Internet Engineering Task Force (IETF)
Request for Comments: 8841
Category: Standards Track
ISSN: 2070-1721

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

January 2021

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

Abstract

The Stream Control Transmission Protocol (SCTP) is a transport protocol used to establish associations between two endpoints. RFC 8261 specifies how SCTP can be used on top of the Datagram Transport Layer Security (DTLS) protocol, which is 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

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8841.

Table of Contents

1. Introduction
2. Conventions
3. SCTP Terminology

4. SDP Media Descriptions
4.1. General
4.2. Protocol Identifiers
4.3. Media-Format Management
4.4. Syntax
4.4.1. General
4.4.2. SDP Media Description Values
4.5. Example
5. SDP "sctp-port" Attribute
5.1. General
5.2. Syntax
5.3. Mux Category
6. SDP "max-message-size" Attribute
6.1. General
6.2. Syntax
6.3. Mux Category
7. UDP/DTLS/SCTP Transport Realization
8. TCP/DTLS/SCTP Transport Realization
9. Association and Connection Management
9.1. General
9.2. SDP "sendrecv"/"sendonly"/"recvonly"/"inactive" Attributes
9.3. SCTP Association
9.4. DTLS Association (UDP/DTLS/SCTP and TCP/DTLS/SCTP)
9.5. TCP Connection (TCP/DTLS/SCTP)
10. SDP Offer/Answer Procedures
10.1. General
10.2. Generating the Initial SDP Offer
10.3. Generating the SDP Answer
10.4. Offerer Processing of the SDP Answer
10.5. Modifying the Session
11. Multihoming Considerations
12. NAT Considerations
12.1. General
12.2. ICE Considerations
13. Examples
13.1. Establishment of UDP/DTLS/SCTP Association
14. Security Considerations
15. IANA Considerations
15.1. New SDP Proto Values
15.2. New SDP Attributes
15.2.1. sctp-port
15.2.2. max-message-size
15.3. association-usage Name Registry
16. References
16.1. Normative References
16.2. Informative References
Acknowledgements
Authors' Addresses

1. Introduction

The Session Description Protocol (SDP) [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 the Session Description Protocol (SDP)" [RFC8122] extends [RFC4145] to describe TCP-based media streams that are protected using TLS.

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

[RFC8261] specifies how SCTP can be used on top of the Datagram

Transport Layer Security (DTLS) protocol, an arrangement referred to as SCTP-over-DTLS.

This specification defines the following new SDP [RFC4566] protocol identifiers (proto values): "UDP/DTLS/SCTP" and "TCP/DTLS/SCTP". This document also specifies how to use the new proto values with the SDP offer/answer mechanism [RFC3264] for negotiating SCTP-over-DTLS associations.

> NOTE: Due to the characteristics of TCP, while multiple SCTP streams can still be used, usage of "TCP/DTLS/SCTP" will always force ordered and reliable delivery of the SCTP packets, which limits the usage of the SCTP options. Therefore, it is RECOMMENDED that TCP is only used in situations where UDP traffic is blocked.

2. Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

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 associated SCTP endpoint to another, within which all user messages are delivered in sequence except for those submitted to the unordered delivery service.

SCTP-over-DTLS: SCTP used on top of DTLS, as specified in [RFC8261].

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]:

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.

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] states that specifications defining new proto values must define the rules by which their media format (fmt) namespace is managed.

An "m=" line with a proto value of "UDP/DTLS/SCTP" or "TCP/DTLS/SCTP" always describes a single SCTP association.

In addition, such an "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.

When the "UDP/DTLS/SCTP" and "TCP/DTLS/SCTP" proto values are used, the "m=" line fmt value, which identifies the application-layer protocol, MUST be registered by IANA. Section 15.3 defines the IANA registry for the media-format namespace.

> NOTE: A mechanism for how to describe and manage individual SCTP streams within an SCTP association is outside the scope of this specification. [RFC8864] defines a mechanism for negotiating individual SCTP streams used to realize WebRTC data channels [RFC8831].

4.4. Syntax

4.4.1. General

This section defines the values that can be used within an SDP media description ("m=" line) associated with an SCTP-over-DTLS association.

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

4.4.2. SDP Media Description Values

When the SCTP association is used to realize a WebRTC data channel [RFC8832], the <fmt> parameter value is ’webrtc-datachannel’.

