in the TR that it is the IMSI, not the PDP context, which is authenticated. The term "authenticated PDP context" is no longer used in the TR. See section 6.1 of TR 33.878.

- *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.*

SA3 response: It has been clarified in the TR that the Gi interface is used by the GGSN to send information to the Radius Server associated with the HSS. See section 6.1 of TR 33.878.

- *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.*

SA3 response: It has been clarified in the TR that an APN used for IMS signalling may also be used for non-IMS services. The term "IMS PDP context" is no longer used in the TR. See section 6.1 of TR 33.878.

- *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*

SA3 response: It has been clarified in the TR that there is only one APN for accessing IMS for a PLMN and that all active PDP contexts, for a single UE, associated with that IMS APN use the same IP address at any given time. SA3 believe that it is an acceptable limitation that the early IMS security solution does not support multiple IP addresses per UE. See section 6.1 of TR 33.878.

- *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.

SA3 response: SA3 would like to clarify to SA2 that the idle timer mentioned in TR 33.878v0.0.3 refers to a GGSN internal timer which measures the length of time that a PDP context remains inactive and deletes the PDP context after a given period of inactivity. It is stressed that the intention of SA3 is that the accounting stop request is sent immediately after the PDP context is deleted. SA3 has clarified the GGSN-HSS interactions in TR 33.878 and, as a consequence, the reference to idle timers has been removed. See section 7.2.1 of TR 33.878.

- *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.*

SA3 response: SA3 agrees that the logging of events in the GGSN should not to be mandated and has modified the TR according to SA2's suggestion. See section 6.2.2 of TR 33.878.

- *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.*

SA3 response: SA3 would like to clarify that it is not the intention of the TR that the HSS shall be able to terminate PDP contexts. Instead, the HSS is used to store the IP address and associated identities provided by the GGSN, so that this information can be used by the S-CSCF to perform checks during SIP registration. Accordingly, SA3 does not believe that any situation would arise from the early IMS solution which would lead to the HSS terminating a PDP context that is used for IMS or non-IMS services. SA3 does acknowledge that the lack of a positive response to an Accounting Request Start at the GGSN would result in the inability to successfully create a new PDP context associated with an APN that may be used for IMS, and that such an APN may also be used for non-IMS services. Relating to this, SA3 has updated the TR to ensure that failures in the IMS domain have a minimal impact on non-IMS services, in the case that those non-IMS services use the same APN as the IMS services. See section 6.2.1 of TR 33.878.

2. Actions:

To SA2 group.

ACTION: SA3 asks SA2 to take note of the above information.

3. Date of Next TSG-SA WG3 Meetings:

TSG-SA WG3 Meeting #37 21-25 February 2005 Sophia Antipolis, France.