MMUSIC Working Group C. Holmberg
Internet-Draft I. Sedlacek
Intended status: Standards Track Ericsson
Expires: July 21, 2014 G. Salgueiro
Cisco
January 17, 2014

UDP Transport Layer (UDPTL) over Datagram Transport Layer Security (DTLS)

draft-ietf-mmusic-udptl-dtls-03

Abstract

This document specifies how the UDP Transport Layer (UDPTL) protocol, the predominant transport protocol for T.38 fax, can be transported over the Datagram Transport Layer Security (DTLS) protocol, how the usage of UDPTL over DTLS is indicated in the Session Description Protocol (SDP), and how UDPTL over DTLS is negotiated in a session established using the Session Initiation Protocol (SIP).

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

While it is possible to transmit highly sensitive documents using traditional telephony encryption devices, secure fax on the Public Switched Telephone Network (PSTN) was never widely considered or prioritized. This was mainly because of the challenges involved with physical access to telephony equipment. As real-time communications transition to IP networks, where information might potentially be intercepted or spoofed, an appropriate level of security for fax that offers integrity and confidentiality protection is vital.

The overwhelmingly predominant fax transport protocol is UDPTL-based [ITU.T38.2010]. The protocol stack for fax transport using UDPTL is shown in Table 1.

```
+-----------------------------+
| Internet facsimile protocol |
+-----------------------------+
|           UDPTL             |
+-----------------------------+
|            UDP              |
+-----------------------------+
|             IP              |
+-----------------------------+
```

Table 1: Protocol stack for UDPTL over UDP

Implementations exist today for securing this fax transport type. Some of these mechanisms are:

- o [ITU.T30.2005] Annex H specifies integrity and confidentiality protection of fax in the application layer, independent of protocol for fax transport.
- o [ITU.T38.2010] specifies fax transport over RTP/SAVP which enables integrity and confidentiality protection of fax in IP network.

Despite these mechanisms to secure fax, there is no transport layer security offering integrity and confidentiality protection for UDPTL. This issue was addressed in a study by the 3rd Generation Partnership Project (3GPP) on how to provide secure fax in the IP Multimedia Subsystem (IMS). They concluded that secure fax shall be transported using UDPTL over DTLS.

This document specifies fax transport using UDPTL over DTLS [RFC6347], which enables integrity and confidentiality protection of fax in IP networks. The protocol stack which enhances fax transport to offer integrity and confidentiality using UDPTL over DTLS is shown in Table 2.

```
+-----------------------------+
| Internet facsimile protocol |
+-----------------------------+
|           UDPTL             |
+-----------------------------+
|            DTLS             |
+-----------------------------+
|            UDP              |
+-----------------------------+
|             IP              |
+-----------------------------+
```

Table 2: Protocol stack for UDPTL over DTLS over UDP

The primary motivations for the mechanism in this document are:

- o The design of DTLS [RFC6347] is clearly defined, well understood and implementations are widely available.
- o No DTLS extensions are required in order to enable UDPTL transport over DTLS.
- o Fax transport using UDPTL over DTLS only requires insertion of the DTLS layer between the UDPTL layer and the UDP layer, as shown in Table 2. The UDPTL layer and layers above UDPTL layer require no modification.
- o UDPTL [ITU.T38.2010] is by far the most widely deployed fax transport protocol in IP networks.
- o 3GPP and the IP fax community need a mechanism to transport UDPTL over DTLS in order to provide secure fax in IMS and other SIP-based networks.

This document specifies the transport of UDPTL over DTLS using the DTLS record layer "application_data" packets [RFC6347].

Since the DTLS record layer "application_data" packet does not indicate whether it carries UDPTL, or some other protocol, the usage of a dedicated DTLS association for transport of UDPTL needs to be negotiated, e.g. using the Session Description Protocol (SDP) [RFC4566] and the SDP offer/answer mechanism [RFC3264].

Therefore, this document specifies a new <proto> value [RFC4566] for the SDP media description ("m=" line) [RFC3264], in order to indicate UDPTL over DTLS in SDP messages [RFC4566].

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 BCP 14, RFC 2119 [RFC2119].

DTLS uses the term "session" to refer to a long-lived set of keying material that spans DTLS associations. In this document, in order to be consistent with SIP/SDP usage of "session" terminology, we use "session" to refer to a multimedia session and use the term "DTLS session" to refer to the DTLS construct. We use the term "DTLS association" to refer to a particular DTLS cipher suite and keying material set that is associated with a single host/port quartet. The same DTLS session can be used to establish the keying material for multiple DTLS associations. For consistency with other SIP/SDP usage, we use the term "connection" when what's being referred to is a multimedia stream that is not specifically DTLS.

