XEP-0476: Pubsub Signing: OpenPGP Profile

Jérôme Poisson
mailto:goffi@goffi.org
xmpp:goffi@jabber.fr

2022-12-20
Version 0.1.0

Status	Type	Short Name
Experimental	Standards Track	pss-ox

Specifies a pubsub signing profile for OpenPGP

Legal

Copyright

Permissions

Warranty

Liability

Conformance

Contents

1 Introduction

This XMPP extension protocol specifies a profile of Pubsub Signing to use OpenPGP for signature.

2 Signing a Pubsub Item With OpenPGP

Signing an item with OpenPGP requires to have OpenPGP for XMPP (XEP-0373) [1] implemented to handle keys, however this specification uses its own <sign/> element because it uses wrapper element from Pubsub Signing XEP, and signed data MUST NOT be included with the signature.
To sign an element, a client process as explained in XEP-0XXX § Signing a Pubsub Item where the ”signing profile” element used is a <sign/> element qualified by the ’urn:xmpp:pubsub-signing:openpgp:0’ namespace. This element MUST contain a Base64 encoded (RFC 4648 [2] § 4) OpenPGP message as specified in RFC 4880 [3] which MUST contain a **detached signature** as defined in RFC 4880 [4] § 11.4 of the signed data as specified in XEP-0XXX § Signing a Pubsub Item.

Listing 1: Juliet Publishes Her Signature as an Attachment With OpenPGP Signing Profile

```
<iq xmlns="jabber:client" from="juliet@capulet.lit/chamber" to="
    juliet@capulet.lit" id="signature_1" type="set">
  <pubsub xmlns="http://jabber.org/protocol/pubsub">
    <items node="urn:xmpp:pubsub-attachments:1/xmpp:juliet@capulet.lit
        ?;node=urn%3Axmpp%3Amicroblog%3A0;item=random-thoughts-12bd">
      <item id="juliet@capulet.lit">
        <attachments xmlns="urn:xmpp:pubsub-attachments:1">
          <signature xmlns="urn:xmpp:pubsub-signing:0">
            <time stamp="2022-10-16T18:39:03Z"/>
            <signer>juliet@capulet.lit</signer>
            <sign xmlns="urn:xmpp:pubsub-signing:openpgp:0">
                iQGzBAABCAAdFiEEyTOMos/ZmE//
                ikYkAzNxB0kY9CIFAmNaomUACgkQAzNxB0kY9CJQcAv9HjIIrzIhtmWvf2IoHBUgY7hUFP
                +CR4K1GHQB842/
                vjPSHwo5qfVgaVEUK3Liw8eXawOZ4SJeSZdmd1KUjjuZ+
                SLlB1SKKEoap3KFhidT9XYA2OU4tkWOwVI2cyBIWE3JRxD0YFh5YMJObZrOoyMiobwaMaG
                +Yaw1BdYzjO8o2Nw/9
                ledMrwO652Ud4hLGpmSpIJI1NTOjmy5crfhEHMA5ERYDbGbaB/
                IoaHxje+8occlI78xChoz7xCQlwVVyHARvuotEbYRimY78s2Ozae+
                uG/8wQZmeLnrvwCrzDiJbEkW4MbiOWUC1QcApNoW8lriLcb+
                ZfNGMeENSSMqMRfi3wL6WOovM2IR8O97/1DkGFiYAZ414CVZV2ZT+
                xxE64pMM</sign>
```

[1] XEP-0373: OpenPGP for XMPP <https://xmpp.org/extensions/xep-0373.html>.
[2] RFC 4648: The Base16, Base32, and Base64 Data Encodings <http://tools.ietf.org/html/rfc4648>.
[3] RFC 4880: OpenPGP Message Format <http://tools.ietf.org/html/rfc4880>.
[4] RFC 4880: OpenPGP Message Format <http://tools.ietf.org/html/rfc4880>.

```
          </signature>
        </attachments>
      </item>
    </items>
  </pubsub>
</iq>
```

3 Discovering Support

If a client supports the protocol specified in this XEP, it MUST advertise it by including the "urn:xmpp:pubsub-signing:openpgp:0" discovery feature in response to a Service Discovery (XEP-0030) [5] information request:

Listing 2: Service Discovery information request

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

Listing 3: Service Discovery information response

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

4 Security Considerations

Security considerations of OpenPGP for XMPP (XEP-0373) [6] and XEP-0XXX apply.

[5] XEP-0030: Service Discovery <https://xmpp.org/extensions/xep-0030.html>.
[6] XEP-0373: OpenPGP for XMPP <https://xmpp.org/extensions/xep-0373.html>.

5 IANA Considerations

TODO

6 XMPP Registrar Considerations

TODO

7 XML Schema

TODO

8 Acknowledgements

Thanks to NLnet foundation/NGI0 Discovery for funding.