MMUSIC
Internet-Draft
Intended status: Standards Track
Expires: April 10, 2017

C. Holmberg
Ericsson
R. Shpount
TurboBridge
S. Loreto
G. Camarillo
Ericsson

October 7, 2016

# Session Description Protocol (SDP) Offer/Answer Procedures For Stream Control Transmission Protocol (SCTP) over Datagram Transport Layer Security (DTLS) Transport.

draft-ietf-mmusic-sctp-sdp-18

## Abstract

The Stream Control Transmission Protocol (SCTP) is a transport protocol used to establish associations between two endpoints. draft-ietf-tsvwg-sctp-dtls-encaps-09 specifies how SCTP can be used on top of the Datagram Transport Layer Security (DTLS) protocol, referred to as SCTP-over-DTLS.

This specification defines the following new Session Description Protocol (SDP) protocol identifiers (proto values):'UDP/DTLS/SCTP' and 'TCP/DTLS/SCTP'. This specification also specifies how to use the new proto values with the SDP Offer/Answer mechanism for negotiating SCTP-over-DTLS associations.

## Status of This Memo

## Copyright Notice



## Table of Contents

1. Introduction . . . . . 3
2. Conventions . . . . . 4
3. SCTP Terminology . . . . . 4
4. SDP Media Descriptions . . . . . 4
  4.1. General . . . . . 4
  4.2. Protocol Identifiers . . . . . 5
  4.3. Media Format Management . . . . . 5
  4.4. Syntax . . . . . 6
    4.4.1. General . . . . . 6
    4.4.2. ABNF . . . . . 6
  4.5. Example . . . . . 6
5. SDP 'sctp-port' Attribute . . . . . 6
  5.1. General . . . . . 6
  5.2. Syntax . . . . . 7
  5.3. Mux Category . . . . . 7
6. SDP 'max-message-size' Attribute . . . . . 7
  6.1. General . . . . . 7
  6.2. Syntax . . . . . 8
  6.3. Mux Category . . . . . 8
7. UDP/DTLS/SCTP Transport Realization . . . . . 8
8. TCP/DTLS/SCTP Transport Realization . . . . . 9
9. Association And Connection Management . . . . . 9
  9.1. General . . . . . 9
  9.2. SDP sendrecv/sendonly/recvonly/inactive Attribute . . . . 9
  9.3. SCTP Association . . . . . 9
  9.4. DTLS Association (UDP/DTLS/SCTP And TCP/DTLS/SCTP) . . . 10
  9.5. TCP Connection (TCP/DTLS/SCTP) . . . . . 11
10. SDP Offer/Answer Procedures . . . . . 11
  10.1. General . . . . . 11
  10.2. Generating the Initial SDP Offer . . . . . 11
  10.3. Generating the SDP Answer . . . . . 12

10.4. Offerer Processing of the SDP Answer . . . . . 13
10.5. Modifying the Session . . . . . 13
11. Multihoming Considerations . . . . . 14
12. NAT Considerations . . . . . 14
12.1. General . . . . . 14
12.2. ICE Considerations . . . . . 14
13. Examples . . . . . 15
13.1. Establishment of UDP/DTLS/SCTP association . . . . . 15
14. Security Considerations . . . . . 16
15. IANA Considerations . . . . . 17
15.1. New SDP proto values . . . . . 17
15.2. New SDP Attributes . . . . . 17
15.2.1. sctp-port . . . . . 17
15.2.2. max-message-size . . . . . 18
15.3. association-usage Name Registry . . . . . 18
16. Acknowledgments . . . . . 19
17. . . . . 19
18. References . . . . . 21
18.1. Normative References . . . . . 21
18.2. Informative References . . . . . 23
Authors' Addresses . . . . . 23

## 1. Introduction

SDP (Session Description Protocol) [RFC4566] provides a general-purpose format for describing multimedia sessions in announcements or invitations. TCP-Based Media Transport in the Session Description Protocol (SDP) [RFC4145] specifies a general mechanism for describing and establishing TCP [RFC0793] streams. Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in SDP [RFC4572] extends RFC4145 [RFC4145] for describing TCP-based media streams that are protected using TLS.

The Stream Control Transmission Protocol (SCTP) [RFC4960] is a transport protocol used to establish associations between two endpoints.

The Stream Control Transmission Protocol (SCTP) [RFC4960] is a transport protocol used to establish associations between two endpoints. [I-D.ietf-tsvwg-sctp-dtls-encaps] specifies how SCTP can be used on top of the Datagram Transport Layer Security (DTLS) protocol, referred to as SCTP-over-DTLS.

