Network Working Group	L. Dondeti, Ed.
Internet-Draft	QUALCOMM, Inc.
Intended status: Informational	A. Jerichow
Expires: April 18, 2008	Nokia Siemens Networks GmbH and
	Co.KG
	October 16, 2007

Session Description Protocol (SDP) Attributes for OMA BCAST Service and Content Protection
draft-dondeti-oma-sip-sdp-attrs-02

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.
Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.
Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."
The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.
The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.
This Internet-Draft will expire on April 18, 2008.

Abstract

This document provides descriptions of SDP attributes used by the Open Mobile Alliance's Broadcast Service and Content Protection specification.

Table of Contents

---

1. Introduction   [TOC](#)

The Open Mobile Alliance (OMA)'s Broadcast (BCAST) group is specifying service and content protection mechanisms for broadcast services over wireless networks. As part of that specification, several new SDP attributes are necessary to allow the broadcast server to signal the service and content protection parameters to clients.
Section 8.2.4 of RFC 4566 [1] (Handley, M., Jacobson, V., and C. Perkins, "SDP: Session Description Protocol," July 2006.) requires that new SDP attributes are registered through IANA with name, contact information and description (and other similar parameters). A standards track specification is RECOMMENDED if the new attribute(s) will have widespread use and interoperability considerations.
OMA BCAST specifications are expected to be used by 3GPP MBMS, 3GPP2 BCMCS and DVB-H based broadcast wireless systems.
This document provides descriptions of the SDP attributes used in the OMA BCAST Service and Content Protection specification [2] (Open Mobile Alliance, "Service and Content Protection for Mobile Broadcast Services," 2007.).

---

2. Terminology   [TOC](#)

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [3] (Bradner,

S., "Key words for use in RFCs to Indicate Requirement Levels,"
March 1997.).

---

3. New SDP Attributes

The following new SDP attributes have been specified:

   *a=bcastversion:<major>.<minor>

   *a=stkmstream:<id of the stkm stream>

   *a=SRTPAuthentication:<id for SRTP authentication algorithm value>

   *a=SRTPROCTxRate:<ROC transmission rate>

See Section 5 for details on IANA considerations.

---

4. Security Considerations

In addition to the notes in Section 7 of RFC 4566 [1] (Handley, M.,
Jacobson, V., and C. Perkins, "SDP: Session Description Protocol,"
July 2006.), the following considerations may be applicable:
Some of the new SDP parameters indicate the version, type of the key
management system used for service or content protection of broadcast
content. Others provide references to relevant key management traffic
streams so that receivers can map the media streams to key streams and
retrieve the necessary keys to decrypt media.
Modification of references to key streams will result in DoS attacks,
but nothing more. However, if the kmsversion parameter is sent
unprotected, there may be possibilities for downgrade attacks.

---

5. IANA Considerations

This document, following the guidelines of [5] (Narten, T. and H.
Alvestrand, "Guidelines for Writing an IANA Considerations Section in
RFCs," October 1998.), instructs IANA to register a number of SDP
attributes.

5.1. Registration of new SDP attributes

This memo provides instructions to IANA to register a number of OMA BCAST only attributes in the Session Description Protocol Parameters registry [1] (Handley, M., Jacobson, V., and C. Perkins, "SDP: Session Description Protocol," July 2006.). The registration data, according to RFC 4566 [1] (Handley, M., Jacobson, V., and C. Perkins, "SDP: Session Description Protocol," July 2006.) follows.
Note to the RFC Editor: replace "RFC XXXX" with the RFC number of this specification.

5.1.1. Registration of the attribute a=bcastversion:<major>.<minor>

Contact: Anja Jerichow <anja.jerichow@nsn.com>

Phone: +49 89 636-45868

Attribute name: bcastversion:<major>.<minor>

Long-form attribute name: BCAST version

Type of attribute: session-level

   This attribute is not dependent on charset.

Description: This attribute specifies the OMA BCAST version "bcastversion" Value in the format x.y. The Value field is of XML data type Decimal.

Specification: RFC XXXX and OMA-TS-BCAST_SvcCntProtection, Section 10.1.1 [2] (Open Mobile Alliance, "Service and Content Protection for Mobile Broadcast Services," 2007.)

5.1.2. Registration of the attribute a=stkmstream:<id of the stkm stream>

Contact: Anja Jerichow <anja.jerichow@nsn.com>

Phone: +49 89 636-45868

Attribute name: stkmstream:<id of the stkm stream>

Long-form attribute name: Short Term Key Message stream identifyer

Type of attribute:

> session-level or media-level attribute

> The attribute can be at session level, in which case it applies to all media streams, or it can be at media level, in which case it only applies to the specified media and would overwrite possible session level attribute.

