Internet Engineering Task Force (IETF)
Request for Comments: 8842
Updates: 5763, 7345
Category: Standards Track
ISSN: 2070-1721

C. Holmberg
Ericsson
R. Shpount
TurboBridge

January 2021

Session Description Protocol (SDP) Offer/Answer Considerations for Datagram Transport Layer Security (DTLS) and Transport Layer Security (TLS)

Abstract

This document defines the Session Description Protocol (SDP) offer/answer procedures for negotiating and establishing a Datagram Transport Layer Security (DTLS) association. The document also defines the criteria for when a new DTLS association must be established. The document updates RFCs 5763 and 7345 by replacing common SDP offer/answer procedures with a reference to this specification.

This document defines a new SDP media-level attribute, "tls-id".

This document also defines how the "tls-id" attribute can be used for negotiating and establishing a Transport Layer Security (TLS) connection, in conjunction with the procedures in RFCs 4145 and 8122.

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/rfc8842.

Table of Contents

1. Introduction

[RFC5763] defines Session Description Protocol (SDP) offer/answer procedures for Secure Real-time Transport Protocol using Datagram Transport Layer Security (DTLS-SRTP). [RFC7345] defines SDP offer/answer procedures for UDP Transport Layer over Datagram Transport Layer Security (UDPTL-DTLS). This specification defines general offer/answer procedures for DTLS, based on the procedures in [RFC5763]. Other specifications, defining specific DTLS usages, can then reference this specification, in order to ensure that the DTLS aspects are common among all usages. Having common procedures is essential when multiple usages share the same DTLS association [RFC8843]. This document updates [RFC5763] and [RFC7345] by replacing common SDP offer/answer procedures with a reference to this specification.

> NOTE: Since the publication of [RFC5763], [RFC4474] has been obsoleted by [RFC8224]. The updating of the references (and the associated procedures) within [RFC5763] is outside the scope of this document. However, implementers of [RFC5763] applications are encouraged to implement [RFC8224] instead of [RFC4474].

As defined in [RFC5763], a new DTLS association MUST be established when transport parameters are changed. Transport parameter change is not well defined when Interactive Connectivity Establishment (ICE) [RFC8445] is used. One possible way to determine a transport change is based on ufrag [RFC8445] change, but the ufrag value is changed both when ICE is negotiated and when ICE restart [RFC8445] occurs. These events do not always require a new DTLS association to be established, but previously there was no way to explicitly indicate in an SDP offer or answer whether a new DTLS association was required. To solve that problem, this document defines a new SDP attribute, "tls-id". The pair of SDP "tls-id" attribute values (the attribute values of the offerer and the answerer) uniquely identifies

the DTLS association. Providing a new value of the "tls-id" attribute in an SDP offer or answer can be used to indicate whether a new DTLS association is to be established.

The SDP "tls-id" attribute can be specified when negotiating a Transport Layer Security (TLS) connection, using the procedures in this document in conjunction with the procedures in [RFC5763] and [RFC8122]. The unique combination of SDP "tls-id" attribute values can be used to identify the negotiated TLS connection. The unique value can be used, for example, within TLS protocol extensions to differentiate between multiple TLS connections and correlate those connections with specific offer/answer exchanges. The TLS-specific considerations are described in Section 7.

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. Establishing a New DTLS Association

3.1. General

A new DTLS association must be established between two endpoints after a successful SDP offer/answer exchange in the following cases:

* The negotiated DTLS setup roles change; or

* One or more fingerprint values are modified, added, or removed in either an SDP offer or answer; or

* The intent to establish a new DTLS association is explicitly signaled using SDP, by changing the value of the SDP "tls-id" attribute defined in this document;

  | NOTE: The first two items above are based on the procedures in [RFC5763]. This specification adds the support for explicit signaling using the SDP "tls-id" attribute.

A new DTLS association can only be established as a result of the successful SDP offer/answer exchange. Whenever an entity determines that a new DTLS association is required, the entity MUST initiate an SDP offer/answer exchange, following the procedures in Section 5.

The sections below describe typical cases where a new DTLS association needs to be established.

In this document, a "new DTLS association" between two endpoints refers to either an initial DTLS association (when no DTLS association is currently established between the endpoints) or a DTLS association replacing a previously established one.

3.2. Change of Local Transport Parameters

If an endpoint modifies its local transport parameters (address and/or port), and if the modification requires a new DTLS association, the endpoint MUST change its local SDP "tls-id" attribute value (see Section 4).

If the underlying transport protocol prohibits a DTLS association from spanning multiple 5-tuples (transport/source address/source port/destination address/destination port), and if the 5-tuple is changed, the endpoint MUST change its local SDP "tls-id" attribute

value (see Section 4). An example of such a case is when DTLS is carried over the Stream Control Transmission Protocol (SCTP), as described in [RFC6083].

3.3. Change of ICE ufrag Value

If an endpoint uses ICE and modifies a local ufrag value, and if the modification requires a new DTLS association, the endpoint MUST change its local SDP "tls-id" attribute value (see Section 4).

4. SDP "tls-id" Attribute

The pair of SDP "tls-id" attribute values (the attribute values of the offerer and the answerer) uniquely identifies the DTLS association or TLS connection.

Name: tls-id

Value: tls-id-value

Usage Level: media

Charset Dependent: no

Default Value: N/A

Syntax:

```
tls-id-value = 20*255(tls-id-char)
tls-id-char = ALPHA / DIGIT / "+" / "/" / "-" / "_"

<ALPHA and DIGIT defined in RFC 4566>
```

Example:

```
a=tls-id:abc3de65cddef001be82
```

Every time an endpoint requests to establish a new DTLS association, the endpoint MUST generate a new local "tls-id" attribute value. An unchanged local "tls-id" attribute value, in combination with non-changed fingerprints, indicates that the endpoint intends to reuse the existing DTLS association.

The "tls-id" attribute value MUST be generated using a strong random function and include at least 120 bits of randomness.

No default value is defined for the SDP "tls-id" attribute. Implementations that wish to use the attribute MUST explicitly include it in SDP offers and answers. If an offer or answer does not contain a "tls-id" attribute (this could happen if the offerer or answerer represents an existing implementation that has not been updated to support the "tls-id" attribute), a modification of one or more of the following characteristics MUST be treated as an indication that an endpoint wants to establish a new DTLS association, unless there is another mechanism to explicitly indicate that a new DTLS association is to be established:

* DTLS setup role; or

* fingerprint set; or

* local transport parameters

> | NOTE: A modification of the ufrag value is not treated as an indication that an endpoint wants to establish a new DTLS association. In order to indicate that a new DTLS association is to be established, one or more of the characteristics listed above have to be modified.

The mux category [RFC8859] for the "tls-id" attribute is "IDENTICAL", which means that the attribute value applies to all media descriptions being multiplexed [RFC8843]. However, as described in [RFC8843], in order to avoid duplication, the attribute is only associated with the "m=" line representing the offerer/answerer BUNDLE tag.

For RTP-based media, the "tls-id" attribute applies to the whole associated media description. The attribute MUST NOT be defined per source (using the SDP "ssrc" attribute [RFC5576]).

The SDP offer/answer procedures [RFC3264] associated with the attribute are defined in Section 5.

5. SDP Offer/Answer Procedures

5.1. General

This section defines the generic SDP offer/answer procedures for negotiating a DTLS association. Additional procedures (e.g., regarding usage of specific SDP attributes) for individual DTLS usages (e.g., DTLS-SRTP) are outside the scope of this specification and need to be specified in a usage-specific document.

> NOTE: The procedures in this section are generalizations of procedures first specified in the DTLS-SRTP document [RFC5763], with the addition of usage of the SDP "tls-id" attribute. That document is herein updated to make use of these new procedures.

The procedures in this section apply to an SDP media description ("m=" line) associated with DTLS-protected media/data.

When an offerer or answerer indicates that it wants to establish a new DTLS association, it needs to make sure that media packets associated with any previously established DTLS association and the new DTLS association can be demultiplexed. In the case of an ordered transport (e.g., SCTP), this can be done simply by sending packets for the new DTLS association after all packets associated with a previously established DTLS association have been sent. In the case of an unordered transport, such as UDP, packets associated with a previously established DTLS association can arrive after the answer SDP and the first packets associated with the new DTLS association have been received. The only way to demultiplex packets associated with a previously established DTLS association and the new DTLS association is on the basis of the 5-tuple. Because of this, if an unordered transport is used for the DTLS association, a new 3-tuple (transport/source address/source port) MUST be allocated by at least one of the endpoints so that DTLS packets can be demultiplexed.

When an offerer needs to establish a new DTLS association, and if an unordered transport (e.g., UDP) is used, the offerer MUST allocate a new 3-tuple for the offer in such a way that the offerer can disambiguate any packets associated with the new DTLS association from any packets associated with any other DTLS association. This typically means using a local address and/or port, or a set of ICE candidates (see Section 6), which were not recently used for any other DTLS association.

When an answerer needs to establish a new DTLS association, if an unordered transport is used, and the offerer did not allocate a new 3-tuple, the answerer MUST allocate a new 3-tuple for the answer in such a way that it can disambiguate any packets associated with the new DTLS association from any packets associated with any other DTLS association. This typically means using a local address and/or port, or a set of ICE candidates (see Section 6), which were not recently

used for any other DTLS association.

In order to negotiate a DTLS association, the following SDP attributes are used:

* The SDP "setup" attribute, defined in [RFC4145], is used to negotiate the DTLS roles;

* The SDP "fingerprint" attribute, defined in [RFC8122], is used to provide one or more fingerprint values; and

* The SDP "tls-id" attribute, defined in this specification, is used to identity the DTLS association.

This specification does not define the usage of the SDP "connection" attribute [RFC4145] for negotiating a DTLS association. However, the attribute MAY be used if the DTLS association is used together with another protocol (e.g., SCTP or TCP) for which the usage of the attribute has been defined.

Unlike for TCP and TLS connections, endpoints MUST NOT use the SDP "setup" attribute "holdconn" value when negotiating a DTLS association.

Endpoints MUST support the hash functions as defined in [RFC8122].

The certificate received during the DTLS handshake [RFC6347] MUST match a certificate fingerprint received in SDP "fingerprint" attributes according to the procedures defined in [RFC8122]. If fingerprints do not match the hashed certificate, then an endpoint MUST tear down the media session immediately (see [RFC8122]).

SDP offerers and answerers might reuse certificates across multiple DTLS associations, and provide identical fingerprint values for each DTLS association. The combination of the SDP "tls-id" attribute values of the SDP offerer and answerer identifies each individual DTLS association.

> NOTE: There are cases where the SDP "tls-id" attribute value generated by the offerer will end up being used for multiple DTLS associations. For that reason, the combination of the attribute values of the offerer and answerer is needed in order to identity a DTLS association. An example of such a case is where the offerer sends an updated offer (Section 5.5) without modifying its attribute value, but the answerer determines that a new DTLS association is to be created. The answerer will generate a new local attribute value for the new DTLS association (Section 5.3), while the offerer will use the same attribute value that it used for the current association. Another example is when the Session Initiation Protocol (SIP) [RFC3261] is used for signaling, and an offer is forked to multiple answerers. The attribute value generated by the offerer will be used for DTLS associations established by each answerer.

5.2. Generating the Initial SDP Offer

When an offerer sends the initial offer, the offerer MUST insert an SDP "setup" attribute [RFC4145] with an "actpass" attribute value, as well as one or more SDP "fingerprint" attributes according to the procedures in [RFC8122]. In addition, the offerer MUST insert in the offer an SDP "tls-id" attribute with a unique attribute value.

As the offerer inserts the SDP "setup" attribute with an "actpass" attribute value, the offerer MUST be prepared to receive a DTLS ClientHello message [RFC6347] from the answerer (if a new DTLS

association is established by the answerer) before the offerer receives the SDP answer.

If the offerer receives a DTLS ClientHello message, and a DTLS association is established before the offerer receives the SDP answer carrying the fingerprint associated with the DTLS association, any data received on the DTLS association before the fingerprint MUST be considered to be coming from an unverified source. The processing of such data and sending of data by the offerer to the unverified source is outside the scope of this document.

5.3. Generating the Answer

When an answerer sends an answer, the answerer MUST insert in the answer an SDP "setup" attribute according to the procedures in [RFC4145] and one or more SDP "fingerprint" attributes according to the procedures in [RFC8122]. If the answerer determines, based on the criteria specified in Section 3.1, that a new DTLS association is to be established, the answerer MUST insert in the associated answer an SDP "tls-id" attribute with a new unique attribute value. Note that the offerer and answerer generate their own local "tls-id" attribute values, and the combination of both values identifies the DTLS association.

If the answerer receives an offer that requires establishment of a new DTLS association, and if the answerer does not accept the establishment of a new DTLS association, the answerer MUST reject the "m=" lines associated with the suggested DTLS association [RFC3264].

If an answerer receives an offer that does not require the establishment of a new DTLS association, and if the answerer determines that a new DTLS association is not to be established, the answerer MUST insert in the associated answer an SDP "tls-id" attribute with the previously assigned attribute value. In addition, the answerer MUST insert an SDP "setup" attribute with an attribute value that does not change the previously negotiated DTLS roles, as well as one or more SDP "fingerprint" attributes values that do not change the previously sent fingerprint set, in the associated answer.

If the answerer receives an offer that does not contain an SDP "tls-id" attribute, the answerer MUST NOT insert a "tls-id" attribute in the answer.

If a new DTLS association is to be established, and if the answerer inserts an SDP "setup" attribute with an "active" attribute value in the answer, the answerer MUST initiate a DTLS handshake [RFC6347] by sending a DTLS ClientHello message towards the offerer.

Even though an offerer is required to insert an "SDP" setup attribute with an "actpass" attribute value in initial offers (Section 5.2) and subsequent offers (Section 5.5), the answerer MUST be able to receive initial and subsequent offers with other attribute values, in order to be backward compatible with older implementations that might insert other attribute values in initial and subsequent offers.

5.4. Offerer Processing of the SDP Answer

When an offerer receives an answer that establishes a new DTLS association based on criteria defined in Section 3.1, if the offerer becomes DTLS client (based on the value of the SDP "setup" attribute value [RFC4145]), the offerer MUST establish a DTLS association. If the offerer becomes DTLS server, it MUST wait for the answerer to establish the DTLS association.

If the offerer indicated a desire to reuse an existing DTLS association, and the answerer does not request the establishment of a

new DTLS association, the offerer will continue to use the previously established DTLS association.

A new DTLS association can be established based on changes in either an SDP offer or answer. When communicating with legacy endpoints, an offerer can receive an answer that includes the same fingerprint set and setup role. A new DTLS association will still be established if such an answer is received as a response to an offer that requested the establishment of a new DTLS association, as the transport parameters would have been changed in the offer.

5.5. Modifying the Session

When an offerer sends a subsequent offer, if the offerer wants to establish a new DTLS association, the offerer MUST insert an SDP "setup" attribute [RFC4145] with an "actpass" attribute value, as well as or more SDP "fingerprint" attributes according to the procedures in [RFC8122]. In addition, the offerer MUST insert in the offer an SDP "tls-id" attribute with a new unique attribute value.