"m=" line parameter	parameter value(s)
<media>	"application"
<proto>	"UDP/DTLS/SCTP" or "TCP/DTLS/SCTP"
<port>	UDP port number (for "UDP/DTLS/SCTP") TCP port number (for "TCP/DTLS/SCTP")
<fmt>	A string denoting the association-usage, limited to the syntax of a "token" as defined in RFC 4566

Table 1: SDP Media Description Values

4.5. Example

```
m=application 12345 UDP/DTLS/SCTP webrtc-datachannel
a=sctp-port:5000
a=max-message-size:100000
```

> | NOTE: "webrtc-datachannel" indicates the WebRTC Data Channel
> | Establishment Protocol defined in [RFC8832].

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.

> | NOTE: This specification only defines the usage of the SDP
> | "sctp-port" 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.

5.2. Syntax

The definition of the SDP "sctp-port" attribute is:

Attribute name: sctp-port

Type of attribute: media

Mux category: CAUTION

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: RFC 8841

Syntax:

```
sctp-port-value = 1*5(DIGIT) ; DIGIT defined in RFC 4566
```

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

Example:

```
a=sctp-port:5000
```

5.3. Mux Category

The mux category [RFC8859] for the SDP "sctp-port" attribute is CAUTION.

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 SCTP user 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.

An SCTP endpoint MUST NOT send a SCTP user message with a message size that is larger than the maximum size indicated by the peer, as it cannot be assumed that the peer would accept such a message.

If the SDP "max-message-size" attribute contains a maximum message size value of zero, it indicates that 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 definition of the SDP "max-message-size" attribute is:

Attribute name: max-message-size

Type of attribute: media

Mux category: CAUTION

Subject to charset: No

Purpose: Indicate the maximum message size (indicated in bytes) 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: RFC 8841

Syntax:

```
max-message-size-value = 1*DIGIT ; DIGIT defined in RFC 4566
```

Leading zeroes MUST NOT be used.

Example:

```
a=max-message-size:100000
```

6.3. Mux Category

The mux category for the SDP "max-message-size" attribute is CAUTION.

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:

* SCTP on top of DTLS is realized according to the procedures defined in [RFC8261]; and

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

> | NOTE: While [RFC8261] allows multiple SCTP associations on top of a single DTLS association, the procedures in this specification only support 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:

* SCTP on top of DTLS is realized according to the procedures defined in [RFC8261]; and

* DTLS on top of TCP is realized using the framing method defined in [RFC4571], with DTLS packets being sent and received instead of RTP/RTCP packets using the shim defined in [RFC4571]. The length field defined in [RFC4571] precedes each DTLS message, and SDP signaling is done according to the procedures defined in this specification.

> | NOTE: TLS 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 manage an SCTP association, DTLS association, and TCP connection using SDP attributes.

The SCTP association, the DTLS association, and the TCP connection are managed independently from each other. Each can be established and closed without impacting others.

The detailed SDP offer/answer [RFC3264] procedures for the SDP attributes are described in Section 10.

9.2. SDP "sendrecv"/"sendonly"/"recvonly"/"inactive" Attributes

This specification does not define semantics for the SDP direction

attributes [RFC4566]. Unless the semantics of these attributes for an SCTP association usage have been defined, SDP direction attributes MUST be ignored if present.

9.3. SCTP Association

When an SCTP association is established, both SCTP endpoints MUST initiate the SCTP association (i.e., both SCTP endpoints take the "active" role). In addition, both endpoints 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, the SDP "setup" attribute [RFC4145] does not apply to SCTP association establishment. However, the "setup" attribute does apply to establishment of the underlying DTLS association and TCP connection.

> 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: When the SCTP association is established, it is assumed that any NAT traversal procedures for the underlying transport protocol (UDP or TCP) have successfully been performed.

The SDP "connection" attribute [RFC4145] does not apply to the SCTP association. In order to trigger the closure of an existing SCTP association and establishment of a new SCTP association, the SDP "sctp-port" attribute (Section 5) is used to indicate a new (different than the ones currently used) SCTP port. The existing SCTP association is closed, and the new SCTP association is established, if one or both endpoints signal a new SCTP port. The "connection" attribute does apply to establishment of underlying TCP connections.

