

Network Working Group	J. Fischl	
Internet-Draft	CounterPath Solutions, Inc.	
Intended status: Standards Track	H. Tschofenig	
Expires: July 26, 2008	Nokia Siemens Networks	
	January 23, 2008	

[TOC](#)

Session Description Protocol (SDP) Indicators for Datagram Transport Layer Security (DTLS)

draft-ietf-mmusic-sdp-dtls-00.txt

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/lid-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 July 26, 2008.

Abstract

This specification defines how to use the Session Description Protocol (SDP) to signal that media will be transported over Datagram Transport Layer Security (DTLS) or where the SRTP security context is established using DTLS and. It reuses the syntax and semantics for an SDP 'fingerprint' attribute that identifies the certificate which will be presented during the DTLS handshake.

Table of Contents

- [1. Introduction](#)
- [2. Terminology](#)
- [3. DTLS Certificates](#)

- [4.](#) SDP
 - [5.](#) Session Description for RTP/SAVP over DTLS
 - [6.](#) IANA Considerations
 - [7.](#) Security Considerations
 - [8.](#) Acknowledgments
 - [9.](#) References
 - [9.1.](#) Normative References
 - [9.2.](#) Informational References
 - [§](#) Authors' Addresses
 - [§](#) Intellectual Property and Copyright Statements
-

1. Introduction

[TOC](#)

Session Description Protocol (SDP) [RFC 2327 \(Handley, M. and V. Jacobson, "SDP: Session Description Protocol," April 1998.\)](#) [7] has been used to set up the transport of various types of media with RTP [\[9\] \(Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications," July 2003.\)](#) over UDP [\[10\] \(Schulzrinne, H. and S. Casner, "RTP Profile for Audio and Video Conferences with Minimal Control," July 2003.\)](#), TCP [\[14\] \(Lazzaro, J., "Framing Real-time Transport Protocol \(RTP\) and RTP Control Protocol \(RTCP\) Packets over Connection-Oriented Transport," July 2006.\)](#), and TLS [\[2\] \(Lennox, J., "Connection-Oriented Media Transport over the Transport Layer Security \(TLS\) Protocol in the Session Description Protocol \(SDP\)," July 2006.\)](#). DTLS [\[12\] \(Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security," April 2006.\)](#) is a protocol for applying TLS security to datagram protocols such as UDP and DCCP [\[1\] \(Kohler, E., "Datagram Congestion Control Protocol \(DCCP\)," December 2005.\)](#). This specification defines new SDP protocol syntax that allow SDP to indicate that DTLS should be used to transport the media when TLS is used. The handling of TLS sessions in SDP is defined in [\[2\] \(Lennox, J., "Connection-Oriented Media Transport over the Transport Layer Security \(TLS\) Protocol in the Session Description Protocol \(SDP\)," July 2006.\)](#) that discusses only TLS over TCP. This document extends that specification to also deal with TLS over datagram protocols such as UDP and DCCP and when (D)TLS is used to establish keys for SRTP as in [\[5\] \(McGrew, D. and E. Rescorla, "Datagram Transport Layer Security \(DTLS\) Extension to Establish Keys for Secure Real-time Transport Protocol \(SRTP\)," February 2009.\)](#)

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 \(Bradner, S.,](#)

["Key words for use in RFCs to Indicate Requirement Levels," March 1997.\)](#)
[6].

3. DTLS Certificates

[TOC](#)

The two endpoints in the exchange present their identities as part of the DTLS handshake procedure using certificates. This document uses certificates in the same style as described in Comedia over TLS in SDP [2] ([Lennox, J., "Connection-Oriented Media Transport over the Transport Layer Security \(TLS\) Protocol in the Session Description Protocol \(SDP\)," July 2006.\)](#)).

If self-signed certificates are used, the content of the subjectAltName attribute inside the certificate MAY use the uniform resource identifier (URI) of the user. This is useful for debugging purposes only and is not required to bind the certificate to one of the communication endpoints. The integrity of the certificate is ensured through the fingerprint attribute in the SDP. The subjectAltName is not an important component of the certificate verification.

