Network Working Group
Internet-Draft
Updates: 5763,7345 (if approved)
Intended status: Standards Track
Expires: October 20, 2017

C. Holmberg
Ericsson
R. Shpount
TurboBridge

April 18, 2017

Using the SDP Offer/Answer Mechanism for DTLS
draft-ietf-mmusic-dtls-sdp-23.txt

Abstract

This document defines the SDP offer/answer procedures for negotiating and establishing a DTLS association. The document also defines the criteria for when a new DTLS association must be established. The document updates RFC 5763 and RFC 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 TLS connection, in conjunction with the procedures in RFC 4145 and RFC 8122.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on October 20, 2017.

Table of Contents

1. Introduction

[RFC5763] defines SDP offer/answer procedures for SRTP-DTLS. [RFC7345] defines SDP offer/answer procedures for 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 [I-D.ietf-mmusic-sdp-bundle-negotiation]. The 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 [I-D.ietf-stir-rfc4474bis]. 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 [I-D.ietf-stir-rfc4474bis] 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) [I-D.ietf-ice-rfc5245bis] is used. One possible way to determine a transport change is based on ufrag [I-D.ietf-ice-rfc5245bis] change, but the ufrag value is changed both when ICE is negotiated and when ICE restart [I-D.ietf-ice-rfc5245bis] occurs. These events do not always require a new DTLS association to be established, but currently there is no way to explicitly indicate in an SDP offer or answer whether a new DTLS association is 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 answers can be used to indicate whether a new DTLS association is to be established.

The SDP 'tls-id' attribute can also be used for negotiating a TLS connection, using the procedures in this document in conjunction with the procedures in [RFC5763] and [RFC8122]. The TLS specific considerations are described in Section 8.

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. 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 an DTLS association replacing a previously established DTLS association.

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 prohibits a DTLS association from spanning multiple transports, and if the transport 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 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 [RFC4566]>
```

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. A non-changed 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), unless there is another mechanism to explicitly indicate that a new DTLS association is to be established, 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:

- DTLS setup role; or
- fingerprint set; or
- local transport parameters; or
- ICE ufrag value

The mux category [I-D.ietf-mmusic-sdp-mux-attributes] for the 'tls-id' attribute is 'IDENTICAL', which means that the attribute value must be identical across all media descriptions being multiplexed [I-D.ietf-mmusic-sdp-bundle-negotiation].

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 [RFC3264] procedures 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 etc.) for individual DTLS usages (e.g., SRTP-DTLS) are outside the scope of this specification, and need to be specified in a usage specific specification.

NOTE: The procedures in this section are generalizations of procedures first specified in SRTP-DTLS [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 de-multiplexed. In 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 has been sent. In case of an unordered transport, such as UDP, packets associated with a previously established DTLS association can arrive after the answer SDP was received and after the first packets associated with the new DTLS association were received. The only way to de-multiplex packets associated with with a previously established DTLS association and the new DTLS association is on the basis of transport 5-tuple. Because of this, if an unordered transport is used for the DTLS association, a new transport (3-tuple) must be allocated by at least one of the endpoints so that DTLS packets can be de-multiplexed.

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 transport (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 if the offerer did not allocate a new transport, the answerer MUST allocate a new transport 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 cipher suites as defined in [RFC8122].

The certificate received during the DTLS handshake 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]). Note that it is permissible to wait until the other side's fingerprint(s) has been received before establishing the connection; however, this may have undesirable latency effects.

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.

5.2. Generating the Initial SDP Offer

When an offerer sends the initial offer, the offerer MUST insert an SDP 'setup' attribute according to the procedures in [RFC4145], and 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 value.

If the offerer inserts the SDP 'setup' attribute with an 'actpass' or 'passive' attribute value, the offerer MUST be prepared to receive a DTLS ClientHello message (if a new DTLS association is established by the answerer) from the answerer before the offerer receives the SDP answer.

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 value. Note that the offerer and answerer generate their own local 'tls-id' attribute

values, and the combination of both values identify 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 an SDP 'tls-id' attribute with the previously assigned value in the associated answer. In addition, the answerer MUST insert an SDP 'setup' attribute with a value that does not change the previously negotiated DTLS roles, and 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' value in the answer, the answerer MUST initiate a DTLS handshake by sending a DTLS ClientHello message towards the offerer.

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, and 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 indiciated a desire to reuse an existing DTLS association and the answerer does not request the establishment of a new DTLS assocation, the offerer will continue to use the previously established DTLS association.

NOTE: 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 MUST still be established if such an answer was received as a response to an offer which requested the establishment of a new DTLS association.

5.5. Modifying the Session

When the offerer sends a subsequent offer, and if the offerer wants to establish a new DTLS association, the offerer MUST insert an SDP 'setup' attribute according to the procedures in [RFC4145], and 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 new unique value.

When the offerer sends a subsequent offer, and the offerer does not want to establish a new DTLS association, and if a previously established DTLS association exists, the offerer MUST insert an SDP 'tls-id' attribute with the previously assigned value in the offer. In addition, the offerer MUST insert an SDP 'setup' attribute, and one or more SDP 'fingerprint' attributes with values that do not change the previously sent fingerprint set, in the offer. The value of the 'setup' attribute SHOULD be set to 'actpass', in order to allow the answerer to establish a new DTLS association with a different role, but MAY be set to the current negotiated role ('active' or 'passive'). It MUST NOT be set to a value that changes the current negotiated role.

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 [I-D.ietf-ice-rfc5245bis] 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 [I-D.ietf-ice-rfc5245bis].

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 which 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 [I-D.ietf-ice-rfc5245bis]. 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. [RFC5764] 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. Transport Protocol Considerations

7.1. Transport Re-Usage

If DTLS is transported on top of a connection-oriented transport protocol (e.g., TCP or SCTP), where all IP packets are acknowledged, all DTLS packets associated with a previous DTLS association MUST be acknowledged (or timed out) before a new DTLS association can be established on the same instance of that transport (5-tuple).

8. TLS Considerations

The procedures in this document can also be used for negotiating and establishing aTLS 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 does 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 mulitple TLS connections and correlate those connections with specific offer/ answer exchanges.

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

If an offerer or answerer inserts an SDP 'connection' attribute with a 'existing' value in the offer/answer, and if a previously established TLS connection exists, 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 [RFC3261], 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
```

