3GPP TSG SA WG3 Security — S3#30 **S3-030506**
06 - 10 October 2003
Povoa de Varzim, Portugal

3GPP TSG-WG4 Meeting #28 **Tdoc S4 (03)0660**
Erlangen, Germany, 3-Sept-2003.

Title: LS on cipher suite for DRM-protected streamed media for PSS
Response to:
Release: Rel-6
Work Item: Packet Switched Streaming Services Rel-6

Source: S4
To: S3
Cc:

Contact Person:
Name: **Jeremy Worley**
Tel. Number: +1 206 674 2676
E-mail Address: jworley@real.com

Attachments: S4-030639

---

1. Overall Description:

As part of S4's Rel-6 work item, it is considering DRM specific impacts on PSS and MMS services. Such impacts include: storage file format, payload format for streaming, associated signalling for streaming, and cipher suite. S4 has been liasing with OMA DL+DRM working group regarding interworking between OMA DRM 2.0 and PSS Rel-6 service.

S4 requires the determination of symmetric cryptographic algorithm to be used. S4 views the choice of cryptographic algorithm as being within the authority of S3 and asks S3 to consider this question and provide a decision on which symmetric key algorithm shall be used.

Tdoc S4-030639 proposed the use of AES Counter Mode (AES-CTR) at 128-bit key length, as it is believed to offer the following benefits:

- it provides adequate cryptographic security for dynamic media,
- it allows encrypting arbitrary byte lengths,
- it is the cipher algorithm used by ISMA in ISMAcryp,
- it is low complexity to decrypt on the client, and
- the management of IVs for AES-CTR becomes the management of counter values, which can be done compactly.

2. Actions:

To S3 group.

ACTION: S4 kindly asks S3 group to consider the question of cryptographic suite to be used for encrypting media delivered over RTP and to reply to S4 regarding whether AES-CTR is acceptable, and if not, with which cryptographic suite S4 can use.

3. Date of Next TSG-WG4 Meetings:

TSG-WG4 Meeting #29	24th – 28th November 2003	Location TBD.
TSG-WG4 Meeting #30	23rd – 27th February 2004	Location TBD

TSG-SA4#28 meeting

Tdoc S4 (03) 0639

September 1-5, 2003, Erlangen, Germany

Source: **Nokia, RealNetworks**

Title: **File format extensions and real-time transport of DRM protected continuous PSS media**

Document for: **Discussion**

Agenda Item: **6.6.1**

---

1 Introduction

According to the requirements laid out in [1], media tracks are encrypted and stored in a 3GP file. This document addresses the impact of applying the OMA key management system to protect PSS streams and files.

The 3GP file can be downloaded as a whole or encrypted packets can be extracted from the 3GP file and transported to the client using real-time transport protocols and mechanisms (e.g. RTP/UDP).

OMA DRM Content

2 General Encryption Properties

2.1 Encryption Scheme

The content encryption scheme is AES in counter mode at key length 128 bits. This mode is used for encrypting both downloaded as well as streamed content.

3 Downloadable file format modifications

3.1 Overview

The suggested modifications to the file format supporting encryption are in-line with the general ISO base file format constructs. A non DRM Player should still be able to understand and parse the protected format. Player will differentiate protected and non-protected content in the same way the ISO base format differentiates codec type. The following parts of the format are here defined: (a) how a content track is marked as protect (b) actual underlying protected codec (c) key management system used.

3.2 New codec type identifier

The 3GPP will add support for a new codec type code. The codec type will indicate to players that the tracks are encrypted. The actual codec information will be maintained in the underlying codec box/atom.

