3GPP TSG SA WG3 Security — S3#34 **S3-040461**
July 6 - 9, 2004
Acapulco, Mexico

3GPP TSG SA WG4 Codec — S4#31 S4-040322
17 - 21 May 2004
Montréal, Canada

Title: Reply LS on MBMS security issues
Response to: S4-040329 (S3-040443), S4-040330 (S3-040444)
Work Item: MBMS

Source: SA4
To: SA3
Cc: Download + DRM of the OMA, SA2

Contact Person:
Name: Sami Pippuri
Tel. Number: +358 50 487 6829
E-mail Address: sami.pippuri@nokia.com

1. Overall Description:

SA4 would like to thank SA3 for the productive collaboration and information exchange. SA4 has discussed the liaisons sent from SA3 to the SA4 Montréal meeting and with this LS SA4 reply to documents S4-040329 (S3-040443) and S4-040330 (S3-040444).

Actions for SA4 in S4-040329 were:

- SA3 would like to ask SA4 to comment on the suitability and feasibility of using SRTP (RFC 3711) for protecting MBMS streaming data from SA4 point of view
  - SA4 have no technical issues with the adoption of SRTP. SA4 have already adopted SRTP as optional for integrity protection purposes.
  - SA4 have a requirement for pre-encrypted content and have a separate mechanism for confidentiality protection using OMA DRM.
  - SA4 would like to inform SA3 that there are also other solutions available.
  - SA4 believe that the final decision should be made by SA3.
  - SA4 assumes that the usage of confidentiality protection would also be optional.
- SA3 would like to ask SA4 to comment on the suitability and feasibility of using S/MIME (RFC 2633) without PKI for protecting MBMS download data from SA4 point of view
  - SA4 assumes that the data transport equates to MBMS bearer service and that the multicast transmission equates to MBMS user service.
  - SA4 would like to inform SA3 that in the MBMS download delivery method, it is only possible to indicate the MIME type of separate objects in the download session. This is not possible for the entire download session (which may consist of several objects).
- SA3 would like to propose a joint meeting with SA4 to get a common understanding and progress the MBMS work. SA3 would like to ask SA4 to propose date and venue for the meeting
  - SA4 need some more time to form a common SA4 view on MBMS security issues, and is considering an ad-hoc meeting after the next SA4 meeting (16 - 20 Aug 2004).
  - As a possible date, 23rd August (week after SA4#32) is being considered, venue to be confirmed.
  - The presence of SA3 delegates interested in the subject would be welcomed.

Action for SA4 in SA4-040330 (LS on MBMS MSK key update):

- SA4 are kindly asked to comment on the solutions or to suggest an alternative solution.
  - SA4 have discussed this issue but have not come to a conclusion yet.
  - SA4 sees that there may be similarities with the PTP repair and reception reporting requirements that are currently under discussion in SA4.

2. Actions

Actions to SA3:

- SA4 would like to ask SA3 delegates interested in the topic to join the SA4 ad-hoc meeting, possibly 23rd August (to be confirmed).

3. Dates of Next SA4 Meetings:

SA4#32	16 - 20 August 2004	TBD
SA4#33	22 - 26 November 2004	Helsinki, Finland