K.1.4 Signalling

This clause specifies the RTP payload format MIME type, and how it is utilized in SDP. An example is included as well.

Any unknown MIME parameter shall be ignored.

K.1.4.1 MIME type definition

K.1.4.1.1 audio/rtp-enc-aescm128

Type name: audio

Subtype name: rtp-enc-aescm128

Required parameters:

opt: The payload type number of the payload type contained in the encrypted payload. An integer value between 0-127.

rate: The timestamp rate of this payload type, which shall be the same as that of the original payload type. This is an integer value between 1 and 2^32.

ContentID: The OMA DRM content ID [75] used to identify the content when establishing a crypto context. The value is an RFC 3986 [60] URI, which shall be quoted using <">.

RightsIssuerURL: The right issuer URL as defined by OMA DRM [75]. The value is an URI in accordance with RFC 3986 [60], which shall be quoted using <">.

IVnonce: The value of this parameter is the nonce that forms the IV as specified by the crypto transform, encoded using Base 64 [69].

Optional parameters:

SelectiveEncryption: Indicates if this stream is selectively encrypted. Allowed values are 0 (false) and 1 (true). If not present, selective encryption shall not be used. Please note that unless this indicator is integrity protected, it fulfills no purpose.

Encoding considerations:

This type is framed and binary as defined in [96].

Security considerations:

See considerations raised in RTP RFC 3550 [9] and any applicable profile like RFC 3551 [10] or RFC 3711 [72]. Further see 3GPP TS 26.234, Release 6, Annex K for comments on security issues. The main issues that exists are:

- This RTP payload format only confidentiality protects the RTP payload, thus header information is leaked, similarly to SRTP.

- The use of stream ciphers as AES CM and no integrity protection allows an attacker to purposefully attack the content of the encrypted RTP payload by switching individual bits.

- The usage of selective encryption without integrity protection allows for an attacker to perform any replacements of complete RTP payloads and packets it desires.

- The payload format makes the receiver vulnerable to denial of service attacks that inserts RTP packets into the stream, that the receiver then interprets as being encrypted thus wasting computational resources. To prevent this attack, authentication needs to be used.

Interoperability considerations:

Published specification:

3GPP TS 26.234, Release 6.

Open Mobile Alliance DRM Content Format V2.0

Applications which use this media type:

Third Generation Partnership Project (3GPP) Packet-switched Streaming Service (PSS) clients and servers, which supports the Open Mobile Alliance's specification of Digital Rights Management version 2.0.

Additional information:

Magic number(s): N/A

File extension(s): N/A

Macintosh File Type Code(s): N/A

Person & email address to contact for further information:

Magnus Westerlund

magnus.westerlund@ericsson.com

Intended usage:

Common

Restrictions on usage:

This type is only defined for transfer via RTP (RFC 3550).

Author:

3GPP TSG SA WG4

Change controller:

3GPP TSG SA

K.1.4.1.2 video/rtp-enc-aescm128

Type name: video

Subtype name: rtp-enc-aescm128

Required parameters:

opt:	The payload type number of the payload type contained in the encrypted payload. An integer value between 0-127.
rate:	The timestamp rate of this payload type, which shall be the same as that of the original payload type. This is an integer value between 1 and 2^32.
ContentID:	The OMA DRM content ID [75] used to identify the content when establishing a crypto context. The value is an RFC 3986 [60] URI, which shall be quoted using <">.
RightsIssuerURL:	The right issuer URL as defined by OMA DRM [75]. The value is an URI in accordance with RFC 3986 [60], which shall be quoted using <">.
IVnonce:	The value of this parameter is the nonce that forms the IV as specified by the crypto transform, encoded using Base 64 [69].

Optional parameters:

SelectiveEncryption: Indicates if this stream is selectively encrypted. Allowed values are 0 (false) and 1 (true). If not present, selective encryption shall not be used. Please note that unless this indicator is integrity protected, it fulfills no purpose.

Encoding considerations:

This type is framed and binary as defined in [96].