The Protection Info Box contains information about the encrypted format. This box contains all the information required both to understand the encryption transform applied and its parameters. It also contains the other information about the key management system. The Protection Info Box is a container Box.

```
aligned(8) class ProtectionInfoBox(fmt) extends FullBox('sinf', 0, 0) {
   OriginalFormatBox(fmt)     original-format;
   SchemeTypeBox              scheme-type;
   SchemeInformationBox       info;
}
```

The encrypted (protected) versions of the audio and video sample descriptions are as follows:

```
   // Visual Sequences
class EncVisualSampleEntry(codingname) extends VisualSampleEntry ('encv'){
   ProtectionInfoBox(codingname) info;
}
   // Audio Sequences
class EncAudioSampleEntry(codingname) extends AudioSampleEntry ('enca'){
   ProtectionInfoBox(codingname) info;
}
   // Timed text
class EncTextSampleEntry(codingname) extends TextSampleEntry (‘enct’){
   ProtectionInfoBox(codingname) info;
}
```

3.3 Actual Codec

The four-character-code (e.g. h263) that was replaced is stored in the OriginalFormatBox. The player uses this to understand the original media format, for player/codec initialization & required information. It is stored inside the protection information box (above).

```
aligned(8) class OriginalFormatBox(codingname) extends Box ('frma') {
   unsigned int(32)  data-format = codingname;
               // format of decrypted, encoded data
}
```

3.4 Key management system

The protection scheme is also referenced in the ProtectionInfoBox. This is used to store information about the protection scheme used to protect the track.

```
Protection scheme


aligned(8) class SchemeTypeBox extends FullBox('schm', 0, flags) {
   unsigned int(32)  scheme_type;          // 4CC identifying the scheme
   unsigned int(16)  scheme_version;       // scheme version
   if (flags & 0x000001) {
      unsigned int(8)   scheme_uri[];      // browser uri
   }
}


Scheme Information
```

```
aligned(8) class SchemeInformationBox extends FullBox('schi', 0, 0) {
   Box   scheme-specific-data[];
}
```

3.5 Example Scheme

For example, the OMA scheme specific information would look like this:

```
aligned(8) class OMADRMKMSBox extends FullBox('odrm', 0, 0) {
   OMADRMSampleFormatBox  sample_format;
   OMADRMHeadersBox headers;
}
```

The OMA DRM key management system (KMS) box refers to a location where a license for the encrypted content can be obtained. Also contained in the header is a sample format box. This box is used to indicate the format of the headers placed on media access units.

```
aligned(8) class OMADRMSampleFormatBox extends FullBox('osfm', 0, 0) {
   bit(1)   selective-encryption;
   bit(7)   reserved;
   uint(8)  key-indicator-length;
   uint(8)  IV-length;
}
aligned(8) class OMADRMHeadersBox extends Box('ohdr') {
   bit(8) data[]; // OMA DRM headers, to the end of the box
}
```

The OMA DRM headers box is used to contain OMA DRM specific information, which is to be defined by OMA. The box will contain e.g. ContentID and RightsIssuerURI fields.

4 Real-time transport of protected PSS media

Since the media streams / tracks / packets are encrypted, they are not any longer compliant to the payload formats defined by the IETF and used in 3GPP PSS [2][3][4]. Thus, it is necessary to define a 3GPP RTP wrapper payload format that can transport any encrypted payload, specifically encrypted versions of [2][3][4], but also any other defined RTP payload format.

One new wrapper payload format is defined that we call “RTP payload format for encrypted streams” (RPES). It gets an own new MIME type, e.g “X-3gpp-pss-encrypted” An instance of this wrapper payload format contains

- An initialization vector (IV), size to be defined[1]
- The encrypted original payload format, that means the media data packaged into a payload format, e.g. into one appropriate of [2][3][4], and this whole payload format (payload header+payload) is encrypted.

The two pictures below explain the concept. Fig. 1 depicts one unprotected packet of a stream (say, an H.263 packet, using payload format [2]). Fig. 2 depicts the protected version of the same packet.

[1] A standard size for an IV is 128 bits. It can however be reduced to a 32 bit counter per packet if a salt key k_s is distributed to the receiver; in this case the IV (for AES in counter mode) can be reproduced as IV = (k_s || counter).

