Doc# OMA-BAC-DLDRM-2003-0221R3-liaison-to-3GPP-SA4-and-SA3
Originated by OMA Download+DRM
30 October 2003

3GPP TSG SA WG3 Security — S3#31 **S3-030758**
18 - 21 November 2003
Munich, Germany

LIAISON STATEMENT

Title:	Liaison to 3GPP SA4 and SA3 on issues on DRM for PSS and MBMS streams
To:	3GPP SA4 and 3GPP SA3
Cc:	3GPP2 S4
Response to:	3GPP S4-030647 (Liaison Response to OMA)
Source:	Download+DRM group of the Open Mobile Alliance
Contact(s):	Frank Hartung, Ericsson +49 2407 575389 Frank.Hartung@ericsson.com
Attachments:	n/a

1 Overview

This liaison statement (LS) is sent from Open Mobile Alliance Download+DRM group (OMA DLDRM) to 3GPP SA4 and SA3 in reply to liaison statements

- S4-030647 “Liaison Response to OMA”, which was sent from SA4 in response to LS OMA-MAG-DLDRM-2003-0172R1-liaison-to-3GPP-SA4/S4-030626, which was sent in response to the two liaison statements S4-030510 and S4-030552
- S3-030650 “Reply LS on cipher suite for DRM-protected streamed media for PSS”, which was sent from SA3 in response to S4-030647 and S4-030660

It informs 3GPP SA4 and SA3 about

- a recommendation for the choice of a stream cipher for continuous PSS media
- Considerations on stream integrity protection for continuous PSS media
- the DRM information to be conveyed to a terminal
- a request from OMA DLDRM to provide a version of TS 26.244 that can be normatively referenced, by January 2004
- a request to SA4 to include signalling of DRM support for PSS clients into the 3GPP PSS UAProf vocabulary
- a request to SA3 for information on the requirements and solutions for protection of MBMS streams

2 Proposal

OMA DLDRM thanks 3GPP SA4 for the ongoing good cooperation and information exchange, and in particular for the recent liaison statement S4-030647.

The following two issues have been raised by you in this LS:

- *"The actual choice of cipher suite (encryption transform) would not be handled by SA4 in 3GPP. Security related work is done in SA3 and it is our understanding that they will decide on the choice of cipher. We will confirm with SA3 that this understanding is correct. If OMA feels that, since OMA has already defined such a transform for static files, it is in OMA's area for real-time content also, we would welcome clarification to us and SA3."*

  DLDRM has discussed the issue and recommends to use AES in Counter Mode with 128 bit key as the encryption transform. The choice of AES in CM being a stream cipher and in addition the case of selective encryption means that the stream is not robustly integrity protected. The integrity protection of the stream is not a DRM requirement as such, and therefore not a DLDRM requirement, but may be a requirement from the perspectives of other services. SA3 should therefore consider itself it if wishes to specify a message authentication transform or other method of integrity protection. We would like to point out that these are recommendations and that the adoption of these recommendations is at the discretion of 3GPP.

- *"We understand that the DRM information conveyed to the terminal needs to describe the encryption transform and its parameters. However, we expect that it may also need to convey to the terminal information about the interface to the areas that OMA is handling, specifically a reference to where the rights etc. may be obtained. We will proceed with the assumption that at most a URL is needed for this purpose, unless you have further information."*

  The DRM information stored in 3GP files and conveyed to terminals should be compatible with the DRM information defined by OMA DLDRM. This includes, as you proposed, a rights issuer URL, but also other information. DLDRM has not yet finalized the corresponding part of the DRM 2.0 specification. We believe at the current stage it would be sufficient if SA4 reserves a box in the file format that can be used to store OMA DRM information, and complete the specification as soon as OMA DLDRM can provide the final specification of the DRM information to be stored and transported. The following example type definition of a header box shall clarify the concept.

```
aligned(8) class OMADRMHeaders extends Box('ohdr'){
        bit(8) content_type_length; // fixed headers for performance reasons,
        bit(8) content_id_length;          // following v1 syntax
        char content_type[content_type_length];
        char content_id[content_id_length];
        string headers[ ]; // rest of the headers, like rights issuer URL, to the end of the box
}
```

Further, we would like to discuss the following issues with SA4:

- We informed you earlier that DLDRM intends to adopt the 3GP file format defined by SA4. However, we are not able to do this if the 3GP file format specification is not in a state where it can be normatively referenced at the time we will freeze our DRM specification, which is anticipated to be done latest in the February 2004 meeting. We would therefore like to ask whether SA4 will be able to produce, in or around January 2004, a version of the Rel6 3GPP file format specification (TS 26.244 Rel6) that can be normatively referenced in the DRM 2.0 specification.

- It will be necessary for PSS clients to signal whether they support DRM protection for streams. Options would e.g. be to signal that as a subset of the OMA DRM UAProf signalling, or as a subset of the 3GPP PSS UAProf signalling. OMA DLDRM would prefer if DRM support of PSS clients would be signalled in the PSS UAProf signalling. Thus, we would like to ask SA4 for confirmation that SA4 will include that into their UAProf vocabulary.

OMA DLDRM thanks 3GPP SA3 for the ongoing good cooperation and information exchange, and in particular for the recent liaison statement S3-030650.

The following issues have been raised by you in this LS:

- *"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."*

  OMA DLDRM acknowledges that SA3 is the final authority on all DRM-related security mechanisms that are included in SA4 specifications, and intends to send / copy all further DRM related communication to SA3.

- *"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."*

  OMA DLDRM wants to ensure that OMA DRM 2.0 is applicable to as many services as possible, and is interested in solutions for streaming media that are applicable for unicast (3GPP PSS services) and multicast (3GPP MBMS streaming services). DLDRM would like to receive more information on how this interoperability could be achieved and how the solutions and requirements can be aligned.

- *"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."*

  OMA DLDRM noted this proposal.

On a side note, OMA DLDRM would like to inform SA3 and SA4 that OMA MAG has changed its name to OMA BAC ("Browser and Content"), and that OMA DLDRM has changed its full name to OMA BAC DLDRM ("Browser and Content – Download and DRM"), for short still OMA DLDRM.

3 Requested Action(s)

We kindly request 3GPP SA4 and SA3 to note the information contained in this LS, and to reply in case there are questions or comments. We would welcome a reply from SA4 on the issue of a version of TS 26.244 that can be referenced in January 2004., and from SA3 on the requirements and solutions for protection of MBMS streams.

The next known OMA DLDRM meeting dates are:

OMA plenary, 10-14 November 2003, London (UK)

OMA plenary, 1-6 February 2004, Los Angeles (USA)

Also, we are holding weekly telephone conferences.

4 Conclusion

We thank 3GPP SA4 for the good and continued cooperation and information exchange. With this LS we reply to the recent LS S4-030647. We suggest the use of AES 128 CTR as stream cipher, and the optional use of stream integrity protection. We also ask SA4 to reserve space in the 3GP file format to store DRM information, although we cannot yet provide a complete list of the DRM information to be considered. We further ask SA4 whether it would be possible to publish TS 26.244 in January 2004, so that DLDRM can reference it in the DRM 2.0 spec and adopt the 3GP file format. We ask SA3 for information on the requirements and solutions for protection of MBMS streams.

With best regards, OMA Download+DRM group