3. Secure Channel

3.1. Secure Channel Establishment

The SDP offer/answer mechanism [RFC3264] is used by other protocols, e.g. the Session Initiation Protocol (SIP) [RFC3261], to negotiate and establish multimedia sessions.

In addition to the usual contents of an SDP media description ("m=" line) specified for UDPTL over UDP, each SDP media description for UDPTL over DTLS over UDP will also contain several SDP attributes, which were introduced in the context of TCP [RFC4145] and TLS [RFC4572], and are re-used in this document.

The SDP offer and the SDP answer MUST conform to the following requirements:

- o The endpoint MUST set the "proto" field of the "m=" line to the token specified in Table 3.
- o In order to negotiate the TLS roles, the endpoint MUST use the SDP setup attribute [RFC4145]. The offerer SHOULD assign the SDP setup attribute with a setup:actpass value, and MAY assign the SDP setup attribute with a setup:active value or setup:passive value. The offerer MUST NOT assign the SDP setup attribute with a setup:holdconn value. If the offerer assigns the SDP setup attribute with a setup:actpass value or setup:passive value, it MUST be prepared to receive a DTLS client_hello message before it receives the SDP answer. If the answerer accepts the media stream, then it MUST assign the SDP setup attribute with either a setup:active value or setup:passive value, according to the procedures in [RFC4145]. The answerer MUST NOT assign an SDP setup attribute with a setup:holdconn value. Whichever party is active, it MUST initiate a DTLS handshake by sending a ClientHello over each flow (host/port quartet).
- o If the endpoint supports, and is willing to use, a cipher suite with an associated certificate, it MUST include an SDP fingerprint attribute [RFC4572] in the SDP.
- o 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.
- o The endpoint MUST NOT use the SDP connection attribute [RFC4145].

3.2. Secure Channel Usage

DTLS is used as specified in [RFC6347]. Once the DTLS handshake is successfully completed (in order to prevent facsimile data from being transmitted insecurely), the UDPTL packets SHALL be transported in DTLS record layer "application_data" packets.

4. Miscellaneous Considerations

4.1. Anonymous Calls

When making anonymous calls, a new self-signed certificate SHOULD be used for each call and the content of the subjectAltName attribute inside the certificate MUST NOT contain information that either allows correlation or identification of the user making anonymous calls.

4.2. Middlebox Interaction

4.2.1. ICE Interaction

When 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. 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.

4.2.2. Latching Control without ICE

When ICE [RFC5245] is not being used and the DTLS handshake has not completed upon receiving the other side's SDP, then the passive side MUST do a single unauthenticated STUN [RFC5389] connectivity check in order to open up the appropriate pinhole. All UAs MUST be prepared to answer this request during the handshake period even if they do not otherwise do ICE. However, the active side MUST proceed with the DTLS handshake as appropriate even if no such STUN check is received and the passive MUST NOT wait for a STUN answer before sending its ServerHello.

4.2.3. STUN Interaction

The UA SHALL send the STUN packets [RFC5389] directly over UDP, not over DTLS.

The UA MUST demultiplex packets arriving on the IP address and port associated with the DTLS association as follows:

- o If the value of the first byte of the packet is 0 or 1, then the packet is STUN.
- o If the value of the first byte of the packet is between 20 and 63 (inclusive), the packet is DTLS.

4.3. Rekeying

After the DTLS handshake caused by rekeying has completed, because of possible packet reordering on the wire, packets protected by the previous set of keys can arrive. To compensate for this fact, receivers SHOULD maintain both sets of keys for some time in order to be able to decrypt and verify older packets. The duration of maintaining the previous set of keys after the finish of the DTLS handshake is out of scope for this document.

5. Security Considerations

Fax may be used to transmit a wide range of sensitive data, including personal, corporate, and governmental information. It is therefore critical to be able to protect against threats to the confidentiality and integrity of the transmitted data.

The mechanism in this document provides integrity and confidentiality protection for fax by specifying fax transport using UDPTL over DTLS [RFC6347].

DTLS media signaled with SIP requires a mechanism to ensure that the communicating peers' certificates are correct.

The standard DTLS strategy for authenticating the communicating parties is to give the server (and optionally the client) a PKIX [RFC5280] certificate. The client then verifies the certificate and checks that the name in the certificate matches the server's domain name. This works because there are a relatively small number of servers with well-defined names; a situation that does not usually occur in the VoIP context.

