XEP-0420: Stanza Content Encryption

Paul Schaub
mailto:vanitasvitae@fsfe.org
xmpp:vanitasvitae@jabberhead.tk

2019-10-04
Version 0.2.0

<table>
<thead>
<tr>
<th>Status</th>
<th>Type</th>
<th>Short Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Experimental</td>
<td>Standards Track</td>
<td>SCE</td>
</tr>
</tbody>
</table>

The Stanza Content Encryption (SCE) protocol is intended as a way to allow clients to securely exchange arbitrary extension elements using different end-to-end encryption schemes.
Legal

Copyright

This XMPP Extension Protocol is copyright © 1999 – 2019 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 Requirements 1
3 Glossary 1
4 Affix Elements 2
5 Motivation 3
6 Use Cases 5
   6.1 Use in `<message/>` stanzas 5
   6.2 Use in `<iq/>` stanzas 5
7 Sending an encrypted stanza 8
8 Receiving an encrypted stanza 8
9 Blacklist 8
10 Business Rules 10
11 Implementation Notes 10
12 Security Considerations 10
   12.1 Encryption Profiles 11
13 XMPP Registrar Considerations 11
14 XML Schema 11
1 Introduction

There is a number of different end-to-end encryption mechanisms that can be used to secure user communication against unauthorized access from malicious third parties. Popular examples for this are OMEMO Encryption (XEP-0384)\(^1\) and OpenPGP for XMPP (XEP-0373)\(^2\). While the latter allows for encryption of arbitrary extension elements, protocols such as OMEMO Encryption (XEP-0384)\(^3\) are limited to only encrypt the body of a message. This approach is not very flexible and prevents the combined usage with XMPP extension protocols such as Stateless Inline Media Sharing (XEP-0385)\(^4\) or Last Message Correction (XEP-0308)\(^5\) as their extension elements cannot be included in the encrypted part of the message, therefore leaking information about the message content.

This extension protocol proposes a solution to aforementioned issues by generalizing the OpenPGP Content Elements (eg. `<signcrypt>`) introduced by OpenPGP for XMPP (XEP-0373)\(^6\) for the use with other encryption protocols.

2 Requirements

This proposal widens the scope of the security guarantees given by the used encryption mechanism from just the body of the message to all contents of the `<content/>` element. It is intended to serve as a "one size fits all" solution for extension element encryption in XMPP. In order to achieve its goal, Stanza Content Encryption does the following:

- Define elements that hold sensitive information
- Specify rules about how extension elements are encrypted and embedded in the message
- Specify rules about which elements are allowed inside and outside the protected domain

3 Glossary

**Envelope Element `<envelope/>`** An XMPP extension element which is used to hold the encrypted `<content/>` element.

**Content Element `<content/>`** An element which is used to contain all of those extension elements that need to be encrypted. The XML representation of this element is encrypted and then embedded into the `<envelope/>` element.

---

4 Affix Elements

In order to prevent certain attacks, different affix elements MAY be added into the `<content/>` element.

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
<th>Usage</th>
<th>Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;rpad/&gt;</code></td>
<td>Random-length random-content padding</td>
<td>Prevent known cipher-text and message length correlation attacks. The content of this element is a randomly generated sequence of base64 characters of random length between 0 and 200 characters. TODO: sane boundaries?</td>
<td>None. This element is only used to change the length of the ciphertext and doesn't need to be verified</td>
</tr>
<tr>
<td><code>&lt;time/&gt;</code></td>
<td>Timestamp</td>
<td>Prevent replay attacks using old messages. This element MUST have one attribute 'stamp', whose value is a timestamp following the format described in XMPP Date and Time Profiles (XEP-0082) XEP-0082: XMPP Date and Time Profiles <a href="https://xmpp.org/extensions/xep-0082.html">https://xmpp.org/extensions/xep-0082.html</a>. The timestamp represents the time at which the message was encrypted by the sender.</td>
<td>Receiving clients MUST check whether the difference between the timestamp and the sending time derived from the stanza itself lays within a reasonable margin. The client SHOULD use the content of the timestamp element when displaying the send date of the message</td>
</tr>
<tr>
<td><code>&lt;to/&gt;</code></td>
<td>Recipient of the message</td>
<td>Prevent spoofing of the recipient. This element MUST have one attribute 'jid', whose value is the JID of the intended recipient.</td>
<td>Receiving clients MUST check, if the JID matches the to attribute of the enclosing stanza and otherwise alert the user/reject the message</td>
</tr>
</tbody>
</table>
5 Motivation

Some end-to-end encryption protocols like OMEMO Encryption (XEP-0384) are historically limited to encryption of the message body only. This approach excludes other extension elements from the protected domain of the payload element, exposing them to potential attackers.

