



XMPP

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

This XMPP Extension Protocol is copyright © 1999 – 2024 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 Introduction	1
2 Signing a Pubsub Item With OpenPGP	1
3 Discovering Support	2
4 Security Considerations	2
5 IANA Considerations	3
6 XMPP Registrar Considerations	3
7 XML Schema	3
8 Acknowledgements	3

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//
              ikYkAzNxkY9CIFAmaNaomUACgkQAznXkY9CJQcAv9HjIIrzIhtmWvf2IoHBUgY7hUFP
              +CR4K1GHQB842/
              vjPSHwo5qfVgaVEUK3Liw8eXawOZ4SJeSZdmd1KUjjuZ+
              SLlB1SKKEoap3KFhidT9XYA2OU4tkW0wVI2cyBIWE3JRxD0YFh5YMJObZrOoyMiobwaMaG
              +Yaw1BdYzj08o2Nw/9
              ledMrw0652Ud4hLGpmSpIJI1NTOjmy5crfhEHMA5ERYDbGbaB/
              IoaHxje+8occlI78xChoz7xCQlwVVyHARvuotEbYRimY78s20zae+
              uG/8wQZmeLnrvwCrzDiJbEkW4Mbi0WUC1QcApNoW8lriLcb+
              ZfNGMeENSSMqMRfi3wL6W0ovM2IR8097/1DkGFiyAZ414CVZV2ZT+
              xxE64pMM</sign>
            </sign>
          </signature>
        </attachments>
      </item>
    </items>
  </pubsub>
</iq>
```

¹XEP-0373: OpenPGP for XMPP <<https://xmpp.org/extensions/xep-0373.html>>.

²RFC 4648: The Base16, Base32, and Base64 Data Encodings <<http://tools.ietf.org/html/rfc4648>>.

³RFC 4880: OpenPGP Message Format <<http://tools.ietf.org/html/rfc4880>>.

⁴RFC 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.

⁵XEP-0030: Service Discovery <<https://xmpp.org/extensions/xep-0030.html>>.

⁶XEP-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.