The design described in this document is intended to leverage the authenticity of the signaling channel (while not requiring confidentiality). As long as each side of the connection can verify

the integrity of the SDP received from the other side, then the DTLS handshake cannot be hijacked via a man-in-the-middle attack. This integrity protection is easily provided by the caller to the callee via the SIP Identity [RFC4474] mechanism. Other mechanisms, such as the S/MIME mechanism [RFC3261], or perhaps future mechanisms yet to be specified could also serve this purpose.

While this mechanism can still be used without such integrity mechanisms, the security provided is limited to defense against passive attack by intermediaries. An active attack on the signaling plus an active attack on the media plane can allow an attacker to attack the connection (R-SIG-MEDIA in the notation of [RFC5479]).

6. IANA Considerations

This document updates the "Session Description Protocol (SDP) Parameters" registry as specified in Section 8.2.2 of [RFC4566]. Specifically, it adds the values in Table 3 to the table for the SDP "proto" field registry.

Type	SDP Name	Reference
proto	"UDP/TLS/UDPTL"	[RFC-XXXX]

Table 3: SDP "proto" field values

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

7. Acknowledgments

Special thanks to Peter Dawes, who provided comments on the initial version of the draft, and to Paul E. Jones, James Rafferty, Albrecht Schwarz, Oscar Ohlsson and David Hanes who provided valuable feedback and input on the MMUSIC mailing list.

8. Change Log

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

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

- o Editorial comments based on review comments by James Rafferty (http://www.ietf.org/mail-archive/web/mmusic/current/msg12890.html)

- o Editorial comments based on review comments by David Hanes (http://www.ietf.org/mail-archive/web/mmusic/current/msg12886.html)
- o Editorial comments based on review comments by Oscar Ohlsson (http://www.ietf.org/mail-archive/web/mmusic/current/msg12882.html)
- o Editorial comments based on review comments by Albrecht Schwartz (http://www.ietf.org/mail-archive/web/mmusic/current/msg12900.html)

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

- o Usage of the SDP fingerprint attribute depends on whether a cipher suite with an associated certificate is used.
- o Editor's note in section 4.2 removed. Procedure text added.

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

- o SDP offerer is allowed to assign an a=setup:active or a=setup:passive value, in addition to the recommended a=setup:actpass (http://www.ietf.org/mail-archive/web/mmusic/current/msg12331.html).
- o The example for secure fax replacing audio stream in audio-only session added (http://www.ietf.org/mail-archive/web/mmusic/current/msg12428.html).
- o Editor's note on the connection attribute resolved by prohibiting usage of the SDP connection attribute (http://www.ietf.org/mail-archive/web/mmusic/current/msg12772.html).
- o Editorial corrections.

Changes from draft-holmberg-mmusic-udptl-dtls-02

- o Milestone adopted - draft-ietf-mmusic version of the draft submitted.

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

- o Gonzalo Salgueiro added as co-author.
- o PSTN comparison text and Introduction text modified.

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

- o Text about T.30 added.
- o Latest version of T.38 referenced.
- o Additional text about the need for secure fax in IP networks.

Changes from draft-holmberg-dispatch-udptl-dtls-00

- o WG changed to MMUSIC.

o Added text about 3GPP need for UDPTL/DTLS.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[RFC3264] Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model with Session Description Protocol (SDP)", RFC 3264, June 2002.

[RFC4145] Yon, D. and G. Camarillo, "TCP-Based Media Transport in the Session Description Protocol (SDP)", RFC 4145, September 2005.

[RFC4474] Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", RFC 4474, August 2006.

[RFC4566] Handley, M., Jacobson, V., and C. Perkins, "SDP: Session Description Protocol", RFC 4566, July 2006.

[RFC4572] Lennox, J., "Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP)", RFC 4572, July 2006.

[RFC5245] Rosenberg, J., "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols", RFC 5245, April 2010.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

[RFC5389] Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, "Session Traversal Utilities for NAT (STUN)", RFC 5389, October 2008.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, January 2012.

[ITU.T30.2005] International Telecommunications Union, "Procedures for document facsimile transmission in the general switched telephone network", ITU-T Recommendation T.30, September 2005.

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

9.2. Informative References

[RFC5479] Wing, D., Fries, S., Tschofenig, H., and F. Audet, "Requirements and Analysis of Media Security Management Protocols", RFC 5479, April 2009.