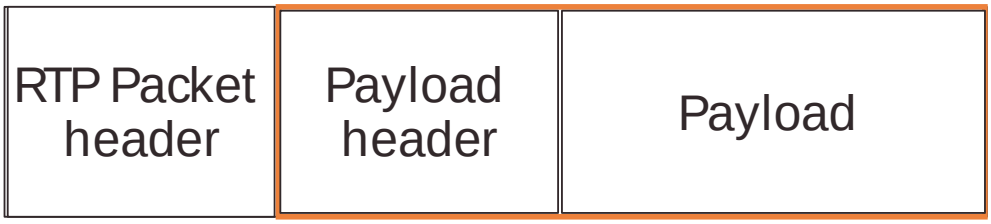


Figure 1: Standard RTP packet format

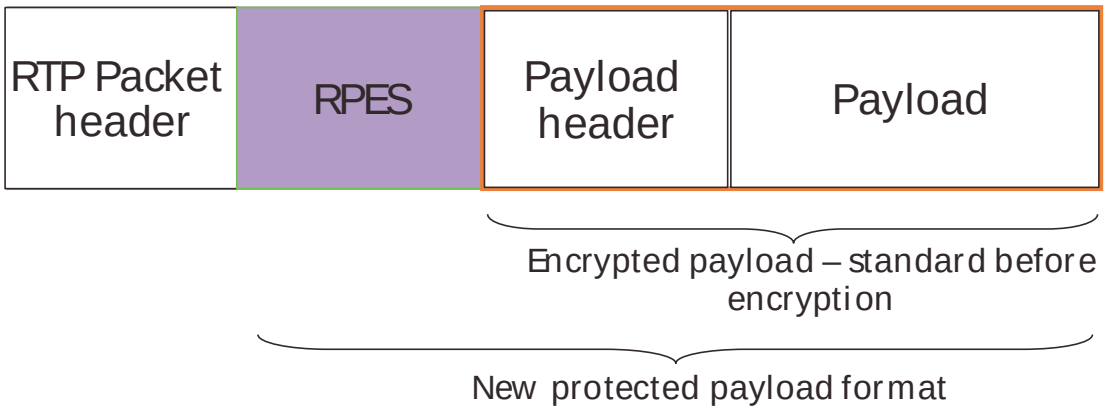


Figure 2: RTP packet containing protected content

The depicted solution allows using all defined RTP payload formats inside the wrapper payload format, and specifically also others than [2][3][4].

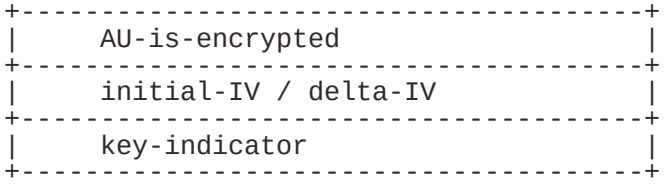
5 Payload format

The RPES is added for each access unit (or access unit fragment) in the RTP payload. The auxiliary header signals if the corresponding access unit is encrypted as well as the values of the corresponding initial vector and key indicator.

```
class 3GPPEncryptionContextAU(int auNum) {
      if (Selective_Encryption) {
         bit(1)   AU-is-encrypted;
         bit(7)   Reserved;
      }
      else AU-is-encrypted = 1;
      if(AU-is-encrypted) {
         if (auNum==0) // First AU in packet?
         {
            unsigned int(IV_Length*8)                 initial-IV;
            unsigned int(Key_Indicator_Length*8)      key-indicator;
         }
         else
         {
            int(Delta_IV_length*8)                    delta-IV;
            if (key_Indicator_Per_AU)
               unsigned int(Key_Indicator_Length*8)   key-indicator;
         }
      }
}
```

The following are constants that need to are signaled to the receiver as part of the session set-up: Selective_encryption, IV_length, Key_indicator_length, delta_IV_length, and key_indicator_per_AU.

So the auxiliary access unit header looks like this:



To reduce the overhead, several optimizations are allowed:

- The AU-is-encrypted field is only required if selective encryption is enabled.
- The Initial Vector need not be signaled for the second and following AUs in an RTP packet if the AU payloads are encrypted consecutively. For second and following AUs, the Initial Vector is only required in case of encryption before packetization in combination with interleaving.
- The key indicator is only required if this function is enabled (either per RTP packet or for each AU in the RTP packet).