If the endpoint is also able to make anonymous sessions, a distinct, unique, self-signed certificate SHOULD be provided for this purpose. The generation of public/private key pairs is relatively expensive. Endpoints are not required to generate certificates for each session. The endpoints MAY cache their certificates and reuse them across multiple sessions.

[Editor's Note: Certificate lifetime issues will be discussed in a future draft version.]

4. SDP

[TOC](#)

In addition to the usual contents of an SDP [13] ([Handley, M., Jacobson, V., and C. Perkins, "SDP: Session Description Protocol," July 2006.\)](#) message, each 'm' line will also contain several attributes as specified in [RFC 4145 \(Yon, D. and G. Camarillo, "TCP-Based Media Transport in the Session Description Protocol \(SDP\)," September 2005.\)](#) [11] and [2] ([Lennox, J., "Connection-Oriented Media Transport over the Transport Layer Security \(TLS\) Protocol in the Session Description Protocol \(SDP\)," July 2006.\)](#)).

The endpoint MUST use the setup and connection attributes defined in "TCP-Based Media Transport in the SDP" [11] ([Yon, D. and G. Camarillo, "TCP-Based Media Transport in the Session Description Protocol \(SDP\)," September 2005.\)](#)). For the purposes of this specification, a setup:active endpoint will act as a DTLS client and a setup:passive endpoint will act as a DTLS server. The connection attribute indicates whether or not to reuse an existing DTLS association.

A certificate fingerprint is the output of a one-way hash function computed over the distinguished encoding rules (DER) form of the

certificate. The endpoint MUST use the certificate fingerprint attribute as specified in [\[2\] \(Lennox, J., "Connection-Oriented Media Transport over the Transport Layer Security \(TLS\) Protocol in the Session Description Protocol \(SDP\)," July 2006.\)](#).

TODD: The MMUSIC working group is currently studying the problem of signalling in SDP the ability/desire to initiate a secure channel rather than an insecure one [\[3\] \(Andreasen, F., "SDP Capability Negotiation," March 2010.\)](#)[\[4\] \(Andreasen, F., "SDP Capability Negotiation: Requirements and Review of Existing Work," March 2007.\)](#). We need to use those techniques when they are finalized.

5. Session Description for RTP/SAVP over DTLS

[TOC](#)

This specification defines new tokens to describe the protocol used in SDP "m=" lines. The new values defined for the proto field are:

- *When a RTP/SAVP stream is transported over DTLS with DCCP, then the token SHALL be DCCP/TLS/RTP/SAVP.
- *When a RTP/SAVP stream is transported over DTLS with UDP, the token SHALL be UDP/TLS/RTP/SAVP.
- *When a RTP/SAVP stream is transported over TLS with TCP, the token SHALL be TCP/TLS/RTP/SAVP.
- *When media is transported over DTLS with UDP, the token SHALL be UDP/TLS.
- *When media is transported over DTLS with DCCP, the token SHALL be DCCP/TLS.

For RTP profiles other than AVP, a new token should be defined in the form of DCCP/TLS/RTP/xyz, UDP/TLS/RTP/xyz and TCP/TLS/RTP/xyz where xyz is replaced with an appropriate token for that profile.

6. IANA Considerations

[TOC](#)

This specification updates the "Session Description Protocol (SDP) Parameters" registry as defined in Appendix B of [RFC 2327 \(Handley, M. and V. Jacobson, "SDP: Session Description Protocol," April 1998.\)](#) [7]. Specifically it adds the following values to the table for the "proto" field.

Type	SDP Name	Reference
----	-----	-----
proto	TCP/TLS/RTP/SAVP	[RFC-XXXX]
	UDP/TLS/RTP/SAVP	[RFC-XXXX]
	DCCP/TLS/RTP/SAVP	[RFC-XXXX]
	UDP/TLS	[RFC-XXXX]
	DCCP/TLS	[RFC-XXXX]

Note to RFC Editor: Please replace RFC-XXXX with the RFC number of this specification.