Appendix A. Examples

A.1. General

Prior to establishing the session, both Alice and Bob generate self-signed certificates which are used for a single session or, more likely, reused for multiple sessions.

The SIP signaling from Alice to her proxy is transported over TLS to ensure an integrity protected channel between Alice and her identity service. Alice's identity service asserts identity of Alice and protects the SIP message, e.g. using SIP Identity. Transport between proxies should also be protected somehow.

Only one element is shown for Alice's and Bob's proxies for the purposes of simplification.

For the sake of brevity and simplicity, only the mandatory SDP T.38 attributes are shown.

A.2. Basic Message Flow

Figure 1 shows an example message flow of session establishment for T.38 fax securely transported using UDPTL over DTLS.

In this example flow, Alice acts as the passive endpoint of the DTLS association and Bob acts as the active endpoint of the DTLS association.

```
   Alice                    Proxies                   Bob
     | (1) SIP INVITE         |                        |
     |----------------------->|                        |
     |                        | (2) SIP INVITE         |
     |                        |----------------------->|
     |                        |   (3) DTLS ClientHello |
     |<-----------------------------------------------|
     |    (4) remaining messages of DTLS handshake     |
     |<---------------------------------------------->|
     |                        |                        |
     |                        |                        |
     |                        |         (5) SIP 200 OK |
     |                        |<-----------------------|
     |         (6) SIP 200 OK |                        |
     |<-----------------------|                        |
     | (7) SIP ACK            |                        |
     |----------------------------------------------->|
     |      (8) T.38 message using UDPTL over DTLS     |
     |<---------------------------------------------->|
     |                        |                        |
```

Figure 1: Basic message flow

Message (1):

Figure 2 shows the initial INVITE request sent by Alice to Alice's proxy. The initial INVITE request contains an SDP offer.

The "m=" line in the SDP offer indicates T.38 fax using UDPTL over DTLS.

The SDP setup:actpass attribute in the SDP offer indicates that Alice has requested to be either the active or passive endpoint.

The SDP fingerprint attribute in the SDP offer contains the certificate fingerprint computed from Alice's self-signed certificate.

```
INVITE sip:bob@example.com SIP/2.0
To: <sip:bob@example.com>
From: "Alice"<sip:alice@example.com>;tag=843c7b0b
Via: SIP/2.0/TLS ua1.example.com;branch=z9hG4bK-0e53sadfkasldkfj
Contact: <sip:alice@ua1.example.com>
Call-ID: 6076913b1c39c212@REVMTEpG
CSeq: 1 INVITE
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, UPDATE
Max-Forwards: 70
Content-Type: application/sdp
Content-Length: xxxx
Supported: from-change

v=0
o=- 1181923068 1181923196 IN IP4 ua1.example.com
s=-
c=IN IP4 ua1.example.com
t=0 0
m=image 6056 UDP/TLS/UDPTL t38
a=setup:actpass
a=fingerprint: SHA-1 \
  4A:AD:B9:B1:3F:82:18:3B:54:02:12:DF:3E:5D:49:6B:19:E5:7C:AB
a=T38FaxRateManagement:transferredTCF
```

Figure 2: Message (1)

Message (2):

Figure 3 shows the SIP INVITE request sent by Bob's proxy to Bob.

When received, Bob verifies the identity provided in the SIP INVITE request.

```
INVITE sip:bob@ua2.example.com SIP/2.0
To: <sip:bob@example.com>
From: "Alice"<sip:alice@example.com>;tag=843c7b0b
Via: SIP/2.0/TLS proxy.example.com;branch=z9hG4bK-0e53sadfkasldk
Via: SIP/2.0/TLS ua1.example.com;branch=z9hG4bK-0e53sadfkasldkfj
Record-Route: <sip:proxy.example.com;lr>
Contact: <sip:alice@ua1.example.com>
Call-ID: 6076913b1c39c212@REVMTEpG
CSeq: 1 INVITE
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, UPDATE
Max-Forwards: 69
Content-Type: application/sdp
Content-Length: xxxx
Supported: from-change

v=0
o=- 1181923068 1181923196 IN IP4 ua1.example.com
s=-
c=IN IP4 ua1.example.com
t=0 0
m=image 6056 UDP/TLS/UDPTL t38
a=setup:actpass
a=fingerprint: SHA-1 \
  4A:AD:B9:B1:3F:82:18:3B:54:02:12:DF:3E:5D:49:6B:19:E5:7C:AB
a=T38FaxRateManagement:transferredTCF
```

Figure 3: Message (2)

Message (3):

Assuming that Alice's identity is valid, Bob sends a DTLS ClientHello directly to Alice.

