

**ISMA**  
**INTERNET STREAMING MEDIA ALLIANCE**

**Output Document Number TD00082**  
**Sept 2005**

**TITLE:**        **Preliminary Liaison Response to OMA BAC of the Open  
Mobile Alliance**

**Response to:** OMA-LS\_0044-BCAST-questions-to-ISMA-20050908-A

**AUTHOR (S) & EMAIL ADDRESS:**  
Peter Schirling, ISMA Liaison Officer, schirlin@us.ibm.com

**AREA:**        **Liaison**

**Status:**       **Draft**

**Addressee:**  
david.castleford@francetelecom.com,  
christine.mera@forapolis.com,  
OMA-LIAISON@mail.openmobilealliance.org

**CC:**



P.O. Box 29920 • 572 B Ruger Street  
San Francisco, CA 94129-0920  
Tel: +1.415.561.6276 • <http://www.isma.tv>

Dear David

Thank you for your liaison on the subject of ISMACryp. We considered the questions you raised at our meeting last week, and in view of your tight time-schedules, we are sending this immediate response. However, as noted below, we will also follow up later, and our members would like to read your documents in more depth than the time in the meeting allowed.

You ask two questions:

1. An ongoing action within BCAST is to investigate the impact of content protection for broadcast services. In particular, how is RTP encapsulation done for encrypted content?
2. An associated question is how this is related to SRTP?

As you are aware, ISMACryp has a design in which encryption is performed on the basic media content, before transport is considered. The advantages of this are many, not least that content can be transferred between different transport environments, or re-adapted (e.g. for a different MTU size) without needing decryption.

However, this does mean that the usual RTP packetization methods, many of which are content-aware, cannot be used. For audio, this is not usually a problem, as audio frames are rarely, if ever, fragmented, and of course such actions as interleaving work even when the frames are encrypted. The payload does, however, have to record that interleave has occurred if the encryption is 'continuous' (e.g. it is using a counter or block chaining). For video, the usual fragmentation rules (e.g. to split a frame at slice or macroblock boundaries) cannot be used. At the moment, ISMACryp uses the 'generic' MPEG-4 RTP payload format, specially configured for pre-encrypted content, for all media types in ISMA 1.0 and 2.0 specifications. However, this is not required; any suitable payload structure for specific pre-encrypted content could be used, including the payload structure for the un-encrypted media. Note that if the same payload structure is used, it nonetheless should be identified with a different payload name, to avoid the possibility that a terminal will interpret the encrypted data as if it were in the clear.

We have considered how to handle encrypted AVC content in our recent meetings, and at the one just concluded have adopted an approach. The editor of the document is currently assembling and writing the text, and we hope to forward it to you as soon as we have a cohesive text. Our approach is completely in line with the current ISMACryp 1.0 approach, that is, it is transport independent. This will be part of a "1.1" edition of ISMACryp, which will also, we intend, include informative text on using it with OMA 2.0 key signaling.

The design of ISMACryp is intended to be to codec-neutral, and we think that any codec can be fitted into the architecture. However, we do realize that our current document only discusses the payloads we use, and in some places the signaling is unclear for a non-



P.O. Box 29920 • 572 B Ruger Street  
San Francisco, CA 94129-0920  
Tel: +1.415.561.6276 • <http://www.isma.tv>

MPEG-4 payload. We are looking into this and may provide some more text, and cleaner documentation, for handling other codecs in a general approach for handling pre-encrypted content in RTP. Our expected time-frame is within the first half of 2006.

We are also starting work on a full second edition of ISMACryp, and we would welcome hearing of your needs, especially if they suggest ways we can improve our existing or upcoming specifications to meet them.

ISMACryp recommends use of SRTP message authentication but not SRTP encryption. Message authentication is optional, but we do recommend it for a variety of reasons. ISMACryp uses pre-encryption (or application encryption if you prefer), so there is no need for SRTP transport encryption. But we do need SRTP transport authentication (i.e. the integrity verification check of each packet) to protect against spoofing, replay, and various attacks that might occur over an IP channel that does not have very strict access control (we suspect, however, that in the case of a wireless transmission, spoofing of the signal is unlikely as it requires active re-transmission equipment physically located in the targeted area). SRTP overhead is a 4-10 byte authentication tag and that's relatively small compared to the roughly 1500-byte Ethernet MTU. ISMACryp, therefore, recommends use of SRTP message authentication but not SRTP encryption.

We hope that this initial response helps you with your work, and we will send more information and documents as they become available. We would be happy to work together with you on those aspects that are of interest or concern to you.

Sincerely,

Peter Schirling  
ISMA Liaison Chairman,