Security considerations:

See considerations raised in RTP RFC 3550 [9] and any applicable profile like RFC 3551 [10] or RFC 3711 [72]. Further see 3GPP TS 26.234, Release 6, Annex K for comments on security issues. The main issues that exists are:

- This RTP payload format only confidentiality protects the RTP payload, thus header information is leaked, similarly to SRTP.

- The use of stream ciphers as AES CM and no integrity protection allows an attacker to purposefully attack the content of the encrypted RTP payload by switching individual bits.

- The usage of selective encryption without integrity protection allows for an attacker to perform any replacements of complete RTP payloads and packets it desires.

- The payload format makes the receiver vulnerable to denial of service attacks that inserts RTP packets into the stream, that the receiver then interprets as being encrypted thus wasting computational resources. To prevent this attack, authentication needs to be used.

Interoperability considerations:

Published specification:

3GPP TS 26.234, Release 6.

Open Mobile Alliance DRM Content Format V2.0

Applications which use this media type:

Third Generation Partnership Project (3GPP) Packet-switched Streaming Service (PSS) clients and servers, which supports the Open Mobile Alliance's specification of Digital Rights Management version 2.0.

Additional information:

Magic number(s): N/A

File extension(s): N/A

Macintosh File Type Code(s): N/A

Person & email address to contact for further information:

Magnus Westerlund
magnus.westerlund@ericsson.com

Intended usage:

Common

Restrictions on usage:

This type is only defined for transfer via RTP (RFC 3550).

Author

3GPP TSG SA WG4

Change controller:

3GPP TSG SA

K.1.4.1.3 text/rtp-enc-aescm128

Type name: text

Subtype name: rtp-enc-aescm128

Required parameters:

opt: The payload type number of the payload type contained in the encrypted payload. An integer value between 0-127.

rate: The timestamp rate of this payload type, which shall be the same as that of the original payload type. This is an integer value between 1 and 2^32.

ContentID: The OMA DRM content ID [75] used to identify the content when establishing a crypto context. The value is an RFC 3986 [60] URI, which shall be quoted using <">.

RightsIssuerURL: The right issuer URL as defined by OMA DRM [75]. The value is an URI in accordance with RFC 3986 [60], which shall be quoted using <">.

IVnonce: The value of this parameter is the nonce that forms the IV as specified by the crypto transform, encoded using Base 64 [69].

Optional parameters:

SelectiveEncryption: Indicates if this stream is selectively encrypted. Allowed values are 0 (false) and 1 (true). If not present, selective encryption shall not be used. Please note that unless this indicator is integrity protected, it fulfills no purpose.

Encoding considerations:

This type is framed as defined in [96].

Security considerations:

See considerations raised in RTP RFC 3550 [9] and any applicable profile like RFC 3551 [10] or RFC 3711 [72]. Further see 3GPP TS 26.234, Release 6, Annex K for comments on security issues. The main issues that exists are:

- This RTP payload format only confidentiality protects the RTP payload, thus header information is leaked, similarly to SRTP.

- The use of stream ciphers as AES CM and no integrity protection allows an attacker to purposefully attack the content of the encrypted RTP payload by switching individual bits.

- The usage of selective encryption without integrity protection allows for an attacker to perform any replacements of complete RTP payloads and packets it desires.

- The payload format makes the receiver vulnerable to denial of service attacks that inserts RTP packets into the stream, that the receiver then interprets as being encrypted thus wasting computational resources. To prevent this attack, authentication needs to be used.

Interoperability considerations:

Published specification:

3GPP TS 26.234, Release 6.

Open Mobile Alliance DRM Content Format V2.0

Applications which use this media type:

Third Generation Partnership Project (3GPP) Packet-switched Streaming Service (PSS) clients and servers, which supports the Open Mobile Alliance's specification of Digital Rights Management version 2.0.

Additional information:

Magic number(s): N/A

File extension(s): N/A

Macintosh File Type Code(s): N/A

Person & email address to contact for further information:

Magnus Westerlund
magnus.westerlund@ericsson.com

Intended usage:

Common

Restrictions on usage:

This type is only defined for transfer via RTP (RFC 3550).

Author

3GPP TSG SA WG4

Change controller:

3GPP TSG SA