Network Working Group
Internet-Draft
Updates: 5763,7315 (if approved)
Intended status: Standards Track
Expires: July 21, 2016

C. Holmberg
Ericsson
R. Shpount
TurboBridge

January 18, 2016

Using the SDP Offer/Answer Mechanism for DTLS
draft-ietf-mmusic-dtls-sdp-04.txt

Abstract

This draft defines the SDP offer/answer procedures for negotiating and establishing a DTLS association. The draft also defines the criteria for when a new DTLS association must be established.

This draft defines a new SDP media-level attribute, 'dtls-connection'.

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 July 21, 2016.

Table of Contents

1. Introduction

[RFC5763] defines SDP Offer/Answer procedures for SRTP-DTLS. This draft defines the SDP Offer/Answer [RFC3264] procedures for negotiation DTLS in general, based on the procedures in [RFC5763].

This draft also defines a new SDP attribute, 'dtls-connection'. The attribute is used in SDP offers and answers to explicitly indicate whether a new DTLS association is to be established.

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) [RFC5245] is used. One possible way to determine a transport change

is based on ufrag change, but the ufrag value is changed both when ICE is negotiated and when ICE restart [RFC5245] 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 draft defines a new SDP attribute, 'dtls-connection'. The attribute is used in SDP offers and answers to explicitly indicate whether a new DTLS association is to be established/re-established. The attribute can be used both with and without ICE.

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 in the following cases:

- The DTLS roles change;
- The fingerprint (certificate) value changes; or
- The establishment of a new DTLS association is explicitly signaled;

NOTE: The first two items list above are based on the procedures in [RFC5763]. This draft adds the support for explicit signaling.

Whenever an entity determines, based on the criteria above, that a new DTLS association is the entity MUST initiate an associated SDP offer/answer transaction, following to the procedures in Section 5.

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

3.2. Change of Local Transport Parameters

If an endpoint modifies its local transport parameters (IP address and/or port), and if the modification requires a new DTLS association, the endpoint MUST either change its DTLS role, its fingerprint value and/or use the SDP 'dtls-connection' attribute with a 'new' value Section 4.

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 either change its DTLS role, its fingerprint value and/or use the SDP 'dtls-connection' attribute with a 'new' value Section 4.

3.4. Multiple SDP fingerprint attributes

It is possible to associate multiple SDP fingerprint attribute values to an 'm-' line. If any of the attribute values associated with an 'm-' line are removed, or if any new attribute values are added, it is considered a fingerprint value change.

4. SDP dtls-connection Attribute

The SDP 'connection' attribute [RFC4145] was originally defined for connection-oriented protocols, e.g. TCP and TLS. This section defines a similar attribute, 'dtls-connection', to be used with DTLS.

Name: dtls-connection

Value: conn-value

Usage Level: media

Charset Dependent: no

Syntax:

```
conn-value = "new" / "existing"
```

Example:

```
a=dtls-connection:existing
```

A 'dtls-connection' attribute value of 'new' indicates that a new DTLS association MUST be established. A 'dtls-connection' attribute value of 'existing' indicates that a new DTLS association MUST NOT be established.

Unlike the SDP 'connection' attribute for TLS, there is no default value defined for the 'dtls-connection' 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 an attribute, other means needs to be used in order for endpoints to

determine whether an offer or answer is associated with an event that requires the DTLS association to be re-established.

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 usage specific SDP attributes etc) for individual DTLS usages (e.g. SRTP-DTLS) are outside the scope of this specification, and needs 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 'dtls-connection' attribute. That document is herein revised to make use of these new procedures.

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

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 [RFC4572], is used to provide the fingerprint value; and
- The SDP 'dtls-connection' attribute, defined in this specification, is used to explicitly indicate whether a new DTLS association is to be established or whether a previous association is to be used.

Endpoints MUST NOT use the SDP 'connection' attribute [RFC4145] when negotiating a DTLS association.

The SDP 'connection' attribute MAY be used if the usage is associated with another protocol layer, e.g. SCTP or TCP, used together with DTLS.

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 algorithms defined in **** Endpoints MUST support SHA-256 for generating and verifying the fingerprint value associated with the DTLS association. The use of SHA-256 is preferred.

Endpoints MUST, at a minimum, 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.

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.