6 Signaling of 3GPP protected streams

The 3GPP PSS shall use SDP fmtp to signal the streams are encrypted. This section defines the SDP FMTP signaling for 3GPP files. A new mime type will be used to do two things (1) define that the stream is protected (2) define the key management scheme used.

At minimum the SDP signaling shall use a payload type (ie “X-3gpp-pss-encrypted”) to signal encrypted streams:

m=video 0 RTP/AVP 99

a=rtpmap:99 X-3gpp-pss-encrypted/56000

a=fmtp:99 [GENERIC-PARMS] [3GPP-ENCRYPTION-PARAMS] [3GPP-PSS-ENCRYPTED-PARAMS]

RTP/SAVP profile MAY be used if integrity protection is required. SRTP encryption SHOULD NOT be used.

The possible 3GPP-ENCRYPTION-PARAMS are defined here. The specific protection scheme’s parameters will “inherit” from the base set of required 3GPP values.

The key management specific parameters (in 3GPP-PSS-ENCRYPTED-PARAMS, since they govern the usage of the format) will be defined by the key management system.

DESCRIPTOR	DEFINED VALUES	DEFAULT
3GPP-CRYPTO-SUITE	AES_CTR_128 (1)	1
3GPP-IV-LENGTH	1..8	1
3GPP-DELTA-IV-LENGTH	0..2	0
3GPP-SELECTIVE-ENCRYPTION	False (0) or True (1)	0

Table 1: 3GPP-ENCRYPTION-PARAMS fmtp parameters

3GPP-CRYPTO-SUITE defines the default cipher, mode, key length and other used for encryption of 3GPP media. AES-CTR is the default and mandatory-to-implement cipher and mode.

3GPP-IV-LENGTH describes the byte length of the initialization vector that is conveyed initially in the 3GPP packet. For the default cipher and mode, this is BSO value.

3GPP-DELTA-IV-LENGTH describes the byte length of the initialization vector, if any, that is conveyed with an individual AU.

3GPP-SELECTIVE-ENCRYPTION indicates that the media stream uses selective encryption when it is set to 1, which indicates that the selective encryption bit will appear in the 3GPP header.

The encrypted 3GPP format parameters shall include a reference to the protected format as in the following example. The example is the SDP sent for an OMA DRM protected PSS session transporting two media types: unprotected AMR audio, and protected MPEG-4 video. The lines in blue font declare the use of the wrapper payload format. The lines in red font declare that MPEG-4 payload format is used inside the wrapper format, and also convey the information needed for the receiver to set up the MPEG-4 codec appropriately

```
v=0
o=harry 2980675221 2980675778 IN IP4 host.example.net
s=Protected Media Session Example
c=IN IP4 0.0.0.0
t=0 0
a=control:*
a=range:npt=0-60
m=audio 0 RTP/AVP 96
b=AS:7
a=rtpmap:96 AMR/8000 octet-align=1
a=control:trackID=1
m=video 0 RTP/AVP 97 98
b=AS:30
a=rtpmap:98 X-3GPP-PSS-ENCRYPTED/56000
a=fmtp:98 3GPP-ENCRYPTED-REF=97;
            ContentID=36739876376;
            RightsIssuer="http://ri.myvendor.com/GetRights?content=36739876376"
a=rtpmap:97 MP4V-ES/56000
a=fmtp:97 profile-level-id=8;
config=000001b008000001b509000001010000012100884007a82c2090a31f
a=control:trackID=2
```

From this, the client can determine that the video track is protected within the wrapper format. Also, the client receives the OMA DRM key management-specific information, and can use this information to acquire the playback rights with the decryption key from a Rights Issuer. The key acquisition process is outside the scope of PSS.

References

[1] Liaison on DRM content format from OMA DLDRM to 3GPP SA4, OMA-DLDRM-2003-0081R2-3GPP-SA4-liaison-01May2003

[2] RFC 2429, "RTP Payload Format for the 1998 Version of ITU-T Rec. H.263 Video (H.263+)"

[3] RFC 3016, "RTP Payload Format for MPEG-4 Audio/Visual Streams"

[4] RFC 3267, "Real-Time Transport Protocol (RTP) Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs"