3GPP TSG SA WG3 Security ó SA3#36 **S3-041132**
November 23-26, 2004
Shenzhen, China

Source: **SA WG3**

Title: **Issue list to complete MBMS Security**

Document for: **Discussion and Proposal**

Agenda Item: **7.3.2: SA WG3 Reporting**

This contribution lists the issues, which need to be resolved to complete MBMS security. The list may not be exhaustive. It is proposed that this list is taken as a basis of discussion when deciding if Release 6 MBMS TS 33.246 should be frozen in SA plenary in December 2004.

An issue list to complete MBMS is presented below. It should be noted that some of the issues marked to be checked may generate standardisation work whose amount cannot be estimated at the moment.

Service announcement/discovery		
Issue	**Type of work needed**	**Estimated completion time**
Protection of Service Announcement over MBMS bearer has not been considered. SA3 is currently assuming, that service announcement is only send via point-to-point bearers, see Threats in B.1 of TS 33.246. However, SA4 TS includes possibility to send Service Announcement over MBMS bearer.	Functional	SA plenary March 2005 ?
Confidentiality and integrity protection is indicated today in Service Announcement. It needs to be specified if key management is initiated at all if both confidentiality and integrity protection are turned off.	Functional	SA plenary March 2005
GBA bootstrapping		
GBA bootstrapping initiation request and bootstrapping renegotiation request have not been defined for MBMS application	Functional	SA plenary March 2005
The MBMS security architecture is incompletely described	Editorial	SA plenary March 2005
HTTP procedures		
The contents of HTTP payloads need to be specified	Functional	SA plenary March 2005
Mutual cross check of SA4 and SA3 seems necessary due to large amount of changes that will be presented by both groups to SA plenary	Check	SA plenary March 2005 ?
SA3 has not defined any mechanism for the UE to leave from the key management service	Functional	SA plenary March 2005
Final decision on the need for SA4 application level joining depends on decision of SA4	Check	SA plenary March 2005
The protection of post delivery procedures depends on decisions of SA4. SA3 may need to analyse the impacts of MSK transport within post delivery procedures. The handling of MSKs may need some enhancement to cover download	Functional	SA plenary March 2005 ?

services, where the MSK is fetched after the UE has received the encrypted data		
Possible error cases in HTTP procedures	Functional	SA plenary March 2005
MIKEY procedures		
Possible need for Security policy payload for download	Check	SA plenary March 2005
Possible error cases in MIKEY procedures	Functional	SA plenary March 2005
Completion of IETF activities for MBMS related MIKEY extensions	Check	SA plenary March 2005 ?
Traffic protection		
Details of download protection method	Functional	SA plenary March 2005
Completion of OMA activities for MBMS download protection	Check	SA plenary March 2005 ?
Other		
Consistency check security threats ñ> requirements -> functions -> mechanisms	Check	SA plenary March 2005
Editorial check	Check	SA plenary March 2005