



XMPP

XEP-0320: Use of DTLS-SRTP in Jingle Sessions

Philipp Hancke

<mailto:fippo@andyet.com>

<xmpp:fippo@goodadvice.pages.de>

2015-10-15

Version 0.3.1

Status	Type	Short Name
Deferred	Standards Track	NOT_YET_ASSIGNED

This specification defines how to use DTLS-SRTP (RFC 5763) in the Jingle application type for the Real-time Transport Protocol (RTP) as a way to negotiate media path key agreement for secure RTP in one-to-one media sessions.

Legal

Copyright

This XMPP Extension Protocol is copyright © 1999 – 2017 by the [XMPP Standards Foundation](#) (XSF).

Permissions

Permission is hereby granted, free of charge, to any person obtaining a copy of this specification (the "Specification"), to make use of the Specification without restriction, including without limitation the rights to implement the Specification in a software program, deploy the Specification in a network service, and copy, modify, merge, publish, translate, distribute, sublicense, or sell copies of the Specification, and to permit persons to whom the Specification is furnished to do so, subject to the condition that the foregoing copyright notice and this permission notice shall be included in all copies or substantial portions of the Specification. Unless separate permission is granted, modified works that are redistributed shall not contain misleading information regarding the authors, title, number, or publisher of the Specification, and shall not claim endorsement of the modified works by the authors, any organization or project to which the authors belong, or the XMPP Standards Foundation.

Warranty

NOTE WELL: This Specification is provided on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE.

Liability

In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall the XMPP Standards Foundation or any author of this Specification be liable for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising from, out of, or in connection with the Specification or the implementation, deployment, or other use of the Specification (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if the XMPP Standards Foundation or such author has been advised of the possibility of such damages.

Conformance

This XMPP Extension Protocol has been contributed in full conformance with the XSF's Intellectual Property Rights Policy (a copy of which can be found at <https://xmpp.org/about/xsf/ipr-policy>) or obtained by writing to XMPP Standards Foundation, P.O. Box 787, Parker, CO 80134 USA).

Contents

1	Protocol	1
2	Determining Support	5
3	Security Considerations	5
4	IANA Considerations	6
5	Acknowledgements	6
6	XMPP Registrar Considerations	6
6.1	Protocol Namespaces	6
6.2	Protocol Versioning	6
7	XML Schemas	6

1 Protocol

Jingle RTP Sessions (XEP-0167) ¹ recommends the use of the Secure Real-time Transport Protocol (SRTP) for end-to-end encryption of RTP sessions negotiated using Jingle (XEP-0166) ². RFC 5763 ³ provides an approach to establish a Secure Real-time Transport Protocol (SRTP) security context using the Datagram Transport Layer Security (DTLS) protocol. A mechanism of transporting the fingerprint attribute that identifies the key that will be presented during the DTLS handshake in Jingle is defined herein. Inclusion of this information is OPTIONAL in both SIP/SDP and Jingle.

Note that while this specification only describes the use in the context of DTLS-SRTP, the fingerprint transported can be used in other contexts like for example establishing connections using SCTP over DTLS as described in Use of DTLS/SCTP in Jingle ICE-UDP (XEP-0343) ⁴.

The SDP format (defined in RFC 4572 ⁵) is shown below.

```
a=fingerprint:hash-func fingerprint
```

An example follows.

```
a=fingerprint:sha-256 02
:1A:CC:54:27:AB:EB:9C:53:3F:3E:4B:65:2E:7D:46:3F:54:42:CD:54:F1:7A:03:A2:7D:F9:B0:
```

Additionally, the SDP setup attribute defined in RFC 4145 ⁶ must be mapped, whose usage for DTLS-SRTP is defined in RFC 5763.

```
a=setup:role
```

Note that no mapping for the 'holdconn' role is defined herein.

These SDP attributes can be translated into Jingle as a <fingerprint/> element qualified by the 'urn:xmpp:jingle:apps:dtls:0' namespace, as shown below.

```
<fingerprint xmlns='urn:xmpp:jingle:apps:dtls:0' hash='hash-func'
  setup='role'>
  fingerprint
</fingerprint>
```

¹XEP-0167: Jingle RTP Sessions <<https://xmpp.org/extensions/xep-0167.html>>.

²XEP-0166: Jingle <<https://xmpp.org/extensions/xep-0166.html>>.

³RFC 5763: Framework for Establishing a Secure Real-time Transport Protocol (SRTP) Security Context Using Datagram Transport Layer Security (DTLS) <<http://tools.ietf.org/html/rfc5763>>.

⁴XEP-0343: Use of DTLS/SCTP in Jingle ICE-UDP <<https://xmpp.org/extensions/xep-0343.html>>.

⁵RFC 4572: Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP) <<http://tools.ietf.org/html/rfc4572>>.

⁶RFC 4145: TCP-Based Media Transport in the Session Description Protocol (SDP) <<http://tools.ietf.org/html/rfc4145>>.

