3GPP TSG SA WG3 Security — S3#32 **S3-040005**
09 - 13 February 2004
Edinburgh, Scotland, UK

TSG-SA WG4#29 meeting ***Tdoc S4 (03)0843***

Nov 24-28, Tampere

Title:	**LS on DRM streaming service**
Response to:	“**LS on Protection of MBMS and DRM Streaming Services” S4-030812 (S3-030805)**
Release:	Release 6
Source:	SA4
To:	SA3
Cc:	OMA DLDRM, SAGE, SA1

Contact Person:

Name:	Olle Franceschi
Tel. Number:	+46 46 23 26 64
E-mail Address:	olle.franceschi@ericsson.com

Attachments: S4-030757

1 Introduction

TSG WG SA4 would like to thank TSG WG SA3 for their LS containing a status report of the ongoing discussion on DRM in SA3.

2 SA4 answer on the action in SA4-030812

The following action was directed to SA4:

- **Give feedback to TSG SA3 whether the SRTP transform as proposed in S3-030750 is a suitable and feasible mechanism for securing MBMS streaming services from an SA4 point of view**

SA4 has not yet defined which protocol should be used for MBMS streaming, the MBMS work is still in an early stage and SA4 are not yet in the position to give any specific comments on a preferred protocol. For integrity protection, SRTP as defined by IETF, or the version described in S3-030750, are two possible candidates for DRM protected MBMS streaming exposed to SA4 so far. SA4 cannot comment on their suitability at this point in time. It is expected that SA4 has better understanding after the SA4#30 meeting (February 23-27, 2004).

For DRM-protected point-to-point streaming (PSS Rel-6) a high level working assumption has been agreed on at the SA4#29 meeting. The working assumption contains the following elements:

a) DRM confidentiality protection of streamed media packets is done through the application of a payload format wrapper, enabling "pre-encryption" with an explicit IV in line with the proposal of S4-030757.

b) Parameters to be considered for inclusion in signaling for the payload format wrapper are described in S4-030757.

c) Specifying key management procedures for the confidentiality protection will be performed by OMA BAC DL+DRM group.

d) An optional (to implement and use) integrity protection through application of the SRTP with default HMAC-SHA1 integrity mechanism, i.e. not through the modified SRTP transform proposed in S3-030750. Integrity protection might be equally applicable to both DRM and non-DRM content.

SA4 hopes that in point to point and MBMS streaming the greatest possible commonality of DRM techniques will be used, subject to their suitability in each environment.

3 Actions

Comments on the solution outlined above are welcome.

4 Date of Next 3GPP SA4 Meetings

3GPPSA4#30	23 - 27 Feb 2004	Sophia Antipolis, F
3GPPSA4#31	17 - 21 May 2004	TBD

TSG-SA WG4#29 meeting **_Tdoc S4 (03)0757_**

Nov 24-28, Tampere Agenda item: 6, 13.2

Title: Proposed RTP and SDP for pre-packetized encrypted media

Release: Release 6

Source: David Singer, Apple Computer

Attachments:

---

1 Introduction

This document define a RTP payload format for pre-packetized encrypted media. It is orthogonal to SRTP in several ways, notably that the encryption transform is not dependent on ephemeral information such as the SSRC, IP addresses or port numbers. Thus, if the path MTU is known in advance, the packetization and encryption may be statically computed and stored. In particular, in ISO-family (e.g. MP4) files, the encryption may be stored in the hint track.

It is compatible with the ISMA cryptography specification, in that it uses the same parameters for the format. It is intended to complement that specification, not replace it. Combining these two specifications, we cover the following cases:

a) Encrypted media in ISO-family (e.g. MP4) files [ISMA];

b) Packetization of pre-encrypted media for some codec formats [ISMA];

c) Encryption of pre-packetized media for any codec format [this specification].

I believe this fulfills the expressed OMA requirements. I think that this is orthogonal to SRTP, and could be used without or with it, as appropriate.

2 Packet Format

The formation of packets to this payload format can be seen as applying the following transformation to an existing RTP stream:

a) changing the association between payload-type in the RTP header and the name of the payload (by changing the payload type value), for all encrypted packets;

b) inserting information in each packet before the payload, documenting the initialization vector (IV) and key used;

c) encrypting the payload;

d) documenting the encryption format and its parameters – the format for SDP is defined below.

After this transformation has been applied, the packet appears as below:

```
+---------------------+
|     RTP header      |
+---------------------+
|     IV              |
+---------------------+
|     key_indicator   |
+---------------------+
|     payload         |
+---------------------+
```

The two new fields (IV, key indicator) are configurable in size and appear after the RTP and extension header (if any).

Selective encryption is permitted by not performing the packet transformation on selected packets; their association between payload type and payload format remains unchanged.

Note that this makes packets larger; if the packetization was previously at MTU, then the packets will now exceed MTU (as the IV is unlikely to have a zero length).

> *Example. Assume an AAC audio stream is send with an RTPMAP that says payload type 96 is AAC. When the AAC stream is encrypted then the RTPMAP may say 96 is AAC and 97 is EncryptedPacket. The format parameter for payload 97 says OriginalFormat is 96. Each encrypted packet has the payload type changed to 97, the unencrypted packets are left alone. Note that the transformation only applies to the payload type PT in the RTP header and that all other parameters such as RTP timestamp, sequence number and SDP parameters are unchanged.*

3 Signalling

The signaling parameters for this format are defined in the following table.

DESCRIPTOR	**DEFINED VALUES**	**DEFAULT**
CryptoSuite	AES_CTR_128	AES_CTR_128
IVLength	0..8	4
SelectiveEncryption	0 (False) or 1 (True)	0
KeyIndicatorLength	0..255	0
{Key}		""
OriginalFormat	0..127	Mandatory parameter

This payload format is added to the RTPMAP for this session, using a dynamic payload type. The remaining RTPMAP must be preserved unaltered.

The parameters have the meaning assigned in the ISMA specification, except for:

a) SelectiveEncryption; if this value is true (1), then the stream may contain encrypted packets and un-encrypted packets, distinguishable by their payload type; if this is false (0) then only encrypted packets shall be in the stream.

b) OriginalFormat; this is a mandatory parameter for this format. Its value is the RTP payload type (PT) value that the packets had before they were encrypted (a number).

Thus the remaining are:

a) CryptoSuite: the name of the encruption suite (identifies the transform and its parameters, e.g. AES Counter Mode in 128 bits);

b) IVLength: the length o fthe IV in each packet, in bytes.

c) KeyIndicatorLength: the length of the key indicator in each packet, in bytes.

d) Key: an indication of the need to signal in SDP whatever we and OMA decide is the appropriate way to indicate keys: URL etc.

4 Authentication

Packet authentication (as defined in the ISMA and SRTP specifications) may also be applied.