

Network Working Group  
Internet-Draft  
Expires: August 29, 2006

H. Tschofenig  
Siemens  
E. Rescorla  
Network Resonance  
February 25, 2006

Real-Time Transport Protocol (RTP) over Datagram Transport Layer  
Security (DTLS)  
draft-tschofenig-avt-rtp-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 August 29, 2006.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

This specification defines how to establish secure Real-Time Transport Protocol (RTP) sessions over the Datagram Transport Layer Security (DTLS) protocol.

Internet-Draft

RTP over DTLS

February 2006

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Conventions Used In This Document . . . . .	<a href="#">3</a>
<a href="#">3.</a>	RTP Packet Generation . . . . .	<a href="#">3</a>
<a href="#">4.</a>	SRTP Compatibility Mode . . . . .	<a href="#">4</a>
<a href="#">5.</a>	RTP and RTCP . . . . .	<a href="#">5</a>
<a href="#">6.</a>	Size Comparison to SRTP . . . . .	<a href="#">5</a>
<a href="#">7.</a>	Security Considerations . . . . .	<a href="#">6</a>
<a href="#">8.</a>	IANA Considerations . . . . .	<a href="#">7</a>
<a href="#">9.</a>	Acknowledgments . . . . .	<a href="#">7</a>
<a href="#">10.</a>	References . . . . .	<a href="#">7</a>
<a href="#">10.1.</a>	Normative References . . . . .	<a href="#">7</a>
<a href="#">10.2.</a>	Informational References . . . . .	<a href="#">8</a>
<a href="#">Appendix A.</a>	Packet Header Formats . . . . .	<a href="#">9</a>
<a href="#">A.1.</a>	SRTP Packet Format . . . . .	<a href="#">9</a>
<a href="#">A.2.</a>	DTLS/RTP Packet Format . . . . .	<a href="#">10</a>
<a href="#">A.3.</a>	DTLS/RTP Packet Format in SRTP-compatibility mode . . . . .	<a href="#">12</a>
	Authors' Addresses . . . . .	<a href="#">13</a>
	Intellectual Property and Copyright Statements . . . . .	<a href="#">14</a>

## [1.](#) Introduction

Security is a major concern for real-time multimedia systems such as Internet telephony. This document is part of a suite of documents describing a complete system for securing such communications using Datagram Transport Layer Security (DTLS). Readers should also read [\[18\]](#) and [\[17\]](#) for background. This document focuses on using DTLS to protect the Real-Time Transport Protocol (RTP).

## [2.](#) Conventions Used In This Document

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 [\[1\]](#).

DTLS[4] and TLS[5] uses the term "session" to refer to a long-lived set of keying material that spans associations. In this document, consistent with SIP/SDP usage, we use it to refer to a multimedia session and use the term "TLS session" to refer to the TLS construct. We use the term "association" to refer to a particular DTLS ciphersuite and keying material set. For consistency with other SIP/SDP usage, we use the term "connection" when what's being referred to is a multimedia stream that is not specifically DTLS/TLS.

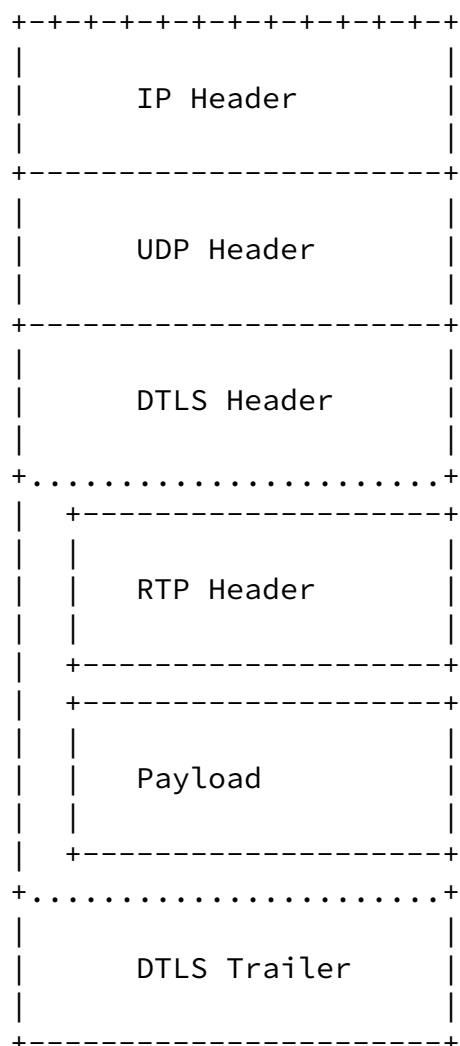
In this document, the term "Mutual DTLS" indicates that both the DTLS client and server present certificates even if one or both certificates are self-signed.

