XEP-0396: Jingle Encrypted Transports - OMEMO

Paul Schaub
mailto:vanitasvitae@riseup.net
xmpp:vanitasvitae@jabberhead.tk

2018-12-06
Version 0.2.0

Status	Type	Short Name
Deferred	Standards Track	jet-omemo

Extension for JET introducing OMEMO End-to-End Encrypted Jingle Transports.

Legal

Copyright

Permissions

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 Introduction

Jingle Encrypted Transports (XEP-0391) [1] can be used to utilize different end-to-end encryption methods to secure Jingle Transports, eg. in the context of Jingle File Transfer (XEP-0234) [2]. This document aims to extend Jingle Encrypted Transports (XEP-0391) [3] to allow the use of OMEMO encryption with Jingle transports. To achieve this goal, this protocol extension makes use of OMEMOs KeyTransportElements.

2 Mappings

Conveniently the OMEMO protocol already provides a way to transport key material to another entity. So called KeyTransportElements are basically normal OMEMO MessageElements, but without a payload, so the contained key can be used for something else (see Section 4.6 of OMEMO Encryption (XEP-0384) [4]). This extension uses the key encrypted in the KeyTransportMessages <key> attribute and initialization vector from the <iv> attribute to secure Jingle Transports. The key corresponds to the Transport Key of XEP-0391, while the iv corresponds to the Initialization Vector. The KeyTransportMessage is the equivalent to the Envelope Element. Note that within the Envelope Element, the Transport Key is encrypted with the OMEMO ratchet.

3 Limitations

Unfortunately OMEMO Encryption (XEP-0384) [5] determines the type of the transported key to be AES-128-GCM-NoPadding, so no other configuration can be used in the context of this extension.
Since OMEMO deviceIds are not bound to XMPP resources, the initiator MUST encrypt the Transport Key for every device of the recipient.

4 Key Transport

In order to transport a key to the responder, the initiator creates a fresh AES-128-GCM-NoPadding Transport Key and Initialization Vector and generates an OMEMO KeyTransportElement from it as described in OMEMO Encryption (XEP-0384) [6]. This is then added as

[1] XEP-0391: Jingle Encrypted Transports <https://xmpp.org/extensions/xep-0391.html>.
[2] XEP-0234: Jingle File Transfer <https://xmpp.org/extensions/xep-0234.html>.
[3] XEP-0391: Jingle Encrypted Transports <https://xmpp.org/extensions/xep-0391.html>.
[4] XEP-0384: OMEMO Encryption <https://xmpp.org/extensions/xep-0384.html>.
[5] XEP-0384: OMEMO Encryption <https://xmpp.org/extensions/xep-0384.html>.
[6] XEP-0384: OMEMO Encryption <https://xmpp.org/extensions/xep-0384.html>.

a child of the JET <security> element. The ’cipher’ attribute MUST be set to ’aes-128-gcm-nopadding:0’ (see the ciphers section of XEP-0391). The value of the ’type’ attribute must be set to the namespace of the used version of XEP-0384 (see Namespace Versioning regarding the possibility of incrementing the version number).

Listing 1: Romeo initiates an OMEMO encrypted file offer

```
<iq from=’romeo@montague.example/dr4hcr0st3lup4c’
    id=’nzu25s8’
    to=’juliet@capulet.example/yn0cl4bnw0yr3vym’
    type=’set’>
  <jingle xmlns=’urn:xmpp:jingle:1’
          action=’session-initiate’
          initiator=’romeo@montague.example/dr4hcr0st3lup4c’
          sid=’851ba2’>
    <content creator=’initiator’ name=’a-file-offer’ senders=’
       initiator’>
      <description xmlns=’urn:xmpp:jingle:apps:file-transfer:5’>
        <file>
          <date>1969-07-21T02:56:15Z</date>
          <desc>This is a test. If this were a real file...</desc>
          <media-type>text/plain</media-type>
          <name>test.txt</name>
          <range/>
          <size>6144</size>
          <hash xmlns=’urn:xmpp:hashes:2’
                algo=’sha-1’>w0mcJylzCn+AfvuGdqkty2+KP48=</hash>
        </file>
      </description>
      <transport xmlns=’urn:xmpp:jingle:transports:s5b:1’
                 mode=’tcp’
                 sid=’vj3hs98y’>
        <candidate cid=’hft54dqy’
                   host=’192.168.4.1’
                   jid=’romeo@montague.example/dr4hcr0st3lup4c’
                   port=’5086’
                   priority=’8257636’
                   type=’direct’/>
      </transport>
      <security xmlns=’urn:xmpp:jingle:jet:0’
                name=’a-file-offer’
                cipher=’urn:xmpp:ciphers:aes-128-gcm-nopadding’
                type=’eu.siacs.conversations.axolotl’>
        <encrypted xmlns=’eu.siacs.conversations.axolotl’>
          <header sid=’27183’>
            <key rid=’31415’>BASE64ENCODED...</key>
            <key prekey=”true” rid=’12321’>BASE64ENCODED...</key>
            <!-{}- ... -{}->
            <iv>BASE64ENCODED...</iv>
          </header>
        </encrypted>
      </security>
    </content>
  </jingle>
</iq>
```

The recipient decrypts the OMEMO KeyTransportElement to retrieve the Transport Secret. Transport Key and Initialization Vector are later used to encrypt/decrypt data as described in Jingle Encrypted Transports (XEP-0391) [7].

5 Determining Support

To advertise its support for JET-OMEMO, when replying to service discovery information ("disco#info") requests an entity MUST return URNs for any version of this extension, as well as of the JET extension that the entity supports -- e.g., "urn:xmpp:jingle:jet-omemo:0" for this version, or "urn:xmpp:jingle:jet:0" for Jingle Encrypted Transports (XEP-0391) [8] (see Namespace Versioning regarding the possibility of incrementing the version number).

Listing 2: Service discovery information request

```
<iq from=’romeo@montague.example/dr4hcr0st3lup4c’
    id=’uw72g176’
    to=’juliet@capulet.example/yn0cl4bnw0yr3vym’
    type=’get’>
  <query xmlns=’http://jabber.org/protocol/disco#info’/>
</iq>
```

Listing 3: Service discovery information response

```
<iq from=’juliet@capulet.example/yn0cl4bnw0yr3vym’
    id=’uw72g176’
    to=’romeo@montague.example/dr4hcr0st3lup4c’
    type=’result’>
  <query xmlns=’http://jabber.org/protocol/disco#info’>
    <feature var=’urn:xmpp:jingle:jet:0’/>
    <feature var=’urn:xmpp:jingle:jet-omemo: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) [9]. However, if an application has not received entity capabilities

[7] XEP-0391: Jingle Encrypted Transports <https://xmpp.org/extensions/xep-0391.html>.

[8] XEP-0391: Jingle Encrypted Transports <https://xmpp.org/extensions/xep-0391.html>.

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

information from an entity, it SHOULD use explicit service discovery instead.