9. 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.

It is possible to send an INVITE request which does not contain an SDP offer. Such an INVITE request is often referred to as an 'empty INVITE', or an 'offer-less INVITE'. The receiving endpoint will include the SDP offer in a response to the request. When the endpoint generates such 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 did 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] and if ICE is used, ICE restart MUST be initiated.

10. RFC Updates

10.1. General

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

10.2. Update to RFC 5763

10.2.1. Update to section 5

OLD TEXT:

5. Establishing a Secure Channel

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)" [RFC4572].

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

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. In addition to the usual contents of an SDP [RFC4566] message, each media description ("m=" line and associated parameters) will also contain several attributes as specified in [RFC5764], [RFC4145], and [RFC4572].

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, the fingerprint of the 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]. The SIP message containing the offer SHOULD be sent to the offerer's SIP proxy over an integrity protected channel. 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 TLS 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, are 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 to the 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 offer and answer MUST conform to the following requirements.

- The endpoint MUST use the setup attribute defined in [RFC4145]. The endpoint that is the offerer MUST use the setup attribute value of setup:actpass and be prepared to receive a client_hello before it receives the answer. The answerer MUST use either a setup attribute value of setup:active or setup:passive. Note that if the answerer uses setup:passive, then the DTLS handshake will

not begin until the answerer is received, which adds additional latency. setup:active allows the answer and the DTLS handshake to occur in parallel. Thus, setup:active is RECOMMENDED. Whichever party is active MUST initiate a DTLS handshake by sending a ClientHello over each flow (host/port quartet).

- The endpoint MUST NOT use the connection attribute defined in [RFC4145].

- The endpoint MUST use the certificate fingerprint attribute as specified in [RFC4572].

- The certificate presented during the DTLS handshake MUST match the fingerprint exchanged via the signaling path in the SDP. The security properties of this mechanism are described in Section 8.

- If the fingerprint does not match the hashed certificate, then the endpoint MUST tear down the media session immediately. Note that it is permissible to wait until the other side's fingerprint has been received before establishing the connection; however, this may have undesirable latency effects.