Listing 2: An imperfectly encrypted message which leaks dangerous information about the conversation through the plaintext OOB extension element

```
<message from='narrator@jabber.org' to='viewer@jabber.org'>
  <encrypted xmlns='eu.siacs.conversations.axolotl'>
  
  </header>
  <payload>
  SSBnb3QgaW4gZXZlcn1vbmUncyBob3N0aWxlIGxpdHRsZSBmYWNlLiBZZXMsIHRoZXNlIGFyZSBi
cnVpc2VzIGZyb20gZm1naHRpbmcuIFllcywgSSdtIGNvbWZvcnRhYmxlIHdpdGggdGhhdC4gSSBh
  bSBiSmxkdZ2h0ZW51ZC4=
  </payload>
</message>
```

Encryption protocols that make use of Stanza Content Encryption MUST define their own profiles that describe mandatory behaviour of which of these elements are used. They MAY also define and add their own specific affix elements.

```
Listing 1: Examples of Affix Elements

<time stamp='2004-01-25T06:05:00+01:00'/>
<to jid='missioncontrol@houston.nasa.gov'/>
<from jid='opportunity@mars.planet'/>
<rpad>C1DH9NHK-9A25SmwK4HUI;jji9%GYK^sy1HJ7Tn14</rpad>
```

5 MOTIVATION

The example above obviously leaks information about the communication through the unencrypted OOB extension element. Most end-to-end encryption mechanisms are also focussed solely on message content encryption and do not tackle <iq/> requests/replies at all. Stanza Content Encryption can be applied to those as well.

Listing 3: Unencrypted IQ request

```xml
<iq from='doctor@shakespeare.lit/pda'
    id='get-data-1'
    to='ladymacbeth@shakespeare.lit/castle'
    type='get'>
    <data xmlns='urn:xmpp:bob'
        cid='sha1+8f35fef110fffc5df08d579a50083ff9308fb6242@bob.xmpp.org'/>
</iq>
```

Listing 4: Likewise unencrypted reply

```xml
<iq from='ladymacbeth@shakespeare.lit/castle'
    id='get-data-1'
    to='doctor@shakespeare.lit/pda'
    type='result'>
    <data xmlns='urn:xmpp:bob'
        cid='sha1+8f35fef110fffc5df08d579a50083ff9308fb6242@bob.xmpp.org'
        max-age='86400'
        type='image/png'>
        iVBORw0KGgoAAAANSUhEUgAAAAoAAAAKCAYAAACNMs+9AAAABGdBTUEAALGP
        C/xhBQAAAAALwSFlzAAALEwAACxMBAJqcGAAAAAd0SU1FB9YGARc5KB0XV+IA
        AAAAdEYVdEnvbw11bQQAQJ1YXr1CB3aXRoIFRoZSBHSU1Q72Q1bgAAAF1J
        REFUGNO9zLONg1AxPEfdLTs4BZM4DI04C70wQg2Jo9LE1exdIyvB8eZ7jg
        ch9/q1uH4TLzw4d6+ErXMMcXuHWxId3KOEEnnXXV6MJpcq2MLaI97CER3N0
        vr4MkhoXe0rZigAAAAABJRUS5ErkJggg==
    </data>
</iq>

6 Use Cases

6.1 Use in <message/> stanzas

The main use case of Stanza Content Encryption is the use of end-to-end encryption protocols in combination with extension protocols that store sensitive information in other places than the message body. This applies to many extension elements that add additional information to <message/> stanzas, such as those of Out-of-Band Data (XEP-0066) \(^8\).

Listing 5: Content element containing the messages body and the OBB element.

```xml
<content xmlns='urn:xmpp:sce:0'>
  <payload>
    <body xmlns='jabber:client'>[...]</body>
    <x xmlns='jabber:x:oob'>
      <url>https://en.wikipedia.org/wiki/Fight_Club#Plot</url>
    </x>
  </payload>
</content>
```

Listing 6: Finished message stanza containing the <content/> element from the previous example encrypted using a hypothetical encryption protocol and SCE.

