MMUSIC Working Group
Internet-Draft
Intended status: Standards Track
Expires: March 28, 2014

C. Holmberg
I. Sedlacek
Ericsson
G. Salgueiro
Cisco

September 24, 2013

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

draft-holmberg-mmusic-udptl-dtls-02

Abstract

This document specifies how the UDP Transport Layer (UDPTL) protocol 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

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 March 28, 2014.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect

to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

While telephony encryption devices have been traditionally used for highly sensitive documents, secure fax on the Public Switched Telephone Network (PSTN) was not as widely considered or prioritized 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. Some of the security mechanisms for securing fax include:

- o [ITU.T30.2005] Annex H specifies integrity and confidentiality protection of fax in 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

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

Protocol
Internet facsimile protocol
UDPTL
UDP
IP

Table 1: Protocol stack for UDPTL over UDP

The 3rd Generation Partnership Project (3GPP) has performed a study on how to provide secure fax in the IP Multimedia Subsystem (IMS) and 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 for integrity and confidentiality protected fax transport using UDPTL over DTLS is shown in Table 2.

Protocol
Internet facsimile protocol
UDPTL
DTLS
UDP
IP

Table 2: Protocol stack for UDPTL 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 needs a mechanism to transport UDPTL over DTLS, in order to provide secure fax in IMS 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 it 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 the UDP, each SDP media description for UDPTL over DTLS over the UDP will also contain several SDP attributes, as specified in [RFC4145] and [RFC4572].

The SDP offer and 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 The endpoint MUST use the SDP setup attribute [RFC4145]. The offerer MUST assign the SDP setup attribute with setup:actpass value, and MUST be prepared to receive a DTLS client_hello message before it receives the SDP answer. The answerer MUST assign the SDP setup attribute with either setup:active value or setup:passive value. The answerer SHOULD assign the SDP setup attribute with the setup:active value. Whichever party is active MUST initiate a DTLS handshake by sending a ClientHello over each flow (host/port quartet).
- o The endpoint MUST use the SDP certificate fingerprint attribute [RFC4572].
- o The certificate presented during the DTLS handshake MUST match the fingerprint exchanged via the signaling path in the SDP.
- o 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.

Editor's note: FFS if connection attribute defined in RFC4145 is needed.

3.2. Secure Channel Usage

DTLS is used as specified in [RFC6347]. Once the DTLS handshake is completed, 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

The procedures defined for SRTP-DTLS in Section 6.7 of [RFC5763] for interaction with middleboxes also apply to UDPTL over DTLS.

The procedures defined for SRTP-DTLS in Section 5.1.2 of [RFC5764] for distinguishing DTLS and STUN packets also apply to UDPTL over DTLS.

Editor's note: The complete SRTP-DTLS implementation is not needed. Only the parts for interaction with middleboxes in RFC5763 and for distinguishing DTLS and STUN packets in RFC5764 are needed. Should those be copied into this document?

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

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 (see sample message flow in Annex A.2) 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 and Albrecht Schwarz 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-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

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

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

- WG changed to MMUSIC.
- 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.

[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.

[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, May 2010.

[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, May 2010.

[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. Example

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. 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 with Identity

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 DTLS association and Bob acts as the active endpoint of 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 with Identity

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 indicates 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=example1
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.

The SIP INVITE request contains an Identity header field and an Identity-Info header fields inserted by Alice's proxy.

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
Identity: CyI4+nAkHrH3ntmaxgr01TMxTmtjP7MASwliNRdupRI1vpkXRvZXx1ja9k
          3W+v1PDsy32MaqZi0M5WfEkXxbgTnPYW0jIoK8HMyY1VT7egt0kk4XrKFC
          HYWGCl0nB2sNsM9CG4hq+YJZTMaSROoMUBhikVIjnQ8ykeD6UXNOyfI=
Identity-Info: https://example.com/cert
Content-Type: application/sdp
Content-Length: xxxx
Supported: from-change

v=0
o=- 1181923068 1181923196 IN IP4 ua1.example.com
s=example1
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 the 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 200 (OK) response to the initial SIP INVITE request, sent by Bob to Bob's proxy. The 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 indicates 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=- 6418913922105372816 2105372818 IN IP4 ua2.example.com
s=example2
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 (6)

Message (6):

Figure 5 shows a 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=- 6418913922105372816 2105372818 IN IP4 ua2.example.com
s=example2
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 (7)

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.

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