## [3.](#) RTP Packet Generation

The normal RTP[3] and RTCP payloads that would be sent inside a UDP packet are also sent inside of a DTLS packet. The synchronization source (SSRC) is filled in as with a normal RTP packet. For example, in an audio session that also contains DTMF using [RFC2833](#) [\[9\]](#) the

audio packets will have different SSRC values than the DTMF packets.

A DTLS/RTP packet has the following layout:



A sample packet is shown in [Appendix A](#) (using the TLS MAC truncation mode from [\[6\]](#) and the TLS Counter mode of [\[14\]](#)).

#### 4. SRTP Compatibility Mode

SRTP [\[13\]](#) is a tightly coupled encryption mode for RTP which utilizes a number of advanced techniques to provide optimal performance and deployability for protected RTP traffic. These benefits include:

- o Leaving the RTP header unencrypted (enabling header compression[\[8\]](#)[\[10\]](#)[\[12\]](#) and easy debugging).
- o Having the packets appear to be RTP packets for firewall compatibility.
- o Zero header overhead

This section describes a profile of RTP over DTLS which allows the use of DTLS key management while providing an on-the-wire packet format which is the same as that of SRTP.

This profile depends on 'Extensions for DTLS in Low Bandwidth

Environments' described in [\[15\]](#) and on 'TLS Partial Encryption Mode' [\[16\]](#). The former extension reduces the per-record bandwidth of the data channel. The latter extension allows partial encryption of record bodies.

In order to use DTLS/RTP in SRTP compatibility mode, implementations SHOULD negotiate:

- o The TLS partial encryption extension with an InitialPlaintext value equal to the length of the RTP header.
- o The DTLS implicit application data header.
- o The TLS MAC truncation extension.

With these extensions negotiated, RTP over DTLS packets look identical to SRTP records with a 10-byte MAC value. In fact, they cannot be distinguished without access to the DTLS or SRTP keying material. In addition, since the RTP header is in the clear, header compression and debugging both work. Note that DTLS running in SRTP compatibility mode has the same security properties as ordinary DTLS (with the truncated MAC); there is a reduction between the two protocols.

## 5. RTP and RTCP

Note that the active endpoint will establish two DTLS sessions with the passive endpoint for each of the RTP and RTCP channels. The RTP and RTCP sessions share the same certificate and thus the same fingerprint.

[Editor's Note: In next draft revision TLS session resumption will be discussed.]

## 6. Size Comparison to SRTP

One of the major arguments for SRTP is its low space overhead, which comes from reusing as much as possible of the RTP infrastructure. There are two areas where RTP over DTLS has overhead greater than that of SRTP:

- o Record header (type, version, length, sequence number, epoch)
- o MAC (DTLS uses a 10 byte MAC and SRTP uses a 4 byte MAC).

Header	DTLS (bytes)	SRTP (bytes)
Record Header	5	0
sequence + epoch	8	0
MAC	10	4
Total	23	4

The DTLS record header consumes 5 bytes for the type, version, and length + 8 bytes for the sequence number and epoch. Thus, the total size difference between DTLS and SRTP is 19 bytes if the master key identifier (MKI) is not used in SRTP and 15 bytes if a 4 byte MKI is used.