```xml
<message from='narrator@jabber.org' to='viewer@jabber.org'>
  <encrypted xmlns='urn:xmpp:encryption:stub:sce:0'>
    <payload>
      PGNvbnRlbmQgeG1sbnM9J3Vybjp4bXBwOnNjZTowJz48cGF5bG9hZD48Ym9keSB4bWxucz0namFiYmVyOmNsaWVuV3Cc+SSBb3QgaW4gZXZlcn1vbmUncyBob3N0aWxlIGxpHRsZSBmYW1lIBZZXMSIHRoZXNhIGFyZSBicnVpc2VzIGZyb20gZmlnaHRpbmcuIFllcywgSSdtIGNvbWZvcmRhYWx1IHdpcGggdGhhdC4gSSBhbiBSb29pZ2h0ZW51Y2hpbmRzL2JvZHkiCg=</payload>
  </encrypted>
</message>
```

6.2 Use in <iq/> stanzas

Stanza Content Encryption thrives not only to allow for rich content encryption in <message/> stanzas, but is also applicable to <iq/> queries. A resource might want to query sensitive

information from another resource capable of Stanza Content Encryption.

Listing 7: Sender prepares a <content/> element containing the query subject.

```xml
<content xmlns='urn:xmpp:sce:0'>
    <payload>
        <data xmlns='urn:xmpp:obob'
            cid='sha1+8f35fef110ffe5df08d579a50083ff9308fb62420bob.xmpp.org'/>
    </payload>
    <from jid='doctor@shakespeare.lit/pda'/>
    <to jid='ladymacbeth@shakespeare.lit/castle'/>
</content>
```

Listing 8: The sender then encrypts the <content/> element for the recipient and sends the <iq/> containing the result of the encryption.

```xml
<iq from='doctor@shakespeare.lit/pda'
    id='get-data-1'
    to='ladymacbeth@shakespeare.lit/castle'
    type='get'>
    <encrypted xmlns='urn:xmpp:encryption:stub:sce:0'>
        <payload>
            V2FpdCwgd2hhdD8gQXJlIHlvdSBzZXJpb3VzPyBEaWQgeW91IHJlYXseSBqdXN0IGdyYW1geW91ciBmYXZvdXJpdGUyUmFzZTY0IjY29kZXIganVzdCBybBjaGVjayB0aGlzIGRvY3VtZW50IGZvciBoYWZ4gbVzc2FnZXM/IFdoYXQgYXJlIHlvdSBzb21lIGtpbmQgb2YgbmVyZD8gU29tZSBnZWVrIHdpdGggYSBiaW5hcnkgd3Jpc3Qgd2F0Y2g/
        </payload>
    </encrypted>
</iq>
```

Listing 9: The recipient prepares the reply to the request by assembling the <content/> element.

```xml
<content xmlns='urn:xmpp:sce:0'>
    <payload>
        <data xmlns='urn:xmpp:obob'
            cid='sha1+8f35fef110ffe5df08d579a50083ff9308fb62420bob.xmpp.org'
            max-age='86400'
            type='image/png'>
            iVBORw0KGgoAAAANSUhEUgAAAAoAAAAKCAMAAAC67D+/IFdoYXQgYXJlIHlvdSBzb21lIGtpbmQgb2YgbmVzD8gU29tZSBnZWVrIHdpdGggYSBiaW5hcnkgd3Jpc3Qgd2F0Y2g/
        </payload>
</content>
```
Listing 10: The <content/> element is then encrypted and sent as a reply to the initiator of the request.