> This attribute is not dependent on charset.

Description: The stkmstream attribute specifies mapping Short Term Key Message streams to media streams in the SDP.

> Each session or media stream can have multiple stkmstream attributes. Using this attribute, the terminal can lookup the corresponding STKM stream announcements and figure out which one to listen to and process. We note that this attribute is optional and hence would not be there for unencrypted media streams.

> This field specifies the type of keystream as a string. The valid values are "stkm" for short term key messages and "ltkm" for long term key messages.

Specification: RFC XXXX and OMA-TS-BCAST_SvcCntProtection, Section 10.1.3 [2] (Open Mobile Alliance, "Service and Content Protection for Mobile Broadcast Services," 2007.)

5.1.3. Registration of the attribute a=SRTPAuthentication:<id for SRTP authentication algorithm value>

Contact: Anja Jerichow <anja.jerichow@nsn.com>

Phone: +49 89 636-45868

Attribute name: SRTPAuthentication:<id for SRTP authentication algorithm value>

Long-form attribute name: SRTP authentication algorithm value identifyer

Type of attribute: media-level

> This attribute is not dependent on charset.

Description: When SRTP is used, the attribute SRTPAuthentication states which authentication algorithm to use. Based on , the

identifier is a transform-independent parameter of the cryptographic context for SRTP in integer format.

One of the following three integrity transforms registered for the three modes MUST be used: value "2" for RCCm1, "3" for RCCm2 and "4" for RCCm3.

Specification: RFC XXXX and OMA-TS-BCAST_SvcCntProtection, Section 10.4 [2] (Open Mobile Alliance, "Service and Content Protection for Mobile Broadcast Services," 2007.)

5.1.4. Registration of the attribute a=SRTPROCTxRate:<ROC transmission rate>

Contact: Anja Jerichow <anja.jerichow@nsn.com>

Phone: +49 89 636-45868

Attribute name: SRTPROCTxRate:<ROC transmission rate>

Long-form attribute name: ROC transmission rate

Type of attribute: media-level

This attribute is not dependent on charset.

Description: When SRTP is used, the attribute SRTPROCTxRate is used to define the ROC transmission rate, R, which is given in network byte order.

R MUST be a non-zero unsigned integer between 1 and 65535 inclusive, as specified in [4] (Lehtovirta, V., Naslund, M., and K. Norrman, "Integrity Transform Carrying Roll-Over Counter for the Secure Real-time Transport Protocol (SRTP)," January 2007.). If the ROC transmission rate is not included in the negotiation, the default value of 1 SHALL be used.

Specification: RFC XXXX and OMA-TS-BCAST_SvcCntProtection, Section 10.4 [2] (Open Mobile Alliance, "Service and Content Protection for Mobile Broadcast Services," 2007.)

---

6. Acknowledgments

Many thanks to Charles Lo, Uwe Rauschenbach, David Castleford, Hosame Abu-Amara, and Miguel Garcia for their help and support.

7. References [TOC]

7.1. Normative References [TOC]

[1]	Handley, M., Jacobson, V., and C. Perkins, "SDP: Session Description Protocol," RFC 4566, July 2006 (TXT).
[2]	Open Mobile Alliance, "Service and Content Protection for Mobile Broadcast Services," OMA OMA-TS-BCAST_SvcCntProtection-V1_0-20070504-D, 2007.
[3]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[4]	Lehtovirta, V., Naslund, M., and K. Norrman, "Integrity Transform Carrying Roll-Over Counter for the Secure Real-time Transport Protocol (SRTP)," RFC 4771, January 2007 (TXT).

7.2. Informative References [TOC]

[5]	Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs," BCP 26, RFC 2434, October 1998 (TXT, HTML, XML).

Authors' Addresses [TOC]

	Lakshminath Dondeti (editor)
	QUALCOMM, Inc.
	5775 Morehouse Dr
	San Diego, CA
	USA
Phone:	+1 858-845-1267
Email:	ldondeti@qualcomm.com
	Anja Jerichow
	Nokia Siemens Networks GmbH and Co.KG
	Martinstr. 76

	81541 Munich
	Germany
Phone:	+49 89 636-45868
Email:	anja.jerichow@nsn.com

Full Copyright Statement

Intellectual Property