This specification defines the following new Session Description Protocol (SDP) [RFC4566] protocol identifiers (proto values):'UDP/DTLS/SCTP' and 'TCP/DTLS/SCTP'. This specification also specifies how to use the new proto values with the SDP Offer/Answer mechanism [RFC3264] for negotiating SCTP-over-DTLS associations.

NOTE: TLS is designed to run on top of a byte-stream oriented transport protocol providing a reliable, in-sequence delivery like TCP. [RFC6083] presents serious limitations with transporting TLS on top of SCTP. Therefore, defining a mechanism to negotiate media streams transported using TLS on top of SCTP, i.e., 'SCTP/TLS', is outside the scope of this specification. In addition, defining a mechanism to negotiate non-protected SCTP associations is also outside the scope of this specification.

## 2. Conventions

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 [RFC2119].

## 3. SCTP Terminology

SCTP Association: A protocol relationship between SCTP endpoints, composed of the two SCTP endpoints and protocol state information including Verification Tags and the currently active set of Transmission Sequence Numbers (TSNs), etc. An association can be uniquely identified by the transport addresses used by the endpoints in the association.

SCTP Stream: A unidirectional logical channel established from one to another associated SCTP endpoint, within which all user messages are delivered in sequence except for those submitted to the unordered delivery service.

SCTP Transport address: A transport address is traditionally defined by a network-layer address, a transport-layer protocol, and a transport-layer port number. In the case of SCTP running over IP, a transport address is defined by the combination of an IP address and an SCTP port number (where SCTP is the transport protocol).

SCTP-over-DTLS: SCTP used on top of DTLS, as specified in [I-D.ietf-tsvwg-sctp-dtls-encaps].

## 4. SDP Media Descriptions

### 4.1. General

This section defines the following new SDP Media Description (m-line) protocol identifiers (proto values) for describing an SCTP association: UDP/DTLS/SCTP' and 'TCP/DTLS/SCTP'. The section also describes how an m- line, associated with the proto values, is created.

The following is the format for an 'm' line, as specified in RFC4566 [RFC4566]:

```
m=<media> <port> <proto> <fmt> ...
```

The 'UDP/DTLS/SCTP' and 'TCP/DTLS/SCTP' proto values are similar to both the 'UDP' and 'TCP' proto values in that they only describe the transport-layer protocol and not the upper-layer protocol.

NOTE: When the 'UDP/DTLS/SCTP' and 'TCP/DTLS/SCTP' proto values are used, the underlying transport protocol is respectively UDP and TCP; SCTP is carried on top of DTLS which is on top of those transport-layer protocols.

The m- line fmt value, identifying the application-layer protocol, MUST be registered by IANA.

### 4.2. Protocol Identifiers

The new proto values are defined as below:

- The 'UDP/DTLS/SCTP' proto value describes an SCTP association on top of a DTLS association on top of UDP, as defined in Section 7.

- The 'TCP/DTLS/SCTP' proto value describes an SCTP association on top of a DTLS association on top of TCP, as defined in Section 8.

### 4.3. Media Format Management

[RFC4566] defines that specifications defining new proto values must define the rules by which their media format (fmt) namespace is managed. Use of an existing MIME subtype for the format is encouraged. If no MIME subtype exists, it is recommended that a suitable one is registered through the IETF process [RFC6838] [RFC4289] by production of, or reference to, a standards-track RFC that defines the transport protocol for the format.

An m- line with a proto value of UDP/DTLS/SCTP' or 'TCP/DTLS/SCTP' always describe a single SCTP association.

In addition, such m- line MUST further indicate the application-layer protocol using an 'fmt' identifier. There MUST be exactly one 'fmt' value per m- line associated with the proto values defined in this specification. The "fmt" namespace associated with those proto values describes the generic application usage of the entire SCTP association, including the associated SCTP streams.

NOTE: A mechanism on how to describe, and manage, individual SCTP streams within an SCTP association, is outside the scope of this specification.

## 4.4. Syntax

### 4.4.1. General

This section defines the ABNF [RFC5234] for the SDP media description when associated with any of the proto values defined in this document.

This specification creates an IANA registry for 'association-usage' values.

### 4.4.2. ABNF

```
sctp-m-line = %x6d "="
 ("application" SP udp-port  SP "UDP/DTLS/SCTP" SP fmt CRLF) /
 ("application" SP tcp-port  SP "TCP/DTLS/SCTP" SP fmt CRLF)

udp-port = port

tcp-port = port

fmt = association-usage

association-usage = token

    token and port as defined in RFC4566
```

## 4.5. Example

```
m=application 12345 UDP/DTLS/SCTP webrtc-datachannel
a=max-message-size: 100000
```

# 5. SDP 'sctp-port' Attribute

## 5.1. General

This section defines a new SDP media-level attribute, 'sctp-port'. The attribute can be associated with an SDP media description (m-line) with a 'UDP/DTLS/SCTP' or a 'TCP/DTLS/SCTP' proto value. In that case the m- line port value indicates the port of the underlying transport layer protocol (UDP or TCP), and the 'sctp-port' value indicates the SCTP port.

