3GPP TSG SA WG3 Security — S3#28 **S3-030268**
6 - 9 May 2003
Berlin, Germany

LIAISON ON DRM CONTENT FORMAT STATEMENT

Title:	Liaison On DRM Content Format Statement
To:	3GPP SA4
Copy:	3GPP SA3
Response to:	n/a
Source:	MAG Download+DRM of the Open Mobile Alliance
Contact(s):	Josh Hug, Realnetworks Frank Hartung, Ericsson Bart van Rijnsoever, Philips Sami Pippuri, Nokia
Attachments:	Arch doc

1 Overview

OMA has released a first set of DRM specifications: OMA Digital Rights Management version 1.0, downloadable from http://www.openmobilealliance.org/documents.asp. Version 1.0 specifies a basic DRM system for content downloading to mobile phones. It also enables secure superdistribution of content between mobile phones. The scope of version 1.0 is for example ring tones and logos.

OMA MAG Download+DRM working group is developing the next version of the DRM specification that will be use full for valuable rich media content. The group is currently finalising the requirements specification for the next version. We are already in the process of the next step of developing the actual technical specifications.

Content format is a key point of required interoperability in any DRM system. In order to create a more flexible and interoperable format, OMA DRM+DL desires to work with the 3GPP SA4 working group. We would like to leverage the format standardization process already working with-in 3GPP. In this liaison we want to explicitly call out the OMA DRM+DL group's requirements for its version 2 content packetized media format.

We desire that the content format specified would enable both download and streaming. OMA's requirements for a defined encrypted format are complementary to the current work items with-in 3GPP SA4. We would like to propose creation of an encrypted content profile. This should include specification of suitable transport, signalling mechanism, and physical file layout. Ideally this profile will define a format that works for both download and streaming of packetized PSS content.

2 Proposal

1 General requirements 2
2 Use Cases 2
2.1 Download of protected PSS content 2
2.2 Streaming of protected PSS content 2
2.2.1 SDP delivery from content provider to device 3
2.2.2 RTSP URL pointing to content 3
2.2.3 RTSP URLs in SMIL file 3
3 Requirements on 3GP file format 3
3.1 Download 3gp file structure 3
3.2 Payload Security Requirements 3
4 Requirements on real-time transport of PSS streams and associated signaling 4
4.1 Requirements on Session Signaling 4
4.1.1 Requirements on Session Description Protocol 4

Note1: The DRM protection of discrete PSS media (e.g., images) is already covered by the OMA DRM v1 and upcoming OMA DRM v2 specifications.

1 General requirements

OMA DLDRM would like to cooperate with 3GPP SA4 in the definition of components that allow the DRM protection of streamed PSS content in accordance with the OMA DRM v2 and 3GPP PSS Rel6 standards. In order for the two standards to interwork, coordination in both specifications are necessary. OMA DLDRM has defined requirements for the coordination that would be necessary in the PSS specs to allow DRM protection of PSS streams. DLDRM kindly requests to SA4 to consider those requirements in the definition of the Rel6 PSS specification.

In general we would like to enable the same use cases for protected content that the 3GPP has defined for non-protected content.

2 Use Cases

For an introduction to the terminology, architecture and components of OMA DRM , we refer to [Arch].

The actors and functional entities, functional architecture and technical use cases in a DRM content distribution scenario are outlined in Chapter 4 of [Arch]. The description of streaming of protected content (currently Section 4.3.3) is under development though the high level content distribution scenario as outlined in Section 4.2 is still valid. In particular there are different trust models on the content delivery side depending on whether the Content Issuer is applying DRM protection of the content or just distributing content pre-packed by content owner or other party.

In general the security of content and rights depend on several parties, an outline is given in Chapter 5 of [Arch]. The cryptographic key(s) necessary for decrypting the content and checking integrity of the rights must be accessible only for authorised DRM agents. Key management is done by means of Rights Objects secured end-to-end from Rights Issuers to DRM agents in dedicated devices using a OMA DRM specified Public Key Infrastructure (PKI).

The following use cases assume the device will examine the OMA DRM headers. The device will then determine if rights exist to consume the content. If no rights exist the Rights Issuer URL can be used by the device to request Rights Objects. When rights are present, the device should be able to use the key provided in the rights object to decrypt the content.

2.1 Download of protected PSS content

A user receives an OMA DRM media file via any method of download (e.g. http). The device will recognize the content as protected content. Further examination reveals OMA DRM was used to package the content and the preserved standard media information.

2.2 Streaming of protected PSS content

It is desirable to enable the delivery of OMA DRM content under the same use cases defined for PSS with-in the 3GPP SA4 group. [26-233]

DRM protection should not directly affect the streaming user experience. Users will still initiate and interact with streams the same way.

Certain DRM specific headers need to be delivered for streaming content along with codec information in the stream initialisation. The use cases should be the same though.