Message (4):

Alice and Bob exchange further messages of DTLS handshake (HelloVerifyRequest, ClientHello, ServerHello, Certificate, ServerKeyExchange, CertificateRequest, ServerHelloDone, Certificate, ClientKeyExchange, CertificateVerify, ChangeCipherSpec, Finished).

When Bob receives the certificate of Alice via DTLS, Bob checks whether the certificate fingerprint calculated from Alice's certificate received via DTLS matches the certificate fingerprint received in the a=fingerprint SDP attribute of Figure 3. In this

message flow, the check is successful and thus session setup continues.

Message (5):

Figure 4 shows a SIP 200 (OK) response to the initial SIP INVITE request, sent by Bob to Bob's proxy. The SIP 200 (OK) response contains an SDP answer.

The "m=" line in the SDP answer indicates T.38 fax using UDPTL over DTLS.

The SDP setup:active attribute in the SDP answer indicates that Bob has requested to be the active endpoint.

The SDP fingerprint attribute in the SDP answer contains the certificate fingerprint computed from Bob's self-signed certificate.

```
SIP/2.0 200 OK
To: <sip:bob@example.com>;tag=6418913922105372816
From: "Alice" <sip:alice@example.com>;tag=843c7b0b
Via: SIP/2.0/TLS proxy.example.com:5061;branch=z9hG4bK-0e53sadfkasldk
Via: SIP/2.0/TLS ua1.example.com;branch=z9hG4bK-0e53sadfkasldkfj
Record-Route: <sip:proxy.example.com;lr>
Call-ID: 6076913b1c39c212@REVMTEpG
CSeq: 1 INVITE
Contact: <sip:bob@ua2.example.com>
Content-Type: application/sdp
Content-Length: xxxx
Supported: from-change

v=0
o=- 8965454521 2105372818 IN IP4 ua2.example.com
s=-
c=IN IP4 ua2.example.com
t=0 0
m=image 12000 UDP/TLS/UDPTL t38
a=setup:active
a=fingerprint: SHA-1 \
  FF:FF:FF:B1:3F:82:18:3B:54:02:12:DF:3E:5D:49:6B:19:E5:7C:AB
a=T38FaxRateManagement:transferredTCF
```

Figure 4: Message (5)

Message (6):

Figure 5 shows a SIP 200 (OK) response to the initial SIP INVITE request, sent by Alice's proxy to Alice. Alice checks if the certificate fingerprint calculated from the Bob's certificate received via DTLS is the same as the certificate fingerprint received in the a=fingerprint SDP attribute of Figure 5. In this message flow, the check is successful and thus session setup continues.

```
SIP/2.0 200 OK
To: <sip:bob@example.com>;tag=6418913922105372816
From: "Alice" <sip:alice@example.com>;tag=843c7b0b
Via: SIP/2.0/TLS ua1.example.com;branch=z9hG4bK-0e53sadfkasldkfj
Record-Route: <sip:proxy.example.com;lr>
Call-ID: 6076913b1c39c212@REVMTEpG
CSeq: 1 INVITE
Contact: <sip:bob@ua2.example.com>
Content-Type: application/sdp
Content-Length: xxxx
Supported: from-change

v=0
o=- 8965454521 2105372818 IN IP4 ua2.example.com
s=-
c=IN IP4 ua2.example.com
t=0 0
m=image 12000 UDP/TLS/UDPTL t38
a=setup:active
a=fingerprint: SHA-1 \
  FF:FF:FF:B1:3F:82:18:3B:54:02:12:DF:3E:5D:49:6B:19:E5:7C:AB
a=T38FaxRateManagement:transferredTCF
```

Figure 5: Message (6)

Message (7):

Alice sends the SIP ACK request to Bob.

Message (8):

At this point, Bob and Alice can exchange T.38 fax securely transported using UDPTL over DTLS.

A.3. Message Flow Of T.38 Fax Replacing Audio Media Stream in An Existing Audio-Only Session

Traditionally, most session with non-secure transport of T.38 fax, transported using UDPTL, are established by modifying an ongoing audio session into a fax session. Figure 6 shows an example message flow of modifying an existing audio session into a session with T.38 fax securely transported using UDPTL over DTLS.