An example follows. Note that the whitespace would not appear in actual XML content.

```
<fingerprint xmlns='urn:xmpp:jingle:apps:dtls:0' hash='sha-256' setup=
  'actpass'>
  02
    :1A:CC:54:27:AB:EB:9C:53:3F:3E:4B:65:2E:7D:46:3F:54:42:CD:54:F1:7A:03:A2:7D:F9:B
</fingerprint>
```

If the Jingle initiator wishes to use DTLS-SRTP, it includes the <fingerprint/> element in its session invitation.

Listing 1: Initiator sends session invitation with DTLS fingerprint

```
<iq from='romeo@montague.lit/orchard'
  id='uz61v4m4'
  to='juliet@capulet.lit/balcony'
  type='set'>
  <jingle xmlns='urn:xmpp:jingle:1'
    action='session-initiate'
    initiator='romeo@montague.lit/orchard'
    sid='a73sjvkla37jfea'>
    <content creator='initiator' name='voice'>
      <description xmlns='urn:xmpp:jingle:apps:rtp:1' media='audio'>
        <payload-type id='96' name='speex' clockrate='16000' />
        <payload-type id='97' name='speex' clockrate='8000' />
        <payload-type id='18' name='G729' />
        <payload-type id='103' name='L16' clockrate='16000' channels='
          2' />
        <payload-type id='98' name='x-ISAC' clockrate='8000' />
      </description>
      <transport xmlns='urn:xmpp:jingle:transports:ice-udp:1'
        pwd='asd88fgpdd777uzjYhagZg'
        ufrag='8hhy'>
        <fingerprint xmlns='urn:xmpp:jingle:apps:dtls:0' hash='sha-256'
          setup='actpass'>
          02
            :1A:CC:54:27:AB:EB:9C:53:3F:3E:4B:65:2E:7D:46:3F:54:42:CD:54:F1:7A:03:A2:7D:F9:B
        </fingerprint>
        <candidate component='1'
          foundation='1'
          generation='0'
          id='e10747fg11'
          ip='10.0.1.1'
          network='1'
          port='8998'
          priority='2130706431'
          protocol='udp'
        </candidate>
      </jingle>
    </content>
  </iq>
```

```

        type='host' />
    <candidate component='1'
        foundation='2'
        generation='0'
        id='y3s2b30v3r'
        ip='192.0.2.3'
        network='1'
        port='45664'
        priority='1694498815'
        protocol='udp'
        rel-addr='10.0.1.1'
        rel-port='8998'
        type='srflx' />
</transport>
</content>
</jingle>
</iq>

```

If the receiving party wishes to use DTLS, it also includes the <fingerprint/> element in its session-accept message.

Listing 2: Responder sends session-accept

```

<iq from='juliet@capulet.lit/balcony'
    id='pn2va48j'
    to='romeo@montague.lit/orchard'
    type='set'>
  <jingle xmlns='urn:xmpp:jingle:1'
    action='session-accept'
    initiator='romeo@montague.lit/orchard'
    responder='juliet@capulet.lit/balcony'
    sid='a73sjjvkl37jfea'>
    <content creator='initiator' name='voice'>
      <description xmlns='urn:xmpp:jingle:apps:rtp:1' media='audio'>
        <payload-type id='97' name='speex' clockrate='8000' />
        <payload-type id='18' name='G729' />
      </description>
      <transport xmlns='urn:xmpp:jingle:transports:ice-udp:1'
        pwd='YH75Fviy6338Vbrhrlp8Yh'
        ufrag='9uB6'>
        <fingerprint xmlns='urn:xmpp:jingle:apps:dtls:0' hash='sha-256'
          setup='active'>
          BD:E8:2C:D3:BD:B6:98:50:45:7D:5B:36:89:53:31:15:52:25:88:82:06:95:88:A3:3D:
        </fingerprint>
      <candidate component='1'
        foundation='1'
        generation='0'
        id='or2ii2syr1'

```

```

        ip='192.0.2.1'
        network='0'
        port='3478'
        priority='2130706431'
        protocol='udp'
        type='host' />
    </transport>
</content>
</jingle>
</iq>

```

Alternatively, if the receiving party wishes to expedite with ICE and DTLS negotiation without accepting the session, it MAY include the <fingerprint/> element when sending a transport-info message:

Listing 3: A transport-info containing a DTLS fingerprint

```

<iq from='juliet@capulet.lit/balcony'
  id='pn2va48j'
  to='romeo@montague.lit/orchard'
  type='set'>
  <jingle xmlns='urn:xmpp:jingle:1'
    action='transport-info'
    initiator='romeo@montague.lit/orchard'
    responder='juliet@capulet.lit/balcony'
    sid='a73sjjvkla37jfea'>
    <content creator='initiator' name='voice'>
      <transport xmlns='urn:xmpp:jingle:transports:ice-udp:1'
        pwd='YH75Fviy6338Vbrhrlp8Yh'
        ufrag='9uB6'>
        <fingerprint xmlns='urn:xmpp:jingle:apps:dtls:0' hash='sha-256'
          setup='active'>
          BD:E8:2C:D3:BD:B6:98:50:45:7D:5B:36:89:53:31:15:52:25:88:82:06:95:88:
        </fingerprint>
      <candidate component='1'
        foundation='1'
        generation='0'
        id='or2ii2syr1'
        ip='192.0.2.1'
        network='0'
        port='3478'
        priority='2130706431'
        protocol='udp'
        type='host' />
    </transport>
  </content>
</jingle>
</iq>