7. Security Considerations

[TOC](#)

When using self signed certificates, the signalling protocol used to transport the SDP MUST ensure the integrity of the SDP so that the fingerprint attribute can not be altered. Failure to do this would allow a attacker to insert themselves in the media channel as a man-in-the-middle. A method of ensuring the integrity of the SDP when transporting over the SIP [RFC 3261 \(Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol," June 2002.\)](#) [8] signalling protocol is described in [\[15\] \(Fischl, J., Tschofenig, H., and E. Rescorla, "Framework for Establishing an SRTP Security Context using DTLS," March 2009.\)](#)

8. Acknowledgments

[TOC](#)

Cullen Jennings contributed substantial text and comments to this document. This document benefitted from discussions with Francois Audet, Nagendra Modadugu, Eric Rescorla, and Dan Wing. Thanks also for useful comments by Flemming Andreasen, Rohan Mahy, David McGrew, and David Oran.

9. References

[TOC](#)

9.1. Normative References

[TOC](#)

[1]	
-----	--

	Kohler, E., " Datagram Congestion Control Protocol (DCCP) ," draft-ietf-dccp-spec-13 (work in progress), December 2005 (TXT , PS).
[2]	Lennox, J., " Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP) ," RFC 4572, July 2006 (TXT).
[3]	Andreasen, F., " SDP Capability Negotiation ," draft-ietf-mmusic-sdp-capability-negotiation-13 (work in progress), March 2010 (TXT).
[4]	Andreasen, F., " SDP Capability Negotiation: Requirements and Review of Existing Work ," draft-ietf-mmusic-sdp-capability-negotiation-reqts-01 (work in progress), March 2007 (TXT).
[5]	McGrew, D. and E. Rescorla, " Datagram Transport Layer Security (DTLS) Extension to Establish Keys for Secure Real-time Transport Protocol (SRTP) ," draft-ietf-avt-dtls-srtp-07 (work in progress), February 2009 (TXT).
[6]	Bradner, S., " Key words for use in RFCs to Indicate Requirement Levels ," BCP 14, RFC 2119, March 1997 (TXT , HTML , XML).
[7]	Handley, M. and V. Jacobson, " SDP: Session Description Protocol ," RFC 2327, April 1998 (TXT , HTML , XML).
[8]	Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, " SIP: Session Initiation Protocol ," RFC 3261, June 2002 (TXT).
[9]	Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, " RTP: A Transport Protocol for Real-Time Applications ," STD 64, RFC 3550, July 2003 (TXT , PS , PDF).
[10]	Schulzrinne, H. and S. Casner, " RTP Profile for Audio and Video Conferences with Minimal Control ," STD 65, RFC 3551, July 2003 (TXT , PS , PDF).
[11]	Yon, D. and G. Camarillo, " TCP-Based Media Transport in the Session Description Protocol (SDP) ," RFC 4145, September 2005 (TXT).
[12]	Rescorla, E. and N. Modadugu, " Datagram Transport Layer Security ," RFC 4347, April 2006 (TXT).

9.2. Informational References

[TOC](#)

[13]	Handley, M., Jacobson, V., and C. Perkins, " SDP: Session Description Protocol ," RFC 4566, July 2006 (TXT).
[14]	Lazzaro, J., " Framing Real-time Transport Protocol (RTP) and RTP Control Protocol (RTCP) Packets over Connection-Oriented Transport ," RFC 4571, July 2006 (TXT).
[15]	Fischl, J., Tschofenig, H., and E. Rescorla, " Framework for Establishing an SRTP Security Context using DTLS ," draft-ietf-sip-dtls-srtp-framework-07 (work in progress), March 2009 (TXT).

Authors' Addresses

[TOC](#)

	Jason Fischl
	CounterPath Solutions, Inc.
	Suite 300, One Bentall Centre, 505 Burrard Street
	Vancouver, BC V7X 1M3
	Canada
Phone:	+1 604 320-3340
Email:	jason@counterpath.com
	Hannes Tschofenig
	Nokia Siemens Networks
	Linnoitustie 6
	Espoo 02600
	Finland
Phone:	+358 (50) 4871445
Email:	Hannes.Tschofenig@nsn.com
URI:	http://www.tschofenig.com

Full Copyright Statement

[TOC](#)

Copyright © The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be

obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.