When an offerer sends a subsequent offer and does not want to establish a new DTLS association, if a previously established DTLS association exists, the offerer MUST insert in the offer an SDP "setup" attribute with an "actpass" attribute value, and one or more SDP "fingerprint" attributes with attribute values that do not change the previously sent fingerprint set. In addition, the offerer MUST insert an SDP "tls-id" attribute with the previously assigned attribute value in the offer.

> NOTE: When a new DTLS association is being established, each endpoint needs to be prepared to receive data on both the new and old DTLS associations as long as both are alive.

6. ICE Considerations

When the Interactive Connectivity Establishment (ICE) mechanism [RFC8445] is used, the ICE connectivity checks are performed before the DTLS handshake begins. Note that if aggressive nomination mode is used, multiple candidate pairs may be marked valid before ICE finally converges on a single candidate pair.

> NOTE: Aggressive nomination has been deprecated from ICE but must still be supported for backwards compatibility reasons [RFC8445].

When a new DTLS association is established over an unordered transport, in order to disambiguate any packets associated with the newly established DTLS association, at least one of the endpoints MUST allocate a completely new set of ICE candidates that were not recently used for any other DTLS association. This means the answerer cannot initiate a new DTLS association unless the offerer initiated ICE restart [RFC8445]. If the answerer wants to initiate a new DTLS association, it needs to initiate an ICE restart and a new offer/answer exchange on its own. However, an ICE restart does not by default require a new DTLS association to be established.

> NOTE: Simple Traversal of the UDP Protocol through NAT (STUN) packets are sent directly over UDP, not over DTLS. [RFC7983] describes how to demultiplex STUN packets from DTLS packets and SRTP packets.

Each ICE candidate associated with a component is treated as being part of the same DTLS association. Therefore, from a DTLS perspective, it is not considered a change of local transport parameters when an endpoint switches between those ICE candidates.

7. TLS Considerations

The procedures in this document can also be used for negotiating and establishing a TLS connection, with the restriction described below.

As specified in [RFC4145], the SDP "connection" attribute is used to indicate whether to establish a new TLS connection. An offerer and answerer MUST ensure that the "connection" attribute value and the "tls-id" attribute value do not cause a conflict regarding whether a new TLS connection is to be established or not.

> NOTE: Even though the SDP "connection" attribute can be used to indicate whether a new TLS connection is to be established, the unique combination of SDP "tls-id" attribute values can be used to identity a TLS connection. The unique value can be used e.g., within TLS protocol extensions to differentiate between multiple TLS connections and correlate those connections with specific offer/answer exchanges. One such extension is defined in [RFC8844].

If an offerer or answerer inserts an SDP "connection" attribute with a "new" value in the offer/answer and also inserts an SDP "tls-id" attribute, the value of the "tls-id" attribute MUST be new and unique.

If an offerer or answerer inserts an SDP "connection" attribute with an "existing" value in the offer/answer, if a previously established TLS connection exists, and if the offerer/answerer previously inserted an SDP "tls-id" attribute associated with the same TLS connection in an offer/answer, the offerer/answerer MUST also insert an SDP "tls-id" attribute with the previously assigned value in the offer/answer.

If an offerer or answerer receives an offer/answer with conflicting attribute values, the offerer/answerer MUST process the offer/answer as misformed.

An endpoint MUST NOT make assumptions regarding the support of the SDP "tls-id" attribute by the peer. Therefore, to avoid ambiguity, both offerers and answerers MUST always use the "connection" attribute in conjunction with the "tls-id" attribute.

> NOTE: As defined in [RFC4145], if the SDP "connection" attribute is not explicitly present, the implicit default value is "new".