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

SCTP associations might be closed without SDP signaling -- for example, in case of a failure. The procedures in this section MUST be followed to establish a new SCTP association. This requires a new SDP offer/answer exchange. New (different than the ones currently used) SCTP ports MUST be used by both endpoints.

> NOTE: Closing and establishing a new SCTP association using the SDP "sctp-port" attribute will not affect the state of the underlying DTLS association.

9.4. DTLS Association (UDP/DTLS/SCTP and TCP/DTLS/SCTP)

A DTLS association is managed according to the procedures in [RFC8842]. Hence, the SDP "setup" attribute is used to negotiate the (D)TLS roles ("client" and "server") [RFC8122].

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

> NOTE: As described in [RFC8445], if the Interactive Connectivity Establishment (ICE) mechanism [RFC8445] is used, all ICE candidates associated with a DTLS association are 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 closure of the DTLS association and establishment of a new DTLS association, according to the procedures in [RFC8842].

> NOTE: As specified in [RFC8842], 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 [RFC8122].

The authentication certificates are interpreted and validated as defined in [RFC8122]. Self-signed certificates can be used securely, provided that the integrity of the SDP description is assured, as defined in [RFC8122].

Each endpoint MUST associate an SDP "tls-id" attribute with the "m=" line, following the procedures in [RFC8842].

10.2. Generating the Initial SDP Offer

When the offerer creates an initial offer, the offerer:

* MUST associate an SDP "setup" attribute with the "m=" line;
* MUST associate an SDP "sctp-port" attribute with the "m=" line;
* MUST, in the case of TCP/DTLS/SCTP, associate an SDP "connection" attribute, with a "new" attribute value, with the "m=" line; and
* 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 that contains an "m=" line describing an SCTP-over-DTLS association, if the answerer accepts the association, the answerer:

* MUST insert a corresponding "m=" line in the answer, with an "m=" line proto value [RFC3264] identical to the value in the offer;
* MUST associate an SDP "setup" attribute with the "m=" line;
* 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, or if the answerer does not accept the SCTP association, the answerer MUST also associate a zero SCTP port value; and

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

Once the answerer has sent the answer:

* in the case of TCP/DTLS/SCTP, if a TCP connection has not yet been established or an existing TCP connection is to be closed and replaced by a new one, the answerer MUST follow the procedures in [RFC4145] for closing and establishing a TCP connection;

* if a DTLS association has not yet been established or an existing DTLS association is to be closed and replaced by a new one, the answerer MUST follow the procedures in [RFC8842] for closing the currently used DTLS association and establishing a new one; and

* if an SCTP association has not yet been established or an existing SCTP association is to be closed and replaced by a new one, the answerer MUST initiate the closing of the existing SCTP association (if applicable) and establishment of the new association.

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

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 a TCP connection, a DTLS 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:

* in the case of TCP/DTLS/SCTP, if a TCP connection has not yet been established or an existing TCP connection is to be closed and replaced by a new one, the offerer MUST follow the procedures in [RFC4145] for closing and establishing a TCP connection;

* if a DTLS association has not yet been established or an existing DTLS association is to be closed and replaced by a new one, the offerer MUST follow the procedures in [RFC8842] for closing and establishing a DTLS association; and

* if an SCTP association has not yet been established or an existing SCTP association is to be closed and replaced by a new one, the offerer MUST initiate the closing of the existing SCTP association (if applicable) and establishment of the new association.

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

If the "m=" line in the answer contains a zero port value, the offerer MUST NOT initiate the establishment of a TCP connection, a

DTLS association, or an SCTP association associated with the "m=" line. If, in addition, a TCP connection, DTLS association, or SCTP association 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 an SCTP association and immediately establish a new SCTP association, it 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 (or TCP connection, in the case of TCP/DTLS/SCTP).

* If the offerer wants to close an SCTP association without immediately establishing a new SCTP association, it MUST associate an SDP "sctp-port" attribute with an attribute value of zero. This will not impact the underlying DTLS association (or TCP connection, in the case of TCP/DTLS/SCTP).

* If the offerer wants to establish an SCTP association, and another SCTP association was previously closed, the offerer MUST associate an SDP "sctp-port" attribute with a new attribute value (different than the value associated with the previous SCTP association). If the previous SCTP association was closed successfully following use of an SDP "sctp-port" attribute with an attribute value of zero, the offerer MAY use the same attribute value for the new SCTP association that was used with the previous SCTP association before it was closed. This will not impact the underlying DTLS association (or TCP connection, in the case of TCP/DTLS/SCTP).