NEW TEXT:

5. Establishing a Secure Channel

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)" [RFC4572].

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, are 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 to 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 [RFCXXXX].

10.2.2. Update to section 6.6

OLD TEXT:

6.6. Session Modification

> 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 the existing associations if they are compatible (i.e., they have the same key fingerprints and transport parameters), or establish a new one following the same rules are for initial exchanges, tearing down the existing association as soon as the offer/answer exchange is completed. Note that if the active/passive status of the endpoints changes, a new connection MUST be established.

NEW TEXT:

6.6. Session Modification

> 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 [RFCXXXX].

10.2.3. Update to section 6.7.1

OLD TEXT:

6.7.1. ICE Interaction

Interactive Connectivity Establishment (ICE), as specified in [RFC5245], provides a methodology of allowing participants in multimedia sessions to verify mutual connectivity. When ICE is being 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. Implementations MUST treat all ICE candidate pairs associated with a single component as part of the same DTLS association. Thus, there will be only one DTLS handshake even if there are multiple valid candidate pairs. Note that this may mean adjusting the endpoint IP addresses if the selected candidate pair shifts, just as if the DTLS packets were an ordinary media stream.

Note that Simple Traversal of the UDP Protocol through NAT (STUN) packets are sent directly over UDP, not over DTLS. [RFC5764] describes how to demultiplex STUN packets from DTLS packets and SRTP packets.

NEW TEXT:

6.7.1. ICE Interaction

The Interactive Connectivity Establishment (ICE) [I-D.ietf-ice-rfc5245bis] considerations for DTLS-protected media are described in [RFCXXXX].

10.3. Update to RFC 7345

10.3.1. Update to section 4

OLD TEXT:

4. SDP Offerer/Answerer Procedures

4.1. General

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 procedures in this section apply to an "m=" line associated with

a UDPTL-over-DTLS media stream.

In order to negotiate a UDPTL-over-DTLS media stream, the following SDP attributes are used:

- The SDP attributes defined for UDPTL over UDP, as described in [ITU.T38.2010]; and

- The SDP attributes, defined in [RFC4145] and [RFC4572], as described in this section.

The endpoint MUST NOT use the SDP "connection" attribute [RFC4145].

In order to negotiate the TLS roles for the UDPTL-over-DTLS transport connection, the endpoint MUST use the SDP "setup" attribute [RFC4145].

If the endpoint supports, and is willing to use, a cipher suite with an associated certificate, the endpoint MUST include an SDP "fingerprint" attribute [RFC4572]. The endpoint MUST support SHA-256 for generating and verifying the SDP "fingerprint" attribute value. The use of SHA-256 is preferred. UDPTL over DTLS, at a minimum, MUST support TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 and MUST support TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256. UDPTL over DTLS MUST prefer TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 and any other Perfect Forward Secrecy (PFS) cipher suites over non-PFS cipher suites. Implementations SHOULD disable TLS-level compression.

If a cipher suite with an associated certificate is selected during the DTLS handshake, the certificate received during the DTLS handshake MUST match the fingerprint received in the SDP "fingerprint" attribute. If the fingerprint does not match the hashed certificate, then the endpoint MUST tear down the media session immediately. Note that it is permissible to wait until the other side's fingerprint has been received before establishing the connection; however, this may have undesirable latency effects.

4.2. Generating the Initial Offer

The offerer SHOULD assign the SDP "setup" attribute with a value of "actpass", unless the offerer insists on being either the sender or receiver of the DTLS ClientHello message, in which case the offerer can use either a value of "active" (the offerer will be the sender of ClientHello) or "passive" (the offerer will be the receiver of ClientHello). The offerer MUST NOT assign an SDP "setup" attribute with a "holdconn" value.

If the offerer assigns the SDP "setup" attribute with a value of

"actpass" or "passive", the offerer MUST be prepared to receive a DTLS ClientHello message before it receives the SDP answer.

4.3. Generating the Answer

If the answerer accepts the offered UDPTL-over-DTLS transport connection, in the associated SDP answer, the answerer MUST assign an SDP "setup" attribute with a value of either "active" or "passive", according to the procedures in [RFC4145]. The answerer MUST NOT assign an SDP "setup" attribute with a value of "holdconn".