No default value is defined for the SDP sctp-port attribute. Therefore, if the attribute is not present, the associated m- line MUST be considered invalid.

Usage of the SDP 'sctp-port' attribute with other proto values is not specified, and MUST be discarded if received.

### 5.2. Syntax

The ABNF for the SDP 'sctp-port' attribute is:

```
sctp-port-attr  =  "a=sctp-port:" port
port            =  (1*5)DIGIT
```

The SCTP port range is between 0 and 65535 (both included). Leading zeroes MUST NOT be used.

### 5.3. Mux Category

The mux category [I-D.ietf-mmusic-sdp-mux-attributes] for the SDP sctp-port' attribute is SPECIAL. Usage of the attribute is only applicable when associated with 'UDP/DTLS/SCTP' and 'TCP/DTLS/SCTP' proto value m- lines.

As the usage of multiple SCTP associations on top of a single DTLS association is outside the scope of this specification, no mux rules are specified for the 'UDP/DTLS/SCTP' and 'TCP/DTLS/SCTP' proto values. Future extensions, that define how to negotiate multiplexing of multiple SCTP associations of top of a single DTLS association, need to also define the mux rules for the attribute.

## 6. SDP 'max-message-size' Attribute

### 6.1. General

This section defines a new SDP media-level attribute, 'max-message-size'. The attribute can be associated with an m- line to indicate the maximum message size (indicated in bytes) that an SCTP endpoint is willing to receive on the SCTP association associated with the m-line. Different attribute values can be used in each direction.

The remote peer MUST assume that larger messages will be rejected by the SCTP endpoint. SCTP endpoints need to decide on appropriate behavior in case a message that exceeds the maximum size needs to be sent.

If the SDP 'max-message-size' attribute contains a maximum message size value of zero, it indicates the SCTP endpoint will handle messages of any size, subject to memory capacity etc.

If the SDP 'max-message-size' attribute is not present, the default value is 64K.

NOTE: This specification only defines the usage of the SDP 'max-message-size' attribute when associated with an m- line containing one of the following proto values: 'UDP/DTLS/SCTP' or 'TCP/DTLS/SCTP'. Usage of the attribute with other proto values needs to be defined in a separate specification.

### 6.2. Syntax

The ABNF for the SDP 'max-message-size' attribute is:

```
max-message-size-attr =  "a=max-message-size:" max-message-size
max-message-size      =  1*40DIGIT
```

Leading zeroes MUST NOT be used.

### 6.3. Mux Category

The mux category for the SDP 'max-message-size' attribute is SPECIAL. The mux rules depends on the proto value of the associated m- line.

As the usage of multiple SCTP associations on top of a single DTLS association is outside the scope of this specification, no mux rules are specified for the 'UDP/DTLS/SCTP' and 'TCP/DTLS/SCTP' proto values.

## 7. UDP/DTLS/SCTP Transport Realization

The UDP/DTLS/SCTP transport is realized as described below:

- o SCTP on top of DTLS is realized according to the procedures defined in [I-D.ietf-tsvwg-sctp-dtls-encaps]; and

- o DTLS on top of UDP is realized according to the procedures in defined in [RFC6347].

NOTE: While [I-D.ietf-tsvwg-sctp-dtls-encaps] allows multiple SCTP associations on top of a single DTLS association, the procedures in this specification only supports the negotiation of a single SCTP association on top of any given DTLS association.

## 8. TCP/DTLS/SCTP Transport Realization

The TCP/DTLS/SCTP transport is realized as described below:

- o SCTP on top of DTLS is realized according to the procedures defined in [I-D.ietf-tsvwg-sctp-dtls-encaps]; and

- o DTLS on top of TCP is realized using the framing method defined in [RFC4571], with DTLS packets being sent instead of RTP/RTCP packets, and SDP signaling according to the procedures defined in this specification.

NOTE: DTLS on top of TCP, without using the framing method defined in [RFC4571] is outside the scope of this specification. A separate proto value would need to be registered for such transport realization.

## 9. Association And Connection Management

### 9.1. General

This section describes how to mange an SCTP association, DTLS association and TCP connection using SDP attributes.

In case of UDP/DTLS/SCTP and TCP/DTLS/SCTP the SCTP association, DTLS association and TCP connection are managed independently for each other. An association/connection can be re-established without impacting other associations/connections.

The detailed SDP Offer/Answer [RFC3264] procedures for the SDP attributes are described in (Section 10).