* If the offerer wants to close an existing SCTP association and the underlying DTLS association (and the underlying TCP connection, in the 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 the case of TCP/DTLS/SCTP), following the procedures in [RFC3264].

* NOTE: This specification does not define a mechanism for explicitly closing a DTLS association while maintaining the overlying SCTP association. However, if a DTLS association is closed and replaced with a new DTLS association as a result of some other action [RFC8842], the state of the SCTP association is not affected.

The offerer follows the procedures in [RFC8842] regarding the DTLS association impacts when modifying a session.

In the case of TCP/DTLS/SCTP, the offerer 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 a 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 [RFC8445], then the procedures for UDP/DTLS/SCTP (Section 7) are used.

When SCTP-over-DTLS is used with TCP-based ICE candidates [RFC6544], then the procedures for TCP/DTLS/SCTP (Section 8) are used.

In ICE environments, during the nomination process, endpoints go through multiple ICE candidate pairs until the most preferred candidate pair is found. During the nomination process, data can be sent as soon as the first working candidate pair is found, but the nomination process still continues, and selected candidate pairs can still change while data is sent. Furthermore, if endpoints roam between networks -- for instance, when a mobile endpoint switches from mobile connection to WiFi -- endpoints will initiate an ICE restart. This will trigger a new nomination process between the new set of candidates, which will likely result in the new nominated candidate pair.

Implementations MUST treat all ICE candidate pairs associated with 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; shifting from one candidate pair to another, including switching between UDP and TCP candidate pairs, 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.

In order to maximize the likelihood of interoperability between the endpoints, all ICE-enabled SCTP-over-DTLS endpoints SHOULD implement support for UDP/DTLS/SCTP.

When an SDP offer or answer is sent with multiple ICE candidates during initial connection negotiation or after ICE restart, UDP-based candidates SHOULD be included, and the default candidate SHOULD be chosen from one of those UDP candidates. The proto value MUST match the transport protocol associated with the default candidate. If UDP transport is used for the default candidate, then the "UDP/DTLS/SCTP" proto value MUST be used. If TCP transport is used for the default candidate, then the "TCP/DTLS/SCTP" proto value MUST be used. Note that under normal circumstances, the proto value for offers and answers sent during ICE nomination SHOULD be "UDP/DTLS/SCTP".

When a subsequent SDP offer or answer is sent after ICE nomination is complete, and it does not initiate ICE restart, it will contain only the nominated ICE candidate pair. In this case, the proto value MUST match the transport protocol associated with the nominated ICE candidate pair. If UDP transport is used for the nominated pair, then the "UDP/DTLS/SCTP" proto value MUST be used. If TCP transport is used for the nominated pair, then the "TCP/DTLS/SCTP" proto value MUST be used. Please note that if an endpoint switches between TCP-based and UDP-based candidates during the nomination process, the endpoint is not required to send an SDP offer for the sole purpose of keeping the proto value of the associated "m=" line in sync.