If the answerer assigns an SDP "setup" attribute with a value of "active" value, the answerer MUST initiate a DTLS handshake by sending a DTLS ClientHello message on the negotiated media stream, towards the IP address and port of the offerer.

4.4. Offerer Processing of the Answer

When the offerer receives an SDP answer, if the offerer ends up being active it MUST initiate a DTLS handshake by sending a DTLS ClientHello message on the negotiated media stream, towards the IP address and port of the answerer.

4.5. Modifying the Session

Once an offer/answer exchange has been completed, either endpoint MAY send a new offer in order to modify the session. The endpoints can reuse the existing DTLS association if the key fingerprint values and transport parameters indicated by each endpoint are unchanged. Otherwise, following the rules for the initial offer/answer exchange, the endpoints can negotiate and create a new DTLS association and, once created, delete the previous DTLS association, following the same rules for the initial offer/answer exchange. Each endpoint needs to be prepared to receive data on both the new and old DTLS associations as long as both are alive.

NEW TEXT:

4. SDP Offerer/Answerer Procedures

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 [RFCXXXX] 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.T38.2010].

10.3.2. Update to section 5.2.1

OLD TEXT:

5.2.1. ICE Usage

When Interactive Connectivity Establishment (ICE) [RFC5245] is being 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. User Agents (UAs) MUST treat all ICE candidate pairs associated with a single component as part of the same DTLS association. Thus, there will be only one DTLS handshake even if there are multiple valid candidate pairs. Note that this may mean adjusting the endpoint IP addresses if the selected candidate pair shifts, just as if the DTLS packets were an ordinary media stream. In the case of an ICE restart, the DTLS handshake procedure is repeated, and a new DTLS association is created. Once the DTLS handshake is completed and the new DTLS association has been created, the previous DTLS association is deleted.

NEW TEXT:

5.2.1. ICE Usage

The Interactive Connectivity Establishment (ICE) [I-D.ietf-ice-rfc5245bis] considerations for DTLS-protected media are described in [RFCXXXX].

[RFC EDITOR NOTE: Througout the document, please replace RFCXXXX with the RFC number of this document.]

11. 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, the specification simply clarifies the procedures for negotiating and establishing a DTLS association.

12. 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.

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

13. 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 AD review.

14. Change Log

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

Changes from draft-ietf-mmusic-sdp-dtls-22

- Support for TLS added.
- Editorial changes based on sec-dir review by Rich Salz.
- Editorial changes based on gen-art review by Paul Kyzivat.
- Editorial changes based on ops-dir review by Carlos Pignataro.

Changes from draft-ietf-mmusic-sdp-dtls-21

- Changes based on AD review by Ben Campbell.
- (https://www.ietf.org/mail-archive/web/mmusic/current/msg17707.html)

Changes from draft-ietf-mmusic-sdp-dtls-20

- Change to length and randomness of tls-id attribute value.

Changes from draft-ietf-mmusic-sdp-dtls-19

- Change based on comment from Roman.

Changes from draft-ietf-mmusic-sdp-dtls-18

- Changes based on comments from Flemming.
- - Change in tls-id value definition.
- - Editorial fixes.

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

- Reference fix.

Changes from draft-ietf-mmusic-sdp-dtls-16

- Editorial changes based on 2nd WGLC comments from Christian Groves and Nevenka Biondic.

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

- tls-id attribute value made globally unique

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

- Changes based on comments from Flemming:
- - Additional dtls-is clarifiations
- - Editorial fixes

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

- Text about the updated RFCs added to Abstract and Introduction
- Reference to RFC 5763 removed from section 6 (ICE Considerations)
- Reference to RFC 5763 removed from section 8 (SIP Considerations)

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

- "unreliable" changed to "unordered"

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

- Attribute name changed to tls-id
- Additional text based on comments from Roman Shpount.

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

- Modified document to use tls-id instead of dtls-connection
- Changes are based on comments from Eric Rescorla, Justin Uberti, and Paul Kyzivat.

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

- Offer/Answer section modified in order to allow sending of multiple SDP 'fingerprint' attributes.
- Terminology made consistent: 'DTLS connection' replaced with 'DTLS association'.
- Editorial changes based on comments from Paul Kyzivat.