```xml
<iq from='ladymacbeth@shakespeare.lit/castle' id='get-data-1' to='doctor@shakespeare.lit/pda' type='result'>
  <encrypted xmlns='urn:xmpp:encryption:stub:sce:0'>
    <payload>
      PGNvbnRlbnQgeG1sbnM9J3Vybjp4bXBwOnNjZTowJzZKICA8cGF5bG9hZD4KICAgIDxkYXRhIHhtbG5zPSd1cm46eG1wcDpib2InCiAgICA8L2RhdGE + CiAgICBpVkJPcncwS0dnb0FBQUFOU1VoRVVnQUF BQW9BUFBS0NBTUBQUM2N0QrUEFBQFjbeJNVkVVQUFBRFlaQXJmYUE5R01Bb0JBQ0UdOciAgICBR QTNNWgduaWFBaUVPZ1pNSUFUFSWpaaEhVWkJISVhoRHJiUTZzVVE3T11BMR5QXViUndxTVFR cTdUWxLSGdNQUFBszVXUmZKCIAgICBQZk9PUkJGb01CQ3dVUS95Y0E2R1BndmJaaVB1SdsTkR bXJUUWVPUGdReU3UjZNd0FDQQUFCLU1BFL29BUQFBVzBVsfRVFUUkxeFhJCIAgICBSezZFTUUQVVQ OGtKS0B0bmFGRjduOUZRUUE5DZWtB3prbGhnQ3dmcmxOSEVYaHJ2Q3N4VYuU3dM9GFdUIXWkZw QkVSDettOVhmcIagICBkUkgdLZxaDQTF3nSHJzQXRodDA5NWiRZ2VZULNsNTdSFNQZ1AzK0N3 dkFQUBQJUKU1UTRXJsrmdnZz09CiAgICA8L2RhdGE + CiAgPC9wYXlsb2FkPgogIDxmcmt9IGpp ZD0nbGFkeW1hY2J1dGhAc2hha2VzcGVhc15saQy2FzdgX1Jy8 + CiAgPRVgGppZD0nZG9jdG9y QHNoYWtlc3BlY3IjLmxpdC9wZGEvLz4KPC9jb25OZW50Pg0=
    </payload>
  </encrypted>
</iq>
```
7 Sending an encrypted stanza

In order to send an encrypted message without leaking extension elements the sender prepares the message by placing the sensitive extension elements inside a `<payload/>` element inside another `<content/>` element. Depending on the encryption-specific SCE-profile, some affix elements are added as child elements of the `<content/>` element. The `<content/>` element is then serialized into XML and encrypted using the SCE-specific profile of the encryption mechanism in place. The result is appended to the message. Since the outer message element does not contain a `<body/>` element the sender appends an unencrypted `<store/>` hint as specified in Message Processing Hints (XEP-0334) 9. The message can then be sent to the recipient.

8 Receiving an encrypted stanza

The recipient of the message decrypts the content of the `<envelope/>` element to retrieve the `<content/>` element. Depending on the affix profiles specified by the used encryption protocol, the affix elements are verified to prevent certain attacks from taking place. Next the extension elements of the `<content/>` elements `<payload/>` element are checked against the whitelist/blacklist and any disallowed elements are discarded. As a last step, the original unencrypted stanza is recreated by replacing the `<envelope/>` element of the stanza with the contents of the `<payload/>` element.

9 Blacklist

The receiving client MUST ignore certain elements that may allow for attacks to take place. Since it is hard to come up with a complete list of blacklisted elements, a general rule of thumb would be the following: Blacklisted are all elements that need to be read by the server at some point. Below is an additional list of elements that are definitely forbidden inside the `<content/>` element and MUST instead be placed in the message unencrypted.

---

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Origin-ID elements of Unique and Stable Stanza IDs (XEP-0359)</td>
<td>XEP-0359: Unique and Stable Stanza IDs <a href="https://xmpp.org/extensions/xep-0359.html">https://xmpp.org/extensions/xep-0359.html</a>. These IDs may be used to identify a message even though it cannot be decrypted.</td>
</tr>
</tbody>
</table>

TODO: Other elements?
10 Business Rules

Unencrypted `<content/>` elements are NOT ALLOWED as child elements of the stanza and MUST be dropped.
Elements in the `<content/>` elements `<payload/>` element MUST be identified using an element name and namespace. Notably the `<body/>` element MUST contain a valid namespace (i.e. "jabber:client").
The recipient must verify that the decrypted `<content/>` element contains valid XML before processing it any further. Invalid XML must be rejected.
After verifying the integrity of the `<content/>` element, the recipient needs to make sure that no blacklisted elements are found within the payload. Any forbidden elements MUST be dropped before the message is processed any further.
Furthermore the receiving client MUST ignore any extension elements considered as sensitive which are found outside of the `<content/>` element, especially as direct unencrypted child elements of the enclosing stanza.
Duplicate elements within the `<content/>` element MUST be dropped.
Elements in the `<content/>` element override elements in the enclosing stanza. TODO: Maybe we want to remove this rule by disallowing duplicate elements all together?
Since a message encrypted with SCE MUST NOT contain a `<body/>` element, it is not eligible for MAM message storage (Message Archive Management (XEP-0313) \(^{10}\)). Therefore sending entities MUST append an unencrypted Message Processing Hints (XEP-0334) \(^{11}\) `<store/>` hint as a direct child element to the message.

11 Implementation Notes

As a first, naïve approach a recipient of a message containing an `<envelope/>` element could simply reinject the reassembled unencrypted stanza into the XML stream. This might introduce some security issues. Most notably, there is no way to distinguish end-to-end encrypted elements from unencrypted elements.
Implementations should rather handle encrypted elements explicitly.

12 Security Considerations

For the sake of simplicity, the examples in this document are not encrypted. A real-world implementation MUST make use of real cryptographic protocols.

12.1 Encryption Profiles

This specification presents a set of affix elements which can be used to counter certain attacks. However it does not dictate any behaviour regarding what elements MUST be used/verified or when.
Different cryptographic protocols come with different possible attack scenarios which must be taken into consideration, so it is left up to those cryptographic protocols to define profiles that describe the use of affix elements.

13 XMPP Registrar Considerations

TODO: Maybe the Registrar should handle a blacklist of elements that are allowed as child elements of the <content/> element?

14 XML Schema

TODO.