The profile discussed in the previous section allows the complete removal of the header for a net difference of 6 bytes (without MKI) or 2 bytes (with MKI). This difference is entirely due to the longer (and more secure) MAC provided by TLS and DTLS.

This section provides a comparison of packet sizes for G.729 and G.711 codecs using 20ms packets. Comparisons are provided for unencrypted packets, SRTP without MKI, SRTP with MKI, DTLS and DTLS in SRTP compatibility mode.

packet	size(bytes)	bitrate(kb/s)
G.729	60	24.0
G.729 + SRTP	64	25.6
G.729 + SRTP w/ MKI	68	27.2
G.729 + DTLS (SRTP-compatibility)	70	28.0
G.729 + DTLS	98	39.2
G.711	200	80.0
G.711 + SRTP	204	81.6
G.711 + SRTP w/ MKI	208	83.2
G.711 + DTLS (SRTP-compatibility)	210	84.0
G.711 + DTLS	238	95.2

Note that DTLS with the SRTP-compatibility attributes is 1.09 times the bandwidth of SRTP (without MKI) for G.729 and 1.03 times the bandwidth of SRTP with MKI. It is 1.03 times the bandwidth of SRTP with MKI for G.711 and 1.01 times the bandwidth of SRTP with MKI.

## 7. Security Considerations

Because RTP/DTLS runs over DTLS, which is based on TLS, which has seen extensive security analysis, we can have fairly high confidence in the security of the system once the channel is established. Similarly, because DTLS incorporates a handshake mechanism, there is no need to provide for confidentiality of the handshake channel. All that is necessary is to ensure that the communicating peers' certificates are correct.

The standard TLS/DTLS strategy for authenticating the communicating parties is to give the server (and optionally the client) a PKIX [2] certificate. The client then verifies the certificate and checks that the name in the certificate matches the server's domain name. This works because there are a relatively small number of servers with well-defined names; a situation which does not usually occur in the VoIP context.

An alternative strategy can be used where the certificates are self-signed. When using this approach, the endpoint that acts as a client MUST have a way to verify that the server's certificate is correct and vice-versa. An approach to address this using the Session Initiation Protocol (SIP) [11] and the Session Description Protocol (SDP) [7] is described in SIP for DTLS Media [17] and SDP for DTLS [18]

## [8.](#) IANA Considerations

This specification does not require any IANA actions.

## [9.](#) Acknowledgments

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

## [10.](#) References

### [10.1.](#) Normative References

- [1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [2] Housley, R., Polk, W., Ford, W., and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation



- [3] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", STD 64, [RFC 3550](#), July 2003.
- [4] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security", [draft-rescorla-dtls-05](#) (work in progress), June 2005.

## 10.2. Informational References

- [5] Dierks, T. and E. Rescorla, "The TLS Protocol Version 1.1", [draft-ietf-tls-rfc2246-bis-13](#) (work in progress), June 2005.
- [6] Blake-Wilson, S., "Transport Layer Security (TLS) Extensions", [draft-ietf-tls-rfc3546bis-02](#) (work in progress), October 2005.
- [7] Handley, M. and V. Jacobson, "SDP: Session Description Protocol", [RFC 2327](#), April 1998.
- [8] Casner, S. and V. Jacobson, "Compressing IP/UDP/RTP Headers for Low-Speed Serial Links", [RFC 2508](#), February 1999.
- [9] Schulzrinne, H. and S. Petrack, "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals", [RFC 2833](#), May 2000.
- [10] Bormann, C., Burmeister, C., Degermark, M., Fukushima, H., Hannu, H., Jonsson, L-E., Hakenberg, R., Koren, T., Le, K., Liu, Z., Martensson, A., Miyazaki, A., Svanbro, K., Wiebke, T., Yoshimura, T., and H. Zheng, "RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed", [RFC 3095](#), July 2001.
- [11] 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.
- [12] Koren, T., Casner, S., Geevarghese, J., Thompson, B., and P. Ruddy, "Enhanced Compressed RTP (CRTP) for Links with High Delay, Packet Loss and Reordering", [RFC 3545](#), July 2003.
- [13] Baugher, M., McGrew, D., Naslund, M., Carrara, E., and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)", [RFC 3711](#), March 2004.
- [14] Modadugu, N. and E. Rescorla, "AES Counter Mode Cipher Suites for TLS and DTLS", [draft-modadugu-tls-ctr-00](#) (work in progress), October 2005.