> | 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 IP6 2001:DB8::A8FD
a=tls-id:abc3de65cddef001be82
a=setup:actpass
a=fingerprint:SHA-256 \
12:DF:3E:5D:49:6B:19:E5:7C:AB:4A:AD:B9:B1:3F:82:18:3B:54:02:12:DF: \
3E:5D:49:6B:19:E5:7C:AB:4A:AD
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 IP6 2001:DB8::001D
a=tls-id:dbc8de77cddef001be90
a=setup:passive
a=fingerprint:SHA-256 \
3F:82:18:3B:49:6B:19:E5:7C:AB:4A:AD:B9:B1:12:DF:3E:5D:12:DF:54:02: \
49:6B:3E:5D:7C:AB:19:E5:AD:4A
a=sctp-port:6000
a=max-message-size:100000
```

Note that due to RFC formatting conventions, this document splits SDP across lines whose content would exceed 72 characters. A backslash character marks where this line folding has taken place. This backslash and its trailing CRLF and whitespace would not appear in actual SDP content.

* 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 [RFC8122] define security considerations when using the SDP offer/answer mechanism to negotiate media streams.

[RFC4960] defines general SCTP security considerations, and [RFC8261] 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

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	RFC 8841
proto	TCP/DTLS/SCTP	RFC 8841

Table 2: SDP "proto" Field Values

15.2. New SDP Attributes

15.2.1. sctp-port

This document defines a new SDP media-level attribute,"sctp-port". The details of the attribute are defined in Section 5.2.

15.2.2. max-message-size

This document defines a new SDP media-level attribute,"max-message-size". The details of the attribute are defined in Section 6.2.

15.3. association-usage Name Registry

Per this specification, a new IANA registry has been created, following the procedures in [RFC8126], for the 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" values 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 [RFC8126].

IANA has added the following initial values to the registry.

Name	Reference
webrtc-datachannel	RFC 8832, RFC 8841

Table 3: IANA Initial Values

16. References

16.1. Normative References

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

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://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, <https://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, <https://www.rfc-editor.org/info/rfc4145>.

[RFC4566] Handley, M., Jacobson, V., and C. Perkins, "SDP: Session Description Protocol", RFC 4566, DOI 10.17487/RFC4566, July 2006, <https://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, <https://www.rfc-editor.org/info/rfc4571>.

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

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

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

[RFC8122] Lennox, J. and C. Holmberg, "Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP)", RFC 8122, DOI 10.17487/RFC8122, March 2017, <https://www.rfc-editor.org/info/rfc8122>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8261] Tuexen, M., Stewart, R., Jesup, R., and S. Loreto, "Datagram Transport Layer Security (DTLS) Encapsulation of SCTP Packets", RFC 8261, DOI 10.17487/RFC8261, November 2017, <https://www.rfc-editor.org/info/rfc8261>.

[RFC8842] Holmberg, C. and R. Shpount, "Session Description Protocol

(SDP) Offer/Answer Considerations for Datagram Transport Layer Security (DTLS) and Transport Layer Security (TLS)", RFC 8842, DOI 10.17487/RFC8842, January 2021, <https://www.rfc-editor.org/info/rfc8842>.

[RFC8859] Nandakumar, S., "A Framework for Session Description Protocol (SDP) Attributes When Multiplexing", RFC 8859, DOI 10.17487/RFC8859, January 2021, <https://www.rfc-editor.org/info/rfc8859>.

16.2. Informative References

[RFC8445] Keranen, A., Holmberg, C., and J. Rosenberg, "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal", RFC 8445, DOI 10.17487/RFC8445, July 2018, <https://www.rfc-editor.org/info/rfc8445>.

[RFC8831] Jesup, R., Loreto, S., and M. Txen, "WebRTC Data Channels", RFC 8831, DOI 10.17487/RFC8831, January 2021, <https://www.rfc-editor.org/info/rfc8831>.

[RFC8832] Jesup, R., Loreto, S., and M. Txen, "WebRTC Data Channel Establishment Protocol", RFC 8832, DOI 10.17487/RFC8832, January 2021, <https://www.rfc-editor.org/info/rfc8832>.

[RFC8864] Drage, K., Makaraju, M., Ejzak, R., Marcon, J., and R. Even, Ed., "Negotiation Data Channels Using the Session Description Protocol (SDP)", RFC 8864, DOI 10.17487/RFC8864, January 2021, <https://www.rfc-editor.org/info/rfc8864>.

Acknowledgements

The authors wish to thank Harald Alvestrand, Randell Jesup, Paul Kyzivat, Michael Txen, Juergen Stoetzer-Bradler, Flemming Andreasen, and Ari Kernen for their comments and useful feedback. Ben Campbell provided comments as part of his Area Director review. Brian Carpenter performed the Gen-ART review.

Authors' Addresses

Christer Holmberg
Ericsson
Hirsalantie 11
FI-02420 Jorvas
Finland

Email: christer.holmberg@ericsson.com

Roman Shpount
TurboBridge
4905 Del Ray Avenue, Suite 300
Bethesda, MD 20814
United States of America

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

Salvatore Loreto
Ericsson
Grnlandsgatan 31
Kista
Sweden

Email: Salvatore.Loreto@ericsson.com

Gonzalo Camarillo
Ericsson
Hirsalantie 11
FI-02420 Jorvas
Finland

Email: Gonzalo.Camarillo@ericsson.com