XEP-0374: OpenPGP for XMPP Instant Messaging

Florian Schmaus
mailto:flo@geekplace.eu
xmpp:flo@geekplace.eu

Dominik Schürmann
mailto:dominik@dominikschuermann.de
xmpp:dominik@dominikschuermann.de

Vincent Breitmoser
mailto:look@my.amazin.horse
xmpp:valodim@stratum0.org

2018-01-25
Version 0.2.0

Status	Type	Short Name
Deferred	Standards Track	oxim

Specifies a OpenPGP for XMPP (XEP-0373) profile for the Instant Messaging (IM) use case.

Legal

Copyright

Permissions

Warranty

Liability

Conformance

Contents

1 Introduction

This XMPP extension protocol specifies a profile of OpenPGP for XMPP (XEP-0373) [1] for OpenPGP secured Instant Messaging (IM).
Unlike similar XEPs, e.g., OMEMO Encryption (XEP-0384) [2], this XEP *does not* provide Forward Secrecy (FS), but as an advantage in return, allows users to read their archived conversations (respectively their encrypted data) later on. Of course, only as long as they still possess the according secret key. FS and being able to decrypt archived messages are mutually exclusive, i.e., one can not have both. The authors therefore consider this XEP complementary to similar ones which also provide end-to-end encryption but with a different feature set.

2 OX Instant Messaging Profile

2.1 Discovering Support

If an entity supports exchanging OpenPGP encrypted and signed instant messages over XMPP, i.e., what is specified herein, it MUST advertise that fact by announcing a Service Discovery (XEP-0030) [3] feature of 'urn:xmpp:openpgp:im:0'. It thus includes this feature in response to a service discovery request.

Listing 1: Service Discovery information request

```
<iq type='get'
    from='juliet@example.org/balcony'
    to='romeo@example.org/orchard'
    id='disco1'>
  <query xmlns='http://jabber.org/protocol/disco#info'/>
</iq>
```

Listing 2: Service Discovery information response

```
<iq type='result'
    from='romeo@example.org/orchard'
    to='juliet@example.org/balcony'
    id='disco1'>
  <query xmlns='http://jabber.org/protocol/disco#info'>
    ...
    <feature var='urn:xmpp:openpgp:im:0'/>
    ...
  </query>
</iq>
```

[1] XEP-0373: OpenPGP for XMPP <https://xmpp.org/extensions/xep-0373.html>.
[2] XEP-0384: OMEMO Encryption <https://xmpp.org/extensions/xep-0384.html>.
[3] XEP-0030: Service Discovery <https://xmpp.org/extensions/xep-0030.html>.

Because of possible downgrade attacks, users should be given an option to force the usage of the protocol defined herein no matter if the remote announces support or not.

2.2 OpenPGP Secured Instant Messaging

In order to establish an OpenPGP secured IM communication, IM clients first need to determine the public key of their interlocutor(s). OpenPGP historically provides public keyservers which can be used for key retrieval. Additional there are methods to store OpenPGP key information in the Domain Name System (DNS). This specification does not restrict the mechanism of key discovery and retrieval, but compliant clients MUST support the public key announcement as described in XEP-0373 § 4.
After the required public keys have been discovered, XMPP clients engage in an OpenPGP secured IM conversation by exchanging <openpgp/> extension elements. They MUST use the <signcrypt/> OpenPGP content element specified in XEP-0373§ 3.1.
The child elements of the OpenPGP content element's <payload/> can be seen as stanza extension elements which are encrypted and signed. After the <openpgp/> element and the including <signcrypt/>, element was verified, they SHOULD be processed similar as if they had been direct extension elements of the stanza. For example, direct child elements found in <payload/> in the context of IM could be:

- Message bodies (RFC 6121 [4] § 5.2.3): <body xmlns='jabber:client'/>
- Chat State Notifications (XEP-0085) [5]: <active xmlns='http://jabber.org/protocol/chatstates'/>
- XHTML-IM (XEP-0071) [6]: <html xmlns='http://jabber.org/protocol/xhtml-im'/>

But just as with stanza extension elements, child elements of <payload/> can be any extension element. The example above uses the <body/> element as defined in RFC 6121. Note that it uses 'jabber:client' as namespace, but since the same <body/> element is also defined in the 'jabber:server' namespace, recipients MUST accept both.

2.3 OpenPGP Key Handling

2.3.1 Choosing Public Keys

Clients MUST expect multiple public keys to be announced for a single remote entity. In this case all keys MUST be used for encryption.

[4] RFC 6121: Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence <http://tools.ietf.org/html/rfc6121>.
[5] XEP-0085: Chat State Notifications <https://xmpp.org/extensions/xep-0085.html>.
[6] XEP-0071: XHTML-IM <https://xmpp.org/extensions/xep-0071.html>.

2.3.2 OpenPGP Secret Key Synchronization

Clients MAY want to use the mechanism in XEP-0373 § 5 to synchronize their secret key(s) over multiple devices. Thus, they should query the user's PEP service for an eventually stored encrypted secret key.

3 Business Rules

3.1 Always Use <signcrypt/>

Only <signcrypt/> MUST be used for the IM use case. Encrypted but unsigned messages (<crypt/>) do not provide an advantage over unencrypted ones since the sender can not be verified. As result of this rule, the user interface of IM clients implementing the protocol defined herein MUST NOT provide an option for the user to select between sign+crypt, sign or crypt. This also increases the usability.

3.2 Provide Hints

In the IM use case every <message/> equipped with <openpgp/> SHOULD include an unencrypted <body/> explaining that the actual message is encrypted. Furthermore the message SHOULD contain a 'store' hint as defined in Message Processing Hints (XEP-0334) [7] § 4.4 and a "this message contains an encrypted body text" hint in form of an <encryption/> extension element as specified by Explicit Message Encryption (XEP-0380) [8].

Listing 3: An encrypted and signed message with hints.

```
<message to='juliet@example.org'>
  <body>This message is encrypted using OpenPGP.</body>
  <store xmlns='urn:xmpp:hints'/>
  <encryption xmlns='urn:xmpp:eme:0' namespace='urn:xmpp:openpgp:0'/>
  <openpgp xmlns='urn:xmpp:openpgp:0'>
    BASE64_OPENPGP_MESSAGE_CONTAINING_CONTENT_ELEMENT
  </openpgp>
</message>
```

4 IANA Considerations

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

[7] XEP-0334: Message Processing Hints <https://xmpp.org/extensions/xep-0334.html>.

[8] XEP-0380: Explicit Message Encryption <https://xmpp.org/extensions/xep-0380.html>.

[9] The 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

5 XMPP Registrar Considerations

5.1 Protocol Namespaces

The XMPP Registrar [10] includes 'urn:xmpp:openpgp:0' in its registry of protocol namespaces (see <https://xmpp.org/registrar/namespaces.html>).

6 XML Schema

This XEP does not define a Schema, since it exclusively uses elements from XEP-0373 and other XEPs.

7 Acknowledgements

Please refer to the Acknowledgements section of XEP-0373 since the two XEPs where designed together.

<http://www.iana.org/>.

[10] The 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/>.