### 9.2. SDP sendrecv/sendonly/recvonly/inactive Attribute

This specification does not define semantics for the SDP direction attributes [RFC4566]. Unless semantics of these attributes for an SCTP association usage have been defined, SDP direction attributes MUST be discarded if present.

### 9.3. SCTP Association

When an SCTP association is established/re-established, both SCTP endpoints MUST initiate the SCTP association (i.e. both SCTP endpoints take the 'active' role), and MUST use the same SCTP port as client port and server port (in order to prevent two separate SCTP associations from being established).

As both SCTP endpoints take the 'active' role, this specification does not define usage of the SDP 'setup' attribute [RFC4145] for SCTP.

NOTE: The procedure above is different from TCP, where one endpoint takes the 'active' role, the other endpoint takes the 'passive' role, and only the 'active' endpoint initiates the TCP connection [RFC4145].

NOTE: In case of SCTP-over-DTLS, when the SCTP association is established it is assumed that any NAT traversal procedures for the underlying transport protocol (UDP or TCP) has successfully been performed.

Usage of the SDP 'connection' attribute [RFC4145] is not defined for SCTP. In order to trigger the closure and re-establishment of an SCTP association, the SDP 'sctp-port' attribute (Section 5) is used to indicate a new (different than the ones currently used) SCTP port.

Alternatively, an SCTP association can be closed using the SDP 'sctp-port' attribute with a zero attribute value. Later, the SCTP association can be re-established using the procedures in this section for establishing an SCTP association.

SCTP associations might be closed without SDP signalling, e.g, in case of a failure. When such SCTP association is re-established the SCTP endpoints MUST use the procedures in this section for establishing an SCTP association. New (different than the ones currently used) SCTP ports MUST be used.

NOTE: Closing and re-establishing the SCTP association using the SDP 'sctp-port' attribute will not impact the underlying DTLS association.

### 9.4. DTLS Association (UDP/DTLS/SCTP And TCP/DTLS/SCTP)

An DTLS association is managed according to the procedures in [I-D.ietf-mmusic-dtls-sdp]. Hence, the SDP 'setup' attribute is used to negotiate the (D)TLS roles ('client' and 'server') [RFC4572].

NOTE: The SDP 'setup' attribute is used both to negotiate both the DTLS roles and the TCP roles (Section 9.5).

NOTE: As described in [RFC5245], if the Interactive Connectivity Establishment (ICE) mechanism [RFC5245] is used, all ICE candidates associated with an DTLS association as considered part of the same DTLS association. Thus, a switch from one candidate pair to another

candidate pair will not trigger the establishment of a new DTLS association.

### 9.5. TCP Connection (TCP/DTLS/SCTP)

The TCP connection is managed according to the procedures in [RFC4145]. Hence, the SDP 'setup' attribute is used to negotiate the TCP roles ('active' and 'passive'), and the SDP 'connection' attribute is used to indicate whether to use an existing TCP connection, or create a new one. The SDP 'setup' attribute 'holdconn' value MUST NOT be used.

NOTE: A change of the TCP roles will also trigger a re-establishment of the DTLS association, according to the procedures in [I-D.ietf-mmusic-dtls-sdp].

NOTE: As specified in [I-D.ietf-mmusic-dtls-sdp], usage of the SDP 'setup' attribute 'holdconn' value is not allowed. Therefore this specification also forbids usage of the attribute value for TCP, as DTLS is transported on top of TCP.

## 10. SDP Offer/Answer Procedures

### 10.1. General

This section defines the SDP Offer/Answer [RFC3264] procedures for negotiating and establishing an SCTP-over-DTLS association. Unless explicitly stated, the procedures apply to both the 'UDP/DTLS/SCTP' and 'TCP/DTLS/SCTP' m- line proto values.

Each endpoint MUST associate one or more certificate fingerprints, using the SDP 'fingerprint' attribute with the m- line, following the procedures in [RFC4572] and [I-D.ietf-mmusic-4572-update].

The authentication certificates are interpreted and validated as defined in [RFC4572]. Self-signed certificates can be used securely, provided that the integrity of the SDP description is assured as defined in [RFC4572].

Each endpoint MUST associate an SDP 'dtls-id' attribute with the m- line, following the procedures in [I-D.ietf-mmusic-dtls-sdp].

### 10.2. Generating the Initial SDP Offer

When the offerer creates an initial offer, the offerer:

- o MUST associate an SDP setup attribute, with an 'actpass' value, with the m- line;

- o MUST associate an SDP 'sctp-port' attribute with the m- line;

- o MUST, in the case of TCP/DTLS/SCTP, associate an SDP 'connection' attribute, with a 'new' attribute value, with the m- line; and

- o MAY associate an SDP 'max-message-size' attribute (Section 6) with the m- line.

