XEP-0397: Instant Stream Resumption

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

2018-11-03
Version 0.1.1

Status	Type	Short Name
Deferred	Standards Track	isr

This specification introduces a mechanism for instant stream resumption, based on Stream Management (XEP-0198), allowing XMPP entities to instantaneously resume an XMPP stream.

Legal

Copyright

Permissions

Warranty

Liability

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

This XEP specifies an instant stream resumption mechanism based on Stream Management (XEP-0198) [1], allowing XMPP entities to instantaneously resume an XMPP stream. This can be seen as the complementary part to XMPP Quickstart (XEP-0305) [2] allowing for fast XMPP session (re-)establishment.
Compared to the existing stream resumption mechanism of XEP-0198 § 5, the approach defined herein reduces the round trips required to resume a stream to exactly *one*. This is achieved by using just a secure short-lived token to resume the stream.

2 Glossary

ISR Instant Stream Resumption.

Instant Stream Resumption Token (ISR Token) A shared secret that is exclusively ephemeral and represented as string.

TLS Transport Layer Security (RFC 5246 RFC 5246: The Transport Layer Security (TLS) Protocol Version 1.2 <http://tools.ietf.org/html/rfc5246>.).

3 Stream Feature

XMPP entities providing Instant Stream Resumption MUST announce that functionality as stream feature, but only if an instant stream resumption is possible at this stage. The ISR stream future consists of an <isr/> element qualified by the 'htpps://xmpp.org/extensions/isr/0' namespace. And since ISR requires TLS, this means that the <isr/> stream feature only appears on TLS secured connections.
The ISR stream feature element MUST contain a <mechanisms/> element as defined in RFC 6120 [3]. This element contains the SASL mechanism which are available to be used for instant stream resumption.

Listing 1: Server announces the Instant Stream Resumption Stream Feature

```
<stream:stream
  from='example.com'
  xmlns='jabber:client'
  xmlns:stream='http://etherx.jabber.org/stream'
  version='1.0'>

<stream:features>
  <bind xmlns='urn:ietf:params:xml:ns:xmpp-bind'/>
```

[1] XEP-0198: Stream Management <https://xmpp.org/extensions/xep-0198.html>.
[2] XEP-0305: XMPP Quickstart <https://xmpp.org/extensions/xep-0305.html>.
[3] RFC 6120: Extensible Messaging and Presence Protocol (XMPP): Core <http://tools.ietf.org/html/rfc6120>.

```
  <sm xmlns='urn:xmpp:sm:3'/>
  <isr xmlns='https://xmpp.org/extensions/isr/0'>
    <mechanisms xmlns='urn:ietf:params:xml:ns:xmpp-sasl'>
      <mechanism>HT-SHA-256-ENDP</mechanism>
    </mechanisms>
  </isr>
</stream:features>
```

Every ISR enabled entity SHOULD support the HT-SHA-256-ENDP mechanism, support for HT-SHA-256-UNIQ is RECOMMENDED. The family of HT SASL mechanisms is specified in draft-schmaus-sasl-ht-03[4].

4 Obtaining a Instant Stream Resumption Token

In order to obtain an ISR token, the requesting entity must add an 'isr-enable' element qualified by the 'htpps://xmpp.org/extensions/isr/0' namespace to the <enable/> element as defined in Stream Management (XEP-0198) [5] when attempting to enable Stream Management. This <isr-enable/> element MUST contain a 'mechanism' attribute containing the name of the SASL mechanism the requesting entity will use when performing ISR with the returned token. The entities involved in ISR MUST only use or allow this mechanism when performing ISR with the according token. This effectively pins the SASL mechanism [6].

Listing 2: An <enable/> Nonza with the ISR 'mechanism' element

```
<enable xmlns='urn:xmpp:sm:3'>
  <isr-enable xmlns='https://xmpp.org/extensions/isr/0' mechanism='HT-
      SHA-256-ENDP'/>
</enable>
```

Next, the <enabled/> Nonza (see Nonzas (are not Stanzas) (XEP-0360) [7]) which is sent as positive reply upon a request to enable Stream Management, MUST contain an 'isr-enabled' element qualified by the 'https://xmpp.org/extensions/isr/0' namespace containing a ISR token as value of its 'token' attribute. The token MUST be newly generated by a cryptographically secure random number generator and MUST contain at least 128 bit of entropy. The <isr-enabled/> element can optionally also contain a 'location' attribute which specifies the preferred IP address or hostname, and a TCP port number of the host which should be used for instant stream resumption.