The SDP example below is based on the example in Section 3.4 of [RFC8122], with the addition of the SDP "tls-id" attribute.

```
m=image 54111 TCP/TLS t38
c=IN IP4 192.0.2.2
a=tls-id:abc3de65cddef001be82
a=setup:passive
a=connection:new
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=fingerprint:SHA-1 \
 4A:AD:B9:B1:3F:82:18:3B:54:02:12:DF:3E:5D:49:6B:19:E5:7C:AB
```

8. SIP Considerations

When the Session Initiation Protocol (SIP) [RFC3261] is used as the signal protocol for establishing a multimedia session, dialogs [RFC3261] might be established between the caller and multiple callees. This is referred to as forking. If forking occurs,

separate DTLS associations will be established between the caller and each callee.

When forking occurs, an SDP offerer can receive DTLS ClientHello messages and SDP answers from multiple remote locations. Because of this, the offerer might have to wait for multiple SDP answers (from different remote locations) until it receives a certificate fingerprint that matches the certificate associated with a specific DTLS handshake. The offerer MUST NOT declare a fingerprint mismatch until it determines that it will not receive SDP answers from any additional remote locations.

It is possible to send an INVITE request that does not contain an SDP offer. Such an INVITE request is often referred to as an "empty INVITE" or an "offerless INVITE". The receiving endpoint will include the SDP offer in a response to the request. When the endpoint generates such an SDP offer, if a previously established DTLS association exists, the offerer MUST insert an SDP "tls-id" attribute and one or more SDP "fingerprint" attributes, with previously assigned attribute values. If a previously established DTLS association does not exist, the offer MUST be generated based on the same rules as a new offer (see Section 5.2). Regardless of the previous existence of a DTLS association, the SDP "setup" attribute MUST be included according to the rules defined in [RFC4145]. Furthermore, if ICE is used, ICE restart MUST be initiated, according to the third-party call-control considerations described in [RFC8839].

9. RFC Updates

9.1. General

This section updates specifications that use DTLS-protected media, in order to reflect the procedures defined in this specification.

9.2. Update to RFC 5763

9.2.1. Update to Section 1

The reference to [RFC4572] is replaced with a reference to [RFC8122].

9.2.2. Update to Section 5

The text in [RFC5763], Section 5 ("Establishing a Secure Channel") is modified by replacing generic SDP offer/answer procedures for DTLS with a reference to this specification:

NEW TEXT:

| The two endpoints in the exchange present their identities as part
| of the DTLS handshake procedure using certificates. This document
| uses certificates in the same style as described in "Connection-
| Oriented Media Transport over the Transport Layer Security (TLS)
| Protocol in the Session Description Protocol (SDP)" [RFC8122].
|
| If self-signed certificates are used, the content of the
| "subjectAltName" attribute inside the certificate MAY use the
| uniform resource identifier (URI) of the user. This is useful for
| debugging purposes only and is not required to bind the
| certificate to one of the communication endpoints. The integrity
| of the certificate is ensured through the "fingerprint" attribute
| in the SDP.
|
| The generation of public/private key pairs is relatively
| expensive. Endpoints are not required to generate certificates
| for each session.

|
| The offer/answer model, defined in [RFC3264], is used by protocols like the Session Initiation Protocol (SIP) [RFC3261] to set up multimedia sessions.
|
| When an endpoint wishes to set up a secure media session with another endpoint, it sends an offer in a SIP message to the other endpoint. This offer includes, as part of the SDP payload, a fingerprint of a certificate that the endpoint wants to use. The endpoint SHOULD send the SIP message containing the offer to the offerer's SIP proxy over an integrity-protected channel. The proxy SHOULD add an Identity header field according to the procedures outlined in [RFC4474]. When the far endpoint receives the SIP message, it can verify the identity of the sender using the Identity header field. Since the Identity header field is a digital signature across several SIP header fields, in addition to the body of the SIP message, the receiver can also be certain that the message has not been tampered with after the digital signature was applied and added to the SIP message.
|
| The far endpoint (answerer) may now establish a DTLS association with the offerer. Alternately, it can indicate in its answer that the offerer is to initiate the DTLS association. In either case, mutual DTLS certificate-based authentication will be used. After completing the DTLS handshake, information about the authenticated identities, including the certificates, is made available to the endpoint application. The answerer is then able to verify that the offerer's certificate used for authentication in the DTLS handshake can be associated with a certificate fingerprint contained in the offer in the SDP. At this point, the answerer may indicate to the end user that the media is secured. The offerer may only tentatively accept the answerer's certificate, since it may not yet have the answerer's certificate fingerprint
|
| When the answerer accepts the offer, it provides an answer back to the offerer containing the answerer's certificate fingerprint. At this point, the offerer can accept or reject the peer's certificate, and the offerer can indicate to the end user that the media is secured.
|
| Note that the entire authentication and key exchange for securing the media traffic is handled in the media path through DTLS. The signaling path is only used to verify the peers' certificate fingerprints.
|
| The offerer and answerer MUST follow the SDP offer/answer procedures defined in RFC 8842.