### 10.3. Generating the SDP Answer

When the answerer receives an offer, which contains an m- line describing an SCTP-over-DTLS association, if the answerer accepts the association line it:

- o MUST insert a corresponding m- line in the answer, with an identical m- line proto value [RFC3264];

- o MUST associate an SDP 'setup' attribute, with an 'active' or 'passive' value, with the m- line;

- o MUST associate an SDP 'sctp-port' attribute with the m- line. If the offer contained a new (different than the one currently used) SCTP port value the answerer MUST also associate a new SCTP port value. If the offer contained a zero SCTP port value the answerer MUST also associate a zero SCTP port value; and

- o MAY associate an SDP 'max-message-size' attribute (Section 6)with the m- line. The attribute value in the answer is independent from the value (if present) in the corresponding m- line of the offer.

Once the answerer has sent the answer the answerer MUST, if an SCTP association has yet not been established, or if an existing SCTP association is to be re-established, initiate the establishment of the SCTP association.

The answerer follows the procedures in [I-D.ietf-mmusic-dtls-sdp] regarding the establishment/re-establishment of the DTLS association.

In the case of TCP/DTLS/SCTP, the answerer follows the procedures in [RFC4145] regarding the establishment/re-establishment of the TCP connection association.

If the answerer does not accept the m- line in the offer, it MUST assign a zero port value to the corresponding m- line in the answer, following the procedures in [RFC3264]. In addition, the answerer MUST NOT initiate the establishment of an SCTP association, or a DTLS association, associated with the m- line.

### 10.4. Offerer Processing of the SDP Answer

Once the offerer has received the answer, which contains an m- line with a non-zero port value, the offerer MUST, if an SCTP association has yet not been established, or if an existing SCTP association is to be re-established, initiate the establishment of the SCTP association.

If the SDP 'sctp-port' attribute in the answer contains a zero attribute value, the offerer MUST NOT establish an SCTP association. If an SCTP association exists, the offerer MUST close it.

The offerer follows the procedures in [I-D.ietf-mmusic-dtls-sdp] regarding the establishment/re-establishment of the DTLS association.

In the case of TCP/DTLS/SCTP, the offerer follows the procedures in [RFC4145] regarding the establishment/re-establishment of the TCP connection association.

If the m- line in the answer contains a zero port value, the offerer MUST NOT establish a TCP connection, an SCTP association, or a DTLS association, associated with the m- line. If an SCTP association, DTLS association and/or TCP connection exists, the offerer MUST close it.

### 10.5. Modifying the Session

When an offerer sends an updated offer, in order to modify a previously established SCTP association, it follows the procedures in Section 10.2, with the following exceptions:

- If the offerer wants to close and immediately re-establish an existing SCTP association, the offerer MUST associate an SDP 'sctp-port' attribute with a new (different than the one currently used) attribute value. This will not impact the underlying DTLS association (and TCP connection in case of TCP/DTLS/SCTP).

- If the offerer wants to close, but not re-establish an existing SCTP association, the offerer MUST associate an SDP 'sctp-port' attribute with a zero attribute value. This will not impact the underlying DTLS association (and TCP connection in case of TCP/DTLS/SCTP).

- If the offerer wants to re-establish a previously closed SCTP association, the offerer MUST associate an SDP 'sctp-port' attribute with a new (different than the one currently used) attribute value. If the SCTP association was previously closed using an SDP 'sctp-port' attribute with a zero attribute value,

the offerer MAY use the same attribute value that was used prior to the SCTP association was closed. This will not impact the underlying DTLS association (and TCP connection in case of TCP/DTLS/SCTP).

- o If the offerer wants to close an existing SCTP association, and the underlying DTLS association (and the underlying TCP connection in case of TCP/DTLS/SCTP) it MUST assign a zero port value to the m- line associated with the SCTP and DTLS associations (and TCP connection in case of TCP/DTLS/SCTP), following the procedures in [RFC3264].

- o NOTE: This specification does not define a mechanism for explicitly closing an DTLS association while maintaining the overlying SCTP association. However, if a DTLS association is re-established as a result of some other action [I-D.ietf-mmusic-dtls-sdp] the SCTP association is not affected.

The offer follows the procedures in [I-D.ietf-mmusic-dtls-sdp] regarding the DTLS association impacts when modifying a session.

In the case of TCP/DTLS/SCTP, the offer follows the procedures in [RFC4145] regarding the TCP connection impacts when modifying a session;

## 11. Multihoming Considerations

Multihoming is not supported when sending SCTP on top of DTLS, as DTLS does not expose address management of the underlying transport protocols (UDP or TCP) to its upper layer.