- 
- [15] Modadugu, N. and E. Rescorla, "Extensions for DTLS in Low Bandwidth Environments", [draft-modadugu-dtls-short-00](#) (work in progress), October 2005.
  - [16] Rescorla, E., "TLS Partial Encryption Mode", [draft-rescorla-tls-partial-00](#) (work in progress), January 2006.
  - [17] Fischl, J., Tschofenig, H., and E. Rescorla, "Session Initiation Protocol (SIP) for Media Over Transport Layer Security (TLS)", February 2006.
  - [18] Fischl, J. and H. Tschofenig, "Session Description Protocol (SDP) Indicators for Datagram Transport Layer Security (DTLS)", [draft-fischl-mmusic-sdp-dtls-00](#) (work in progress), February 2006.

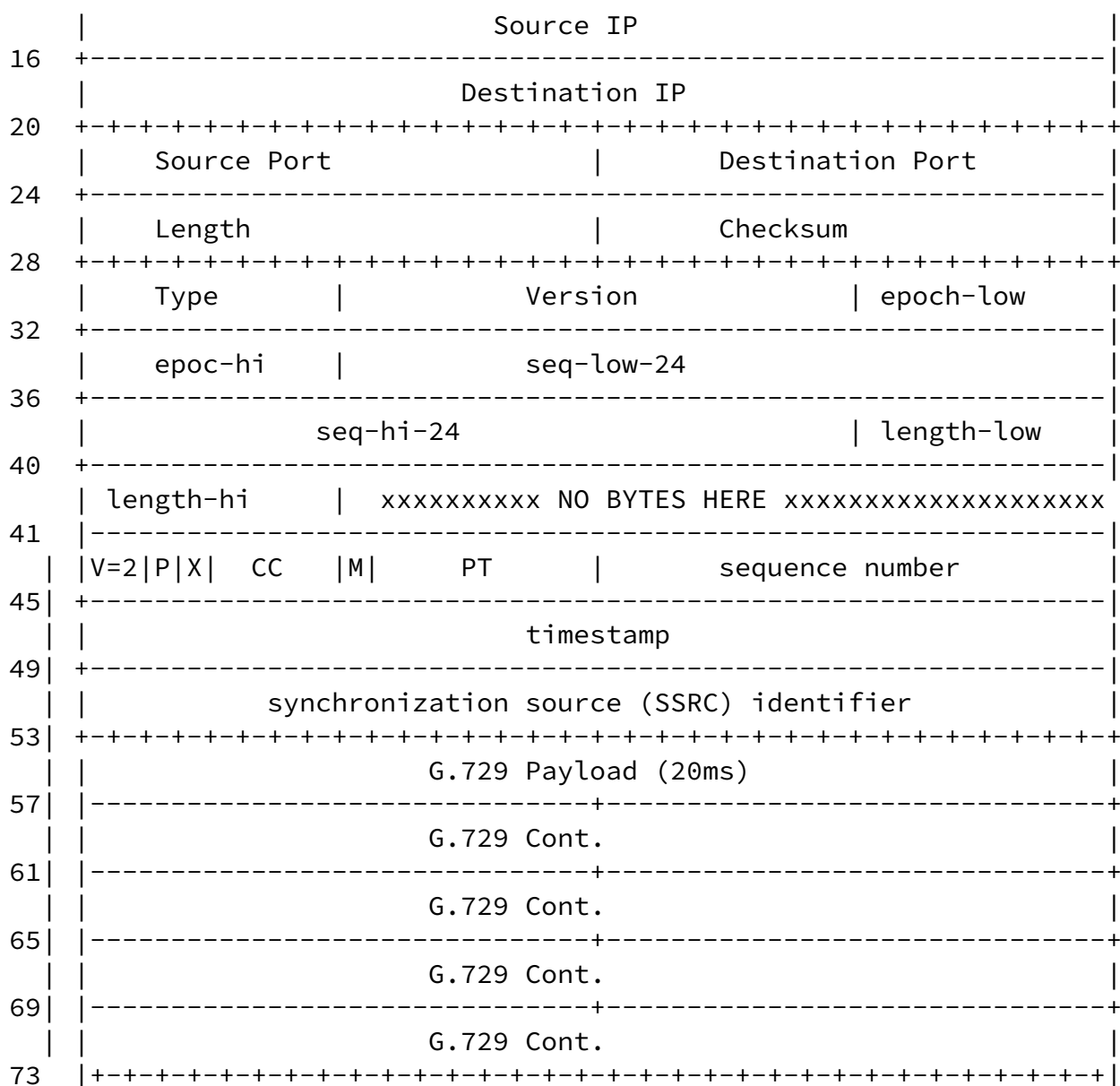
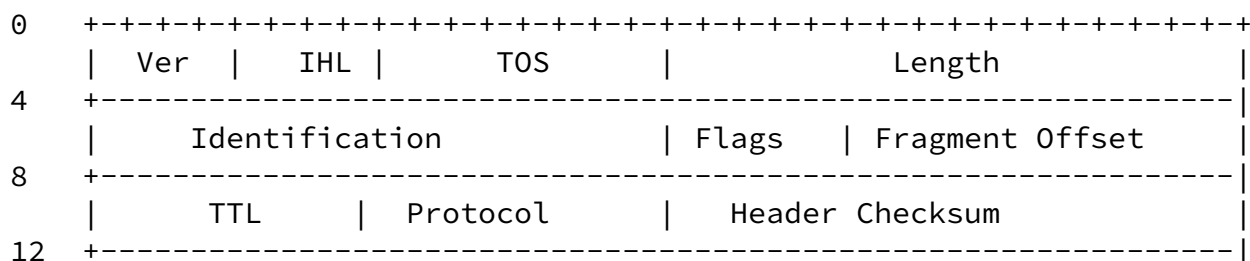
## [Appendix A](#). Packet Header Formats