9.2.3. Update to Section 6.6

The text in [RFC5763], Section 6.6 ("Session Modification") is modified by replacing generic SDP offer/answer procedures for DTLS with a reference to this specification:

NEW TEXT:

| Once an answer is provided to the offerer, either endpoint MAY request a session modification that MAY include an updated offer. This session modification can be carried in either an INVITE or UPDATE request. The peers can reuse an existing DTLS association or establish a new one, following the procedures in RFC 8842.

9.2.4. Update to Section 6.7.1

The text in [RFC5763], Section 6.7.1 ("ICE Interaction") is modified by replacing the ICE procedures with a reference to this

specification:

NEW TEXT:

| The Interactive Connectivity Establishment (ICE) [RFC8445]
| considerations for DTLS-protected media are described in RFC 8842.

9.3. Update to RFC 7345

9.3.1. Update to Section 4

The subsections (4.1 - 4.5) in [RFC7345], Section 4 ("SDP Offerer/ Answerer Procedures") are removed and replaced with the new text below:

NEW TEXT:

| An endpoint (i.e., both the offerer and the answerer) MUST create
| an SDP media description ("m=" line) for each UDPTL-over-DTLS
| media stream and MUST assign a UDP/TLS/UDPTL value (see Table 1)
| to the "proto" field of the "m=" line.
|
| The offerer and answerer MUST follow the SDP offer/answer
| procedures defined in RFC 8842 in order to negotiate the DTLS
| association associated with the UDPTL-over-DTLS media stream. In
| addition, the offerer and answerer MUST use the SDP attributes
| defined for UDPTL over UDP, as defined in [ITU.T38].

9.3.2. Update to Section 5.2.1

The text in [RFC7345], Section 5.2.1 ("ICE Usage") is modified by replacing the ICE procedures with a reference to this specification:

NEW TEXT:

| The Interactive Connectivity Establishment (ICE) [RFC8445]
| considerations for DTLS-protected media are described in RFC 8842.

9.3.3. Update to Section 9.1

A reference to [RFC8122] is added to [RFC7345], Section 9.1 ("Normative References"):

NEW TEXT:

| [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>.

10. Security Considerations

This specification does not modify the security considerations associated with DTLS or the SDP offer/answer mechanism. In addition to the introduction of the SDP "tls-id" attribute, this document simply clarifies the procedures for negotiating and establishing a DTLS association.

This specification does not modify the actual TLS connection setup procedures. The SDP "tls-is" attribute as such cannot be used to correlate an SDP offer/answer exchange with a TLS connection setup. Thus, this document does not introduce new security considerations related to correlating an SDP offer/answer exchange with a TLS connection setup.

11. IANA Considerations

This document updates the "Session Description Protocol Parameters" registry as specified in Section 8.2.2 of [RFC4566]. Specifically, it adds the SDP "tls-id" attribute to the table for SDP media-level attributes as follows.