## 12. NAT Considerations

### 12.1. General

When SCTP-over-DTLS is used in NAT environment, it relies on the NAT traversal procedures for the underlying transport protocol (UDP or TCP).

### 12.2. ICE Considerations

When SCTP-over-DTLS is used with UDP based ICE candidates as defined in [RFC5245] procedures for UDP/DTLS/SCTP, as defined in Section 7 are used.

When SCTP-over-DTLS is used with TCP based ICE candidates as defined in [RFC6544] procedures for TCP/DTLS/SCTP, as defined in Section 8 are used.

Implementations MUST treat all ICE candidate pairs associated with a an SCTP association on top of a DTLS association as part of the same DTLS association. Thus, there will only be one SCTP handshake and one DTLS handshake even if there are multiple valid candidate pairs, and shifting from one candidate pair to another will not impact the SCTP or DTLS associations. If new candidates are added, they will also be part of the same SCTP and DTLS associations. When transitioning between candidate pairs, different candidate pairs can be currently active in different directions and implementations MUST be ready to receive data on any of the candidates, even if this means sending and receiving data using UDP/DTLS/SCTP and TCP/DTLS/SCTP at the same time in different directions.

When an SDP offer or answer is sent, the proto value MUST match the transport protocol associated with the default candidate. Hence, if UDP transport is used for the default candidate the 'UDP/DTLS/SCTP' proto value MUST be used. If TCP transport is used for the default candidate the 'TCP/DTLS/SCTP' proto value MUST be used. However, if an endpoint switch between TCP-based and UDP-based candidates during a session the endpoint is not required to send an SDP offer in order to modify that proto value of the associated m- line.

NOTE: The text in the paragraph above only applies when the usage of ICE has been negotiated. If ICE is not used, the proto value MUST always reflect the transport protocol used at any given time.

## 13. Examples

### 13.1. Establishment of UDP/DTLS/SCTP association

SDP Offer:

```
m=application 54111 UDP/DTLS/SCTP webrtc-datachannel
c=IN IP4 192.0.2.1
a=dtls-id:abc3dl
a=setup:actpass
a=sctp-port:5000
a=max-message-size:100000
```

- The offerer indicates that the usage of the UDP/DTLS/SCTP association will be as defined for the 'webrtc-datachannel' format value.
- The offerer UDP port value is 54111.
- The offerer SCTP port value is 5000.
- The offerer indicates that it can take either the client or the server DTLS role.

SDP Answer:

```
m=application 64300 UDP/DTLS/SCTP webrtc-datachannel
c=IN IP4 192.0.2.2
a=dtls-id:ggr4rd
a=setup:passive
a=sctp-port:6000
a=max-message-size:100000
```

- The answerer UDP port value is 64300.
- The answerer SCTP port value is 6000.
- The answerer takes the server DTLS role.

## 14. Security Considerations

[RFC4566] defines general SDP security considerations, while [RFC3264], [RFC4145] and [RFC4572] define security considerations when using the SDP offer/answer mechanism to negotiate media streams.

[RFC4960] defines general SCTP security considerations and [I-D.ietf-tsvwg-sctp-dtls-encaps] defines security considerations when using SCTP on top of DTLS.

This specification does not introduce new security considerations in addition to those defined in the specifications listed above.

## 15. IANA Considerations

### 15.1. New SDP proto values

[RFC EDITOR NOTE: Please replace RFCXXXX with the RFC number of this document.]

This document updates the "Session Description Protocol (SDP) Parameters" registry, following the procedures in [RFC4566], by adding the following values to the table in the SDP "proto" field registry:

| Type | SDP Name | Reference |
|---|---|---|
| proto | UDP/DTLS/SCTP | [RFCXXXX] |
| proto | TCP/DTLS/SCTP | [RFCXXXX] |

Table 1: SDP "proto" field values

### 15.2. New SDP Attributes

#### 15.2.1. sctp-port

[RFC EDITOR NOTE: Please replace RFCXXXX with the RFC number of this document.]

This document defines a new SDP media-level attribute,'sctp-port', as follows:

```
Attribute name:     sctp-port
Type of attribute:  media
Mux category:       SPECIAL
Subject to charset: No
Purpose:            Indicate the SCTP port value associated
              with the SDP Media Description.
Appropriate values: Integer
Contact name:       Christer Holmberg
Contact e-mail:     christer.holmberg@ericsson.com
Reference:          RFCXXXX
```

### 15.2.2. max-message-size

[RFC EDITOR NOTE: Please replace RFCXXXX with the RFC number of this document.]

