3GPP TSG SA WG3 Security — S3#30 **S3-030650**
7 - 10 October 2003
Povoa de Varzim, Portugal

Title:	Reply LS on cipher suite for DRM-protected streamed media for PSS
Response to:	S4-030647 / S4-030660
Release:	Rel-6
Work Item:	Packet Switched Streaming Services Rel-6
Source:	SA3
To:	OMA-SEC, OMA-DRM+DL, 3GPP SA4
Cc:	

Contact Person:

Name: **Peter Howard**
Tel. Number: +44 7787 154058
E-mail Address: peter.howard@vodafone.com

Attachments:

1. Overall Description:

SA3 has considered the LS from SA4 on the division of work between OMA and 3GPP on DRM protected content (S4-030647). SA3 has also handled another LS from SA4 which asks SA3 to consider whether AES Counter Mode with 128 bit key length is acceptable for encrypting media delivered over RTP (S4-030660).

SA3 would like to confirm that it has the responsibility to endorse any DRM-related security mechanisms that are included in SA4 specifications. However, in order to endorse specific proposals, such as the use of AES counter mode for encryption, SA3 needs to understand the context in which those security mechanisms are used. Therefore SA3 would like to request that SA4 and OMA continue to provide SA3 with the necessary background information (e.g. security goals and requirements) to support any DRM-related security mechanisms that are proposed to be included in SA4 specifications. Furthermore, SA3 would like to request that security-related contributions on DRM protected content are presented directly to SA3 as necessary to ensure that any forthcoming proposals to develop the 3GPP specifications can be approved in a timely fashion.

SA3 would like to highlight that it is working on a security mechanism for the 3GPP Multimedia Broadcast/Multicast Service (MBMS) and on support for subscriber certificates. It would be advantageous to consider potential overlap between our solutions and the work undertaken by OMA DRM+DL and OMA security groups. In particular, SA3 is considering solutions for the encryption and integrity protection of MBMS streaming media and it would be advantageous to consider alignment of these solutions (and the associated requirements) with the encryption and integrity protection mechanisms for DRM.

To help progress and co-ordinate the security work between OMA and 3GPP, SA3 would like to suggest that this topic is added to the agenda of the proposed joint meeting between SA3 and the OMA security group.

2. Actions:

To SA4 and OMA group

- provide SA3 with the necessary background information (e.g. security goals and requirements) to support any DRM-related security mechanisms that are proposed to be included in 3GPP specifications

3. Dates of Next SA3 Meetings:

SA3 Meeting #31	18-21 November 2003	Munich, Germany.
SA3 Meeting #32	10-13 February 2004	Location TBD
SA3 Meeting #33	11-14 May 2004	Location TBD