Attribute name: tls-id

Type of attribute: Media-level

Subject to charset: No

Purpose: Indicates whether a new DTLS association or TLS connection is to be established/re-established.

Appropriate Values: See Section 4

Contact name: Christer Holmberg

Mux Category: IDENTICAL

12. References

12.1. 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, <https://www.rfc-editor.org/info/rfc2119>.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, DOI 10.17487/RFC3261, June 2002, <https://www.rfc-editor.org/info/rfc3261>.

[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>.

[RFC5763] Fischl, J., Tschofenig, H., and E. Rescorla, "Framework for Establishing a Secure Real-time Transport Protocol (SRTP) Security Context Using Datagram Transport Layer Security (DTLS)", RFC 5763, DOI 10.17487/RFC5763, May 2010, <https://www.rfc-editor.org/info/rfc5763>.

[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>.

[RFC7345] Holmberg, C., Sedlacek, I., and G. Salgueiro, "UDP Transport Layer (UDPTL) over Datagram Transport Layer Security (DTLS)", RFC 7345, DOI 10.17487/RFC7345, August 2014, <https://www.rfc-editor.org/info/rfc7345>.

[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>.

[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>.

[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>.

[RFC8843] Holmberg, C., Alvestrand, H., and C. Jennings, "Negotiating Media Multiplexing Using the Session Description Protocol (SDP)", RFC 8843, DOI 10.17487/RFC8843, January 2021, <https://www.rfc-editor.org/info/rfc8843>.

[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>.

12.2. Informative References

[ITU.T38] ITU-T, "Procedures for real-time Group 3 facsimile communication over IP networks", Recommendation T.38, September 2010, <https://www.itu.int/rec/T-REC-T.38/en>.

[RFC4474] Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", RFC 4474, DOI 10.17487/RFC4474, August 2006, <https://www.rfc-editor.org/info/rfc4474>.

[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, <https://www.rfc-editor.org/info/rfc4572>.

[RFC5576] Lennox, J., Ott, J., and T. Schierl, "Source-Specific Media Attributes in the Session Description Protocol (SDP)", RFC 5576, DOI 10.17487/RFC5576, June 2009, <https://www.rfc-editor.org/info/rfc5576>.

[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, <https://www.rfc-editor.org/info/rfc6083>.

[RFC7983] Petit-Huguenin, M. and G. Salgueiro, "Multiplexing Scheme Updates for Secure Real-time Transport Protocol (SRTP) Extension for Datagram Transport Layer Security (DTLS)", RFC 7983, DOI 10.17487/RFC7983, September 2016, <https://www.rfc-editor.org/info/rfc7983>.

[RFC8224] Peterson, J., Jennings, C., Rescorla, E., and C. Wendt, "Authenticated Identity Management in the Session Initiation Protocol (SIP)", RFC 8224, DOI 10.17487/RFC8224, February 2018,

            <https://www.rfc-editor.org/info/rfc8224>.

   [RFC8839] Petit-Huguenin, M., Nandakumar, S., Holmberg, C., Kernen,
              A., and R. Shpount, "Session Description Protocol (SDP)
              Offer/Answer Procedures for Interactive Connectivity
              Establishment (ICE)", RFC 8839, DOI 10.17487/RFC8839,
              January 2021, <https://www.rfc-editor.org/info/rfc8839>.

   [RFC8844] Thomson, M. and E. Rescorla, "Unknown Key-Share Attacks on
              Uses of TLS with the Session Description Protocol (SDP)",
              RFC 8844, DOI 10.17487/RFC8844, January 2021,
              <https://www.rfc-editor.org/info/rfc8844>.

Acknowledgements

   Thanks to Justin Uberti, Martin Thomson, Paul Kyzivat, Jens Guballa,
   Charles Eckel, Gonzalo Salgueiro, and Paul Jones for providing
   comments and suggestions on the document. Ben Campbell performed an
   Area Director review. Paul Kyzivat performed a 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

   Email: rshpount@turbobridge.com