This document defines a new SDP media-level attribute,'max-message-size', as follows:

```
Attribute name:     max-message-size
Type of attribute:  media
Mux category:       SPECIAL
Subject to charset: No
Purpose:            Indicate the maximum message size that
                 an SCTP endpoint is willing to receive
                 on the SCTP association associated
                 with the SDP Media Description.
Appropriate values: Integer
Contact name:       Christer Holmberg
Contact e-mail:     christer.holmberg@ericsson.com
Reference:          RFCXXXX
```

## 15.3. association-usage Name Registry

[RFC EDITOR NOTE: Please replace RFCXXXX with the RFC number of this document.]

This specification creates a new IANA registry, following the procedures in [RFC5226], for the "fmt" namespace associated with the 'UDP/DTLS/SCTP' and 'TCP/DTLS/SCTP' protocol identifiers. Each "fmt" value describes the usage of an entire SCTP association, including all SCTP streams associated with the SCTP association.

NOTE: Usage indication of individual SCTP streams is outside the scope of this specification.

The "fmt" value, "association-usage", used with these "proto" is required. It is defined in [Section 4].

As part of this registry, IANA maintains the following information:

association-usage name: The identifier of the subprotocol, as will be used as the "fmt" value.

association-usage reference: A reference to the document in which the association-usage is defined.

association-usage names are to be subject to the "First Come First Served" IANA registration policy [RFC5226].

IANA is asked to add initial values to the registry.

| name | Reference |
|---|---|
| webrtc-datachannel | draft-ietf-rtcweb-data-protocol-xx |

[RFC EDITOR NOTE: Please hold the publication of this draft until draft-ietf-rtcweb-data-protocol has been published as an RFC. Then, replace the reference to draft-ietf-rtcweb-data-protocol with the RFC number.]

Figure 1

## 16. Acknowledgments

The authors wish to thank Harald Alvestrand, Randell Jesup, Paul Kyzivat, Michael Tuexen, Juergen Stoetzer-Bradler, Flemming Andreasen and Ari Keranen for their comments and useful feedback.

## 17.

[RFC EDITOR NOTE: Please remove this section when publishing]

Changes from draft-ietf-mmusic-sctp-sdp-17

- o Removal of 'SCTP'.
- o Document title changed.
- o Disallow usage of SDP 'setup' attribute 'holdconn' value.
- o Roman Shpount added as co-editor.

Changes from draft-ietf-mmusic-sctp-sdp-15

- o Chapter about SCTP, DTLS and TCP association/connection management modified.
- o Removal of SCTP/DTLS.

Changes from draft-ietf-mmusic-sctp-sdp-14

- Changes based on WGLC comments from Magnus Westerlund.
- - ABNF clarification that token and port are defined in RFC4566.
- - Specify 40 as maximum digit character length for the SDP max-message-size value.
- - Editorial clarification.
- Changes based on discussions at IETF#92.
- - Specify that all ICE candidate pairs belong to the same DTLS association.

Changes from draft-ietf-mmusic-sctp-sdp-13

- Changes based on comments from Paul Kyzivat.
- - Text preventing usage of well-known ports removed.
- - Editorial clarification.

Changes from draft-ietf-mmusic-sctp-sdp-12

- Mux category rules added for new SDP attributes.
- Reference to draft-ietf-mmusic-sdp-mux-attributes added.
- Changes based on comments from Roman Shpount:
- - Specify that fingerprint or setup roles must not be modified, unless underlying transport protocol is also modified.
- Changes based on comments from Ari Keranen:
- - Editorial corrections.
- Changes based on comments from Flemming Andreasen:
- - Clarify that, if UDP/DTLS/SCTP or TCP/DTLS/SCTP is used, the DTLS association is established before the SCTP association.
- - Clarify that max-message-size value is given in bytes, and that different values can be used per direction.
- - Section on fmtp attribute removed.
- - Editorial corrections.

Changes from draft-ietf-mmusic-sctp-sdp-11

o Example added.

Changes from draft-ietf-mmusic-sctp-sdp-10

o SDP max-message-size attribute added to IANA considerations.

o Changes based on comments from Paul Kyzivat:

o - Text about max message size removed from fmtp attribute section.

Changes from draft-ietf-mmusic-sctp-sdp-09

o 'DTLS/SCTP' split into 'UDP/DTLS/SCTP' and 'TCP/DTLS/SCTP'

o Procedures for realizing UDP/DTLS/SCTP- and TCP/DTLS/SCTP transports added.

Changes from draft-ietf-mmusic-sctp-sdp-08

o Default SCTP port removed:

o - Usage of SDP sctp-port attribute mandatory.

o SDP max-message-size attribute defined:

o - Attribute definition.

o - SDP Offer/Answer procedures.

o Text about SDP direction attributes added.

o Text about TLS role determination added.