```

2 Determining Support

If an entity supports establishing a Secure Real-time Transport Protocol security context using the Datagram Transport Layer Security protocol, it MUST advertise that fact in its responses to [Service Discovery \(XEP-0030\)](#)⁷ information (“disco#info”) requests by returning a feature of “urn:xmpp:jingle:apps:dtls:0”:

Listing 4: A disco#info query

```
<iq type='get'
  from='calvin@usrobots.lit/lab'
  to='herbie@usrobots.lit/home'
  id='disco1'>
  <query xmlns='http://jabber.org/protocol/disco#info' />
</iq>
```

Listing 5: A disco#info response

```
<iq type='result'
  from='herbie@usrobots.lit/home'
  to='calvin@usrobots.lit/lab'
  id='disco1'>
  <query xmlns='http://jabber.org/protocol/disco#info'>
    <feature var='urn:xmpp:jingle:1' />
    <feature var='urn:xmpp:jingle:apps:dtls:0' />
  </query>
</iq>
```

In order for an application to determine whether an entity supports this protocol, where possible it SHOULD use the dynamic, presence-based profile of service discovery defined in [Entity Capabilities \(XEP-0115\)](#)⁸. However, if an application has not received entity capabilities information from an entity, it SHOULD use explicit service discovery instead.

3 Security Considerations

Security considerations for DTLS-SRTP itself are provided in RFC 5763. XMPP stanzas such as Jingle messages and service discovery exchanges are not encrypted or signed. As a result, it is possible for an attacker to intercept these stanzas and modify them, thus convincing one party that the other party does not support DTLS-SRTP and therefore denying the parties an opportunity to use DTLS-SRTP.

⁷XEP-0030: Service Discovery <<https://xmpp.org/extensions/xep-0030.html>>.

⁸XEP-0115: Entity Capabilities <<https://xmpp.org/extensions/xep-0115.html>>.

4 IANA Considerations

This document requires no interaction with the [Internet Assigned Numbers Authority \(IANA\)](#)⁹.

5 Acknowledgements

Thanks to Justin Uberti, Peter Saint-Andre and Lance Stout.

6 XMPP Registrar Considerations

6.1 Protocol Namespaces

This specification defines the following XML namespace:

- `urn:xmpp:jingle:apps:dtls:0`

The [XMPP Registrar](#)¹⁰ includes the foregoing namespace to the registry located at [<https://xmpp.org/registrar/namespaces.html>](https://xmpp.org/registrar/namespaces.html), as described in Section 4 of [XMPP Registrar Function \(XEP-0053\)](#)¹¹.

6.2 Protocol Versioning

If the protocol defined in this specification undergoes a revision that is not fully backwards-compatible with an older version, the XMPP Registrar shall increment the protocol version number found at the end of the XML namespaces defined herein, as described in Section 4 of XEP-0053.

7 XML Schemas

```
<?xml version='1.0' encoding='UTF-8'?>
```

⁹The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols, such as port numbers and URI schemes. For further information, see <http://www.iana.org/>.

¹⁰The XMPP Registrar maintains a list of reserved protocol namespaces as well as registries of parameters used in the context of XMPP extension protocols approved by the XMPP Standards Foundation. For further information, see <https://xmpp.org/registrar/>.

¹¹XEP-0053: XMPP Registrar Function [<https://xmpp.org/extensions/xep-0053.html>](https://xmpp.org/extensions/xep-0053.html).

```
<xs:schema
  xmlns:xs='http://www.w3.org/2001/XMLSchema'
  targetNamespace='urn:xmpp:jingle:apps:dtls:0'
  xmlns='urn:xmpp:jingle:apps:dtls:0'
  elementFormDefault='qualified'>

  <xs:annotation>
    <xs:documentation>
      The protocol documented by this schema is defined in
      XEP-xxxx: http://www.xmpp.org/extensions/xep-xxxx.html
    </xs:documentation>
  </xs:annotation>

  <xs:element name='fingerprint'>
    <xs:complexType>
      <xs:simpleContent>
        <xs:extension base='xs:string'>
          <xs:attribute name='hash' type='xs:string' use='required' />
          <xs:attribute name='setup' use='required' />
          <xs:simpleType>
            <xs:restriction base='xs:NCName'>
              <xs:enumeration value='active' />
              <xs:enumeration value='passive' />
              <xs:enumeration value='actpass' />
              <xs:enumeration value='holdconn' />
              <xs:annotation>
                <xs:documentation>
                  the 'holdconn' value is not used and included only
                  for completeness.
                </xs:documentation>
              </xs:annotation>
            </xs:restriction>
          </xs:simpleType>
        </xs:attribute>
      </xs:extension>
    </xs:simpleContent>
  </xs:complexType>
</xs:element>
</xs:schema>
```