Changes from draft-ietf-mmusic-sdp-dtls-07

- Reference to RFC 7315 replaced with reference to RFC 7345.

Changes from draft-ietf-mmusic-sdp-dtls-06

- Text on restrictions regarding spanning a DTLS association over multiple transports added.
- Mux category added to IANA Considerations.
- Normative text regarding mux category and source-specific applicability added.
- Reference to RFC 7315 added.
- Clarified that offerer/answerer that has not been updated to support this specification will not include the tls-id attribute in offers and answers.
- Editorial corrections based on WGLC comments from Charles Eckel.

Changes from draft-ietf-mmusic-sdp-dtls-05

- Text on handling offer/answer error conditions added.

Changes from draft-ietf-mmusic-sdp-dtls-04

- Editorial nits fixed based on comments from Paul Kyzivat:

Changes from draft-ietf-mmusic-sdp-dtls-03

- Changes based on comments from Paul Kyzivat:
- - Modification of tls-id attribute section.
- - Removal of IANA considerations subsection.
- - Making note into normative text in o/a section.
- Changes based on comments from Martin Thompson:
- - Abbreviations section removed.
- - Clarify that a new DTLS association requires a new o/a transaction.

Changes from draft-ietf-mmusic-sdp-dtls-02

- - Updated RFCs added to boilerplate.

Changes from draft-ietf-mmusic-sdp-dtls-01

- - Annex regarding 'tls-id-id' attribute removed.
- - Additional SDP offer/answer procedures, related to certificates, added.
- - Updates to RFC 5763 and RFC 7345 added.
- - Transport protocol considerations added.

Changes from draft-ietf-mmusic-sdp-dtls-00

- - SDP 'connection' attribute replaced with new 'tls-id' attribute.
- - IANA Considerations added.
- - E-mail regarding 'tls-id-id' attribute added as Annex.

Changes from draft-holmberg-mmusic-sdp-dtls-01

- - draft-ietf-mmusic version of draft submitted.
- - Draft file name change (sdp-dtls -> dtls-sdp) due to collision with another expired draft.

- - Clarify that if ufrag in offer is unchanged, it must be unchanged in associated answer.
- - SIP Considerations section added.
- - Section about multiple SDP fingerprint attributes added.

Changes from draft-holmberg-mmusic-sdp-dtls-00

- - Editorial changes and clarifications.

15. References

15.1. 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>.

[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, <http://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, <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>.

[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>.

[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, <http://www.rfc-editor.org/info/rfc5763>.

[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, <http://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, <http://www.rfc-editor.org/info/rfc8122>.

[I-D.ietf-ice-rfc5245bis] Keranen, A., Holmberg, C., and J. Rosenberg, "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal", draft-ietf-ice-rfc5245bis-08 (work in progress), December 2016.

[I-D.ietf-mmusic-sdp-mux-attributes] Nandakumar, S., "A Framework for SDP Attributes when Multiplexing", draft-ietf-mmusic-sdp-mux-attributes-16 (work in progress), December 2016.

[I-D.ietf-mmusic-sdp-bundle-negotiation] Holmberg, C., Alvestrand, H., and C. Jennings, "Negotiating Media Multiplexing Using the Session Description Protocol (SDP)", draft-ietf-mmusic-sdp-bundle-negotiation-38 (work in progress), April 2017.

15.2. Informative References

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

[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>.

[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, <http://www.rfc-editor.org/info/rfc5576>.

[RFC5764] McGrew, D. and E. Rescorla, "Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)", RFC 5764, DOI 10.17487/RFC5764, May 2010, <http://www.rfc-editor.org/info/rfc5764>.

[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>.

[I-D.ietf-stir-rfc4474bis] Peterson, J., Jennings, C., Rescorla, E., and C. Wendt, "Authenticated Identity Management in the Session Initiation Protocol (SIP)", draft-ietf-stir-rfc4474bis-16 (work in progress), February 2017.

[ITU.T38.2010] International Telecommunications Union, "Procedures for real-time Group 3 facsimile communication over IP networks", ITU-T Recommendation T.38, September 2010.

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