3GPP TSG SA WG3 Security — S3#32 **S3-040008**
09 - 13 February 2004
Edinburgh, Scotland, UK

ETSI SAGE **SAGE (03) 03**

22 December 2003

Title:	Response on protection of MBMS and DRM Streaming Services
Response to:	LS S3-030805 "LS on Protection of MBMS and DRM Streaming Services"
Source:	ETSI SAGE
To:	3GPP SA3
Cc:	SA4, OMA DLDRM

Contact Person:
Name: **Steve Babbage**
Tel. Number: + 44 1635 676209
E-mail Address: steve.babbage@vodafone.com

Attachments: None

Introduction

In LS S3-030805, SA3 have asked SAGE to:

- review the AES CTR mode proposals from a cryptographic point of view and comment on its suitability for protecting content;
- if possible comment on the selective encryption mechanism in particular considering the references to research papers in S3-030750.

Comments

SAGE's comments are as follows, although we do not expect that any of them will be new to SA3:

- The suitability of AES CTR mode for protecting content depends, of course, on what you mean by "protecting content". AES-CTR is a perfectly good encryption algorithm, subject to the obvious requirement to ensure that IVs are never re-used. AES-CTR provides no integrity protection.
- The selective encryption mechanism seems adequate for the DRM-specific requirement, which is essentially that someone without the key should not be able to reconstruct the streamed content with a sufficiently high quality for them to be able to redistribute it to other customers.
- We have not attempted to reproduce or validate the research quoted in S3-030750, but we find it perfectly plausible that an eavesdropper may be able to deduce some information about the nature of the content from the unciphered frames. So, if SA3 have identified a requirement for full confidentiality about the content being downloaded by a particular customer, then selective encryption will not satisfy that requirement — additional protection (on this or another layer) will be required.
- It is clearly true that selective encryption without an additional integrity protection mechanism does not prevent an active interceptor from modifying the content. In fact, even if there were integrity protection on the frame encryption flag (but not on the payload), an attacker who knew the plaintext corresponding to a given enciphered frame could substitute a frame that would decrypt to a frame of the attacker's choice (this is because a stream cipher mode of encryption is being used). So, if SA3 have identified a requirement to prevent modification of the content, then the OMA DLDRM mechanism will not satisfy that requirement — additional protection (on this or another layer) will be required.