Listing 3: An <enabled/> Nonza with a ISR token

[4] draft-schmaus-sasl-ht-03: The Hashed Token SASL Mechanism <https://tools.ietf.org/html/draft-schmaus-kitten-sasl-ht-03>.
[5] XEP-0198: Stream Management <https://xmpp.org/extensions/xep-0198.html>.
[6] Pinning the SASL mechanism is believed to increase the security
[7] XEP-0360: Nonzas (are not Stanzas) <https://xmpp.org/extensions/xep-0360.html>.

```
<enabled xmlns='urn:xmpp:sm:3'>
  <isr-enabled xmlns='https://xmpp.org/extensions/isr/0' token='
     a0b9162d-0981-4c7d-9174-1f55aedd1f52'/>
</enabled>
```

Listing 4: An <enabled/> Nonza with a ISR token and location

```
<enabled xmlns='urn:xmpp:sm:3'>
  <isr-enabled xmlns='https://xmpp.org/extensions/isr/0'
               token='a0b9162d-0981-4c7d-9174-1f55aedd1f52'
               location='isr.example.org:5222'/>
</enabled>
```

The <enabled/> Nonza containing an ISR token MUST only be sent over TLS secured connections.

5 Instant Stream Resumption

In order to instantaneously resume an XMPP stream the initiating entity, which is either an XMPP client or server, must posses a valid ISR token. After it has obtained the ISR token, using the process described in the previous section, it first determines the host for resumption, and after that, tries to perform the instant stream resumption.

5.1 Determing the Host for Resumption

The lookup mechanism order to determine host candidates for ISR resumption is as follows:

1. The host provided in the optional 'location' attribute qualified by the 'https://xmpp.org/extensions/isr/0' namespace found in the <enabled/> element of XEP-0198 (the "isr:location").
2. The hosts determined by means of SRV records for XMPP over TLS (XEP-0368) [8].
3. The host announced in the 'location' attribute of the <enabled/> Nonza defined in XEP-0198.
4. Standard host lookup mechanisms.

The host candidates retrieved by those mechanisms SHOULD be tried by the initiating entity in this order.
Note that the hosts announced by the 'location' attribute qualified by the 'https://xmpp.org/extensions/isr/0' namespace MUST be connected to using TLS from

[8] XEP-0368: SRV records for XMPP over TLS <https://xmpp.org/extensions/xep-0368.html>.

the beginning, i.e. <starttls/> MUST NOT be used, instead the TLS handshake is performed right after establishing the connection.
This order prefers hosts which allow connections where TLS is enabled from the beginning. This is desirable to reduce the required round trips by skipping the <starttls/> step.

5.2 Performing Instant Stream Resumption

After the remote host on which the instant stream resumption should be performed was determined, the initiating entity connects to the host, and establishes TLS by either

1. establishing a TLS session right away, or
2. performing STARTTLS (RFC 6120 [9] § 5).

Now the initiating entity sends an XMPP <stream> open element followed by a <authenticate/> Nonza as specified in the Extensible SASL Profile (XEP-0388) [10]. The initiating entity must also provide a <inst-resume/> element qualified by the 'https://xmpp.org/extensions/isr/0' namespace, which must contain a <resume/> element as defined in Stream Management (XEP-0198) [11].
The only defined attributed of the <inst-resume/> element is the 'with-isr-token' attribute, whose value, if omitted, defaults to 'true'. If is set to 'false', then the SASL mechanism is performed as when traditionally authenticating the XMPP session. If the value of the attribute is 'true' then the "password" given to the SASL mechanism is the ISR token. Note that this implies that only SASL mechanisms which take a password/token can be used this way.

Listing 5: Initiating entity requests instant stream resumption via the Extensible SASL Profile (XEP-0388)

```
<?xml version='1.0'?>
<stream:stream
    from='juliet@im.example.com'
    to='im.example.com'
    version='1.0'
    xml:lang='en'
    xmlns='jabber:client'
    xmlns:stream='http://etherx.jabber.org/streams'>

<authenticate xmlns='urn:xmpp:sasl:1' mechanism='HT-SHA-256-ENDP'>
  <initial-response>[base64 encoded SASL data]</initial-response>
  <inst-resume xmlns='https://xmpp.org/extensions/isr/0' with-isr-
     token='true'/>
    <resume xmlns='urn:xmpp:sm:3'
```

[9] RFC 6120: Extensible Messaging and Presence Protocol (XMPP): Core <http://tools.ietf.org/html/rfc6120>.
[10] XEP-0388: Extensible SASL Profile <https://xmpp.org/extensions/xep-0388.html>.
[11] XEP-0198: Stream Management <https://xmpp.org/extensions/xep-0198.html>.

```
            h='some-sequence-number'
            previd='some-long-sm-id'/>
  </inst-resume>
</authenticate>
```

Note that the initiating entity SHOULD pipeline the instant stream resumption request together with then initial <stream> open element. The initiating entity is able to do so since it already knows that the service supports ISR because it announced an ISR token.
Servers MUST destroy the ISR token of a stream after an instant stream resumption was attempted for that stream with an invalid ISR token. Server implementations MUST implement the ISR token comparision in linear runtime.