The subsequent figures illustrate the different packet formats and the size of the headers.

### [A.1](#). SRTP Packet Format

This figure shows the SRTP packet format layout.





		HMAC-SHA1	
77		-----+	
		HMAC-SHA1 (cont)	
81		-----+	
		HMAC-SHA1 (cont)	
85		-----+	
		HMAC-SHA1 (cont)	
89		-----+	
		HMAC-SHA1 (cont)	
93		-----+	
		PAD	
97	+++++		
	PAD LEN	XXX NO BYTES	
98	+++++		

### A.3. DTLS/RTP Packet Format in SRTP-compatibility mode

This figure shows the DTLS/RTP packet with low bandwidth extensions.

0	+ +															
---	---	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

		G.729 Payload (20ms)	
44		-----+	
		G.729 Cont.	
48		-----+	
		G.729 Cont.	
52		-----+	
		G.729 Cont.	
56		-----+	
		G.729 Cont.	
60		+++++	
		SRTP MKI (OPTIONAL)	
64		+++++	
		HMAC-SHA1	
68		-----+	
		HMAC-SHA1 (cont)	
72		-----+	
		HMAC-SHA1 (cont)	
74		-----+	

#### Authors' Addresses

Hannes Tschofenig  
 Siemens  
 Otto-Hahn-Ring 6  
 Munich, Bavaria 81739  
 Germany

Email: Hannes.Tschofenig@siemens.com

Eric Rescorla  
 Network Resonance  
 2483 E. Bayshore #212  
 Palo Alto, CA 94303  
 USA

Email: ekr@networkresonance.com

#### Intellectual Property Statement

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](mailto:ietf-ipr@ietf.org).

#### Disclaimer of Validity

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 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.

#### Copyright Statement

Copyright (C) The Internet Society (2006). 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.

#### Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.