## 18. References

### 18.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC3264] Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model with Session Description Protocol (SDP)", RFC 3264, DOI 10.17487/RFC3264, June 2002, <http://www.rfc-editor.org/info/rfc3264>.

[RFC4145] Yon, D. and G. Camarillo, "TCP-Based Media Transport in the Session Description Protocol (SDP)", RFC 4145, DOI 10.17487/RFC4145, September 2005, <http://www.rfc-editor.org/info/rfc4145>.

[RFC4289] Freed, N. and J. Klensin, "Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures", BCP 13, RFC 4289, DOI 10.17487/RFC4289, December 2005, <http://www.rfc-editor.org/info/rfc4289>.

[RFC4566] Handley, M., Jacobson, V., and C. Perkins, "SDP: Session Description Protocol", RFC 4566, DOI 10.17487/RFC4566, July 2006, <http://www.rfc-editor.org/info/rfc4566>.

[RFC4571] Lazzaro, J., "Framing Real-time Transport Protocol (RTP) and RTP Control Protocol (RTCP) Packets over Connection-Oriented Transport", RFC 4571, DOI 10.17487/RFC4571, July 2006, <http://www.rfc-editor.org/info/rfc4571>.

[RFC4572] Lennox, J., "Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP)", RFC 4572, DOI 10.17487/RFC4572, July 2006, <http://www.rfc-editor.org/info/rfc4572>.

[RFC4960] Stewart, R., Ed., "Stream Control Transmission Protocol", RFC 4960, DOI 10.17487/RFC4960, September 2007, <http://www.rfc-editor.org/info/rfc4960>.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, DOI 10.17487/RFC5226, May 2008, <http://www.rfc-editor.org/info/rfc5226>.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <http://www.rfc-editor.org/info/rfc5234>.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, DOI 10.17487/RFC6347, January 2012, <http://www.rfc-editor.org/info/rfc6347>.

[RFC6838] Freed, N., Klensin, J., and T. Hansen, "Media Type Specifications and Registration Procedures", BCP 13, RFC 6838, DOI 10.17487/RFC6838, January 2013, <http://www.rfc-editor.org/info/rfc6838>.

[I-D.ietf-mmusic-4572-update]
Holmberg, C., "SDP Fingerprint Attribute Usage Clarifications", draft-ietf-mmusic-4572-update-07 (work in progress), September 2016.

[I-D.ietf-mmusic-dtls-sdp]
Holmberg, C. and R. Shpount, "Using the SDP Offer/Answer Mechanism for DTLS", draft-ietf-mmusic-dtls-sdp-14 (work in progress), July 2016.

[I-D.ietf-tsvwg-sctp-dtls-encaps]
Tuexen, M., Stewart, R., Jesup, R., and S. Loreto, "DTLS Encapsulation of SCTP Packets", draft-ietf-tsvwg-sctp-dtls-encaps-09 (work in progress), January 2015.

[I-D.ietf-mmusic-sdp-mux-attributes]
Nandakumar, S., "A Framework for SDP Attributes when Multiplexing", draft-ietf-mmusic-sdp-mux-attributes-13 (work in progress), June 2016.

## 18.2. Informative References

[RFC0793] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, DOI 10.17487/RFC0793, September 1981, <http://www.rfc-editor.org/info/rfc793>.

[RFC5245] Rosenberg, J., "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols", RFC 5245, DOI 10.17487/RFC5245, April 2010, <http://www.rfc-editor.org/info/rfc5245>.

[RFC6083] Tuexen, M., Seggelmann, R., and E. Rescorla, "Datagram Transport Layer Security (DTLS) for Stream Control Transmission Protocol (SCTP)", RFC 6083, DOI 10.17487/RFC6083, January 2011, <http://www.rfc-editor.org/info/rfc6083>.

[RFC6544] Rosenberg, J., Keranen, A., Lowekamp, B., and A. Roach, "TCP Candidates with Interactive Connectivity Establishment (ICE)", RFC 6544, DOI 10.17487/RFC6544, March 2012, <http://www.rfc-editor.org/info/rfc6544>.

Authors' Addresses

Christer Holmberg
Ericsson
Hirsalantie 11
Jorvas 02420
Finland

Email: christer.holmberg@ericsson.com

Roman Shpount
TurboBridge
4905 Del Ray Avenue, Suite 300
Bethesda, MD 20814
USA

Phone: +1 (240) 292-6632
Email: rshpount@turbobridge.com

Salvatore Loreto
Ericsson
Hirsalantie 11
Jorvas 02420
Finland

Email: Salvatore.Loreto@ericsson.com

Gonzalo Camarillo
Ericsson
Hirsalantie 11
Jorvas 02420
Finland

Email: Gonzalo.Camarillo@ericsson.com