2.2.1 SDP delivery from content provider to device

Delivery of SDP file to client (e.g., by download from a content portal). A content distributor should be able to create and distribute an SDP file. This SDP file should contain the following information:

- This is OMA DRM content (e.g. a new mime-type)
- Codec and payload format originally encrypted (e.g. mime-type or RTP profile).
- DRM specific headers as specified in section 3.1.

2.2.2 RTSP URL pointing to content

SDP delivered to client in DESCRIBE part of RTSP session. The SDP should contain the same DRM properties as contained when an SDP file is delivered from content provider to device directly.

2.2.3 RTSP URLs in SMIL file

SMIL file contains RTSP URLs (it may also contain links to discrete objects like images). SDP is delivered via the DESCRIBE RTSP message when the SMIL player establishes the PSS session.

3 Requirements on 3GP file format

3.1 Download 3gp file structure

- New file branding (file type magic number)
- New codec type, so any DRM-aware 3gp player will know it is DRM content
    - o If they don't understand it they will treat it like a 3gp file that contains a codec they don't understand.
    - o Otherwise they will know the DRM structure and how to associate the file with the appropriate rights.
- DRM Specific Headers
    - o We will need space in the 3GP file header to store OMA DRM specific headers.
    - o These should generally be on the Movie level, but they should be override able on a track by track basis.
    - o As a part of the finalization of the OMA DRM 2.0 standard the OMA DRM group will require certain Headers to be present.
        - The OMA DRM group will provide the list of required headers in a timely manor. (after consensus is reached on what will be required for the 2.0 standard.)
        - There always should be space for arbitrary, "optional" headers
        - Therefore we desire a format that would allow an arbitrary number of name value pairs.

3.2 Payload Security Requirements

1. Overall security requirements
    a. Confidentiality of continuous media content.
    b. Encryption algorithm and method
        i. State-of-the art cryptography
        ii. Low or no overhead on payload

iii. No error propagation

iv. Tolerant to loss or re-ordering of transport protocol packets

c. Upgradability to other algorithms and modes

2. General requirements relating to the protected content format
   a. Support for encryption of content off-line
   b. Applicable to all continuous PSS 3GPP media formats.
   c. Support for selective encryption on a frame-by-frame basis
   d. Allow for random access to any frame in the file
   e. Encryption method for both streamed delivery and download.
3. Specific requirements relating to streaming
   a. Support for encryption of streams immediately before delivery (e.g. live content)
   b. Individual packet payloads must be decryptable independent from other packets.
   c. Support for selective encryption on a packet-by-packet basis
   d. Allow for encrypted local storage of received media packets

4 Requirements on real-time transport of PSS streams and associated signaling

4.1 Requirements on Session Signaling

4.1.1 Requirements on Session Description Protocol

The OMA DRM relies on certain headers associated with protected content and rights objects. In streaming case, SDP is used by the OMA DRM system to transport OMA DRM header information from the streaming server to the client. User Experience should be similar with both protected and unprotected streaming. The DRM specific headers are explained section 3.1.

1. Standard RTSP with SDP signalling shall be used as defined in [26-234].
2. The SDP file shall contain all OMA DRM specific headers associated with the content. The potential headers will be provided by OMA in [DRMCF].
   a. It should be possible for the streaming user agent to determine whether or not it can play the stream by using the information contained in the SDP file and provide the DRM agent in the device with the information. This is needed for creating similar kind of user experience than when using plain streaming session.
3. The same session set-up methods as defined in [26-234] shall be supported.
4. It shall be possible for the streaming server to generate the SDP file with DRM headers out of the information contained in a streamable .3gp file.
5. The DRM headers may apply to the session level or individual media stream level. Both cases should be supported.

3 Requested Action(s)

Based on the proposal above, OMA would like to request the following action:

- SA4 to study the requirements
- SA4 to give feedback to OMA DLDRM concerning the requirements, and work with DLDRM to resolve any associated questions and issues

- SA4 to specify methods in Release 6 to fulfil the requirements

OMA Actions

- OMA agrees to review the methods produced by the 3GPP SA4 and provide timely feedback
- OMA will provide versions of the OMA DRMCF as it matures.

4 Conclusion

OMA would like to cooperate with the 3GPP SA4 as they create Rel6 of their specification. Both organizations interests can be furthered with the creation of an interoperable protected content format. We appreciate the 3GPP's prior work in this area and would like to have their future specifications help enable distribution and interoperability of protected multi-media content.

5 Disclaimer

The Open Mobile Alliance takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in any information exchanged pursuant to this liaison or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights.

The Open Mobile Alliance makes no determination that the assurance of reasonable and non-discriminatory terms for the use of a technology has been fulfilled in practice.

Certain licensing obligations as set forth in the Open Mobile Alliance membership documents pertain to the Open Mobile Alliance members only and do not extend to non-members.

6 References

[DRMCF] OMA DRM Content Format version 2.0, to be drafted by OMA DRM+DL group

[Arch] OMA DRM Architecture Overview, Draft version, OMA-DRM-ARCH-v2_0-20030320-d