5.2. Generating the Initial SDP Offer

When the offerer sends the initial offer, and the offerer wants to establish a DTLS association, it MUST insert an SDP 'dtls-connection' attribute with a 'new' value in the offer. In addition, the offerer MUST insert an SDP 'setup' attribute according to the procedures in [RFC4145], and an SDP 'fingerprint' attribute according to the procedures in [RFC4572], in the offer.

If the offerer inserts the SDP 'setup' attribute with an 'actpass' or 'passive' 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 it receives the SDP answer.

5.3. Generating the Answer

If an answerer receives an offer that contains an SDP 'dtls-connection' attribute with a 'new' value, or if the answerer receives and offer that contains an 'dtls-connection' attribute with an 'existing' value and the answerer determines (based on the criteria for establishing a new DTLS association) that a new DTLS association is to be established, the answerer MUST insert a 'new' value in the associated answer. In addition, the answerer MUST insert an SDP 'setup' attribute according to the procedures in [RFC4145], and an

SDP 'fingerprint' attribute according to the procedures in [RFC4572], in the answer.

If an answerer receives an offer that contains an SDP 'dtls-connection' attribute with a 'new' value, 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 contains a 'dtls-connection' attribute with an 'existing' value, and if the answerer determines that a new DTLS association is not to be established, the answerer MUST insert a 'dtls-connection' attribute with an 'existing' 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 an SDP 'fingerprint' attribute with a value that does not change the previously sent fingerprint, in the answer.

If the answerer receives an offer that does not contain an SDP 'dtls-connection' attribute, the answerer MUST NOT insert a 'dtls-connection' 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 the offerer.

5.4. Offerer Processing of the SDP Answer

When an offerer receives an answer that contains an SDP 'dtls-connection' attribute with a 'new' value, 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 answer contains an SDP 'dtls-connection' attribute with an 'existing' value, the offerer will continue using the previously established DTLS association. It is considered an error case if the answer contains a 'dtls-connection' attribute with an 'existing' value, and a DTLS association does not exist.

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 'dtls-connection' attribute with a 'new' value in the offer. In

addition, the offerer MUST insert an SDP 'setup' attribute according to the procedures in [RFC4145], and an SDP 'fingerprint' attribute according to the procedures in [RFC4572], in the offer.

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 'dtls-connection' attribute with an 'existing' value in the offer. In addition, the offerer MUST insert an SDP 'setup' attribute with a value that does not change the previously negotiated DTLS roles, and an SDP 'fingerprint' attribute with a value that does not change the previously sent fingerprint, in the offer.

NOTE: When a new DTLS association is 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 ICE 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.

An ICE restart [RFC5245] does not by default require a new DTLS association to be established.

As defined in [RFC5763], 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 transport.

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 MUST be established between the caller and each callee.

It is possible to send an INVITE request which does not contain an SDP offer. Such 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 associated with the response. When the endpoint generates such SDP offer, it MUST assign an SDP connection attribute, with a 'new' value, to each 'm-' line that describes DTLS protected media. If ICE is used, the endpoint MUST allocate a new set of ICE candidates, in order to ensure that two DTLS association would not be running over the same transport.

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

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 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.

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 offerer and answerer MUST follow the SDP offer/answer procedures defined in [RFCXXXX].

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].

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) [RFC5245] considerations for DTLS-protected media are described in [RFCXXXX].

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.

9.3. Update to RFC 7345

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].

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) [RFC5245] considerations for DTLS-protected media are described in [RFCXXXX].

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 'dtls-connection' attribute, the specification simply clarifies the procedures for negotiating and establishing a DTLS association.

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 dtls-connection attribute to the table for SDP media level attributes.

Attribute name: dtls-connection
Type of attribute: media-level
Subject to charset: no
Purpose: TBD
Appropriate Values: see Section X
Contact name: Christer Holmberg

12. Acknowledgements

Thanks to Justin Uberti, Martin Thomson, Paul Kyzivat and Jens Guballa for providing comments and suggestions on the draft.

13. Change Log

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

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

- Changes based on comments from Paul Kyzivat:
- - Modification of dtls-connection 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 'dtls-connection-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 'dtls-connection' attribute.
- - IANA Considerations added.
- - E-mail regarding 'dtls-connection-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.

14. 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>.

[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>.

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

[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>.

[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>.

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