In this example flow, Alice acts as the passive endpoint of the DTLS association and Bob acts as the active endpoint of the DTLS association.

```
   Alice                    Proxies                   Bob
     |                         |                         |
     |        (1) Audio-only session initiation          |
     |<----------------------+---------------------->|
     |                         |                         |
     | (2) SIP re-INVITE       |                         |
     |----------------------------------------------->|
     |                         |   (3) DTLS ClientHello |
     |<-----------------------------------------------|
     |    (4) remaining messages of DTLS handshake      |
     |<---------------------------------------------->|
     |                         |                         |
     |                         |                         |
     |                         |         (5) SIP 200 OK |
     |<-----------------------------------------------|
     | (6) SIP ACK             |                         |
     |----------------------------------------------->|
     |      (7) T.38 message using UDPTL over DTLS      |
     |<---------------------------------------------->|
     |                         |                         |
```

Figure 6: Message Flow Of T.38 Fax Replacing Audio Media Stream in An Existing Audio-Only Session

Message (1):

Session establishment of audio-only session. The proxies decide not to record-route.

Message (2):

Alice sends SIP re-INVITE request. The SDP offer included in the SIP re-INVITE request is shown in Figure 7.

The first "m=" line in the SDP offer indicates audio media stream being removed. The second "m=" line in the SDP offer indicates T.38 fax using UDPTL over DTLS being added.

The SDP setup:actpass attribute in the SDP offer indicates that Alice has requested to be either the active or passive endpoint.

The SDP fingerprint attribute in the SDP offer contains the certificate fingerprint computed from Alice's self-signed certificate.

```
v=0
o=- 2465353433 3524244442 IN IP4 ua1.example.com
s=-
c=IN IP4 ua1.example.com
t=0 0
m=audio 0 UDP/TLS/RTP/SAVP 0
m=image 46056 UDP/TLS/UDPTL t38
a=setup:actpass
a=fingerprint: SHA-1 \
  4A:AD:B9:B1:3F:82:18:3B:54:02:12:DF:3E:5D:49:6B:19:E5:7C:AB
a=T38FaxRateManagement:transferredTCF
```

Figure 7: SDP offer of message (2)

Message (3):

Bob sends a DTLS ClientHello directly to Alice.

Message (4):

Alice and Bob exchange further messages of DTLS handshake (HelloVerifyRequest, ClientHello, ServerHello, Certificate, ServerKeyExchange, CertificateRequest, ServerHelloDone, Certificate, ClientKeyExchange, CertificateVerify, ChangeCipherSpec, Finished).

When Bob receives the certificate of Alice via DTLS, Bob checks whether the certificate fingerprint calculated from Alice's certificate received via DTLS matches the certificate fingerprint received in the a=fingerprint SDP attribute of Figure 7. In this message flow, the check is successful and thus session setup continues.

Message (5):

Bob sends a SIP 200 (OK) response to the SIP re-INVITE request. The SIP 200 (OK) response contains an SDP answer shown in Figure 8.

The first "m=" line in the SDP offer indicates audio media stream being removed. The second "m=" line in the SDP answer indicates T.38 fax using UDPTL over DTLS being added.

The SDP setup:active attribute in the SDP answer indicates that Bob has requested to be the active endpoint.

The SDP fingerprint attribute in the SDP answer contains the certificate fingerprint computed from Bob's self-signed certificate.

```
v=0
o=- 4423478999 5424222292 IN IP4 ua2.example.com
s=-
c=IN IP4 ua2.example.com
t=0 0
m=audio 0 UDP/TLS/RTP/SAVP 0
m=image 32000 UDP/TLS/UDPTL t38
a=setup:active
a=fingerprint: SHA-1 \
  FF:FF:FF:B1:3F:82:18:3B:54:02:12:DF:3E:5D:49:6B:19:E5:7C:AB
a=T38FaxRateManagement:transferredTCF
```

Figure 8: SDP answer of message (5)

Message (6):

Alice sends the SIP ACK request to Bob.

Message (7):

At this point, Bob and Alice can exchange T.38 fax securely transported using UDPTL over DTLS.

Authors' Addresses

Christer Holmberg
Ericsson
Hirsalantie 11
Jorvas 02420
Finland

Email: christer.holmberg@ericsson.com

Ivo Sedlacek
Ericsson
Sokolovska 79
Praha 18600
Czech Republic

Email: ivo.sedlacek@ericsson.com

Gonzalo Salgueiro
Cisco Systems, Inc.
7200-12 Kit Creek Road
Research Triangle Park, NC 27709
US

Email: gsalguei@cisco.com