5.2.1 Successful Stream Resumption

Listing 6: Successful Instant Stream Resumption

```
<success xmlns='urn:xmpp:sasl:1'>z
  <additional-data></additional-data>
  <inst-resumed xmlns='https://xmpp.org/extensions/isr/0'
                token='006b1a29-c549-41c7-a12c-2a931822f8c0'>
    <resumed xmlns='urn:xmpp:sm:3' h='354' previd='123'/>
  </inst-resumed>
</success>
```

On success the server replies with a <success/> nonza as specified in the Extensible SASL Profile (XEP-0388) [12], which must include a <inst-resumed/> element qualified by the 'https://xmpp.org/extensions/isr/0' namespace. This element MUST contain a *new* ISR Token found in the 'token' attribute. It also MUST include a <resumed/> as specified in Stream Management (XEP-0198) [13] containing the sequence number of the last by Stream Management handled stanza in the 'h' attribute and the 'previd' attribute.
In case of an successful Instant Stream Resumption authenticated by an ISR token, the server MUST immediately destroy the ISR token after authentication, i.e., it MUST no longer be possible to perform an ISR using that ISR token and Stream Management ID (SM-ID, see Stream Management (XEP-0198) [14]) tuple.
After the <inst-resumed/> was received and has been verified both entities MUST consider the resumed stream to be re-established. This includes all previously negotiated stream features like Stream Compression (XEP-0138) [15]. It does however not include the specific state of the features: For example in case of Stream Compression, the dictionary used by the compression mechanism of the resumed stream MUST NOT be considered to be restored after instant stream resumption.
Note that this behavior is different from Stream Management (XEP-0198) [16] stream resump-

[12] XEP-0388: Extensible SASL Profile <https://xmpp.org/extensions/xep-0388.html>.
[13] XEP-0198: Stream Management <https://xmpp.org/extensions/xep-0198.html>.
[14] XEP-0198: Stream Management <https://xmpp.org/extensions/xep-0198.html>.
[15] XEP-0138: Stream Compression <https://xmpp.org/extensions/xep-0138.html>.
[16] XEP-0198: Stream Management <https://xmpp.org/extensions/xep-0198.html>.

tion, where ”outer stream” features like compression are not restored. Since such a behavior would be counterproductive towards the goal of this XEP, it specifies that the negotiation state of such ”outer stream” features is also restored (besides the features which where already negotiated at ISR-time, i.e. TLS).

5.2.2 Successful Authentication but failed Stream Resumption

If the server was able to authenticate the initiating entity but is unable to resume the stream instantly it MUST reply with a <success/> Nonza as defined in the Extensible SASL Profile (XEP-0388) [17] containing a <inst-resume-failed/> element qualified by the ’https://xmpp.org/extensions/isr/0’ namespace. This <inst-resume-failed/> MUST contain a <failed/> element as defined in Stream Management (XEP-0198) [18].

Listing 7: Server indicates instant stream resumption failure

```
<success xmlns='urn:xmpp:sasl:1'>
  <inst-resume-failed xmlns='https://xmpp.org/extensions/isr/0'>
    <failed xmlns='urn:xmpp:sm:3'
            h='another-sequence-number'>
      <item-not-found xmlns='urn:ietf:params:xml:ns:xmpp-stanzas'/>
    </failed>
  </inst-resume-failed>
</sucess>
```

Instant stream resumption errors SHOULD be considered recoverable, the initiating entity MAY continue with normal session establishment; however, misuse of stream management MAY result in termination of the stream. Since the initiating entity is authenticated, it could continue with resource binding by using RFC 6120 [19] § 7. or Bind 2.0 (XEP-0386) [20].

5.2.3 Multi step authentication ISR

As specified in the Extensible SASL Profile (XEP-0388) [21] § 2.6.3, sole SASL authentication may not be sufficient for authentication. In this case, the remote entity sends a <continue/> element as defined in Extensible SASL Profile (XEP-0388) [22] to request the local entity to perform another task.

Listing 8: Server requires Multi SASL Mechanism ISR

[17] XEP-0388: Extensible SASL Profile <https://xmpp.org/extensions/xep-0388.html>.
[18] XEP-0198: Stream Management <https://xmpp.org/extensions/xep-0198.html>.
[19] RFC 6120: Extensible Messaging and Presence Protocol (XMPP): Core <http://tools.ietf.org/html/rfc6120>.
[20] XEP-0386: Bind 2.0 <https://xmpp.org/extensions/xep-0386.html>.
[21] XEP-0388: Extensible SASL Profile <https://xmpp.org/extensions/xep-0388.html>.
[22] XEP-0388: Extensible SASL Profile <https://xmpp.org/extensions/xep-0388.html>.

```
<continue xmlns='urn:xmpp:sasl:1'>
  <additional-data>
   T3B0aW9uYWwgQmFzZSA2NCBlbmNvZGVkIFNBU0wgc3VjY2VzcyBkYXRh
  </additional-data>
  <tasks>
    <task>HOTP-EXAMPLE</task>
    <task>TOTP-EXAMPLE</task>
  <tasks>
</continue>
```

5.2.4 Failed ISR Authentication

If the server is unable to authenticate the initiating entity it replies with a <failure/> Nonza as defined in Extensible SASL Profile (XEP-0388) [23]. The server MUST delete any state of the stream which was attempted to resume in case the SM-ID was correct but the authentication failed.[24]

Listing 9: Server indicates instant stream resumption failure

```
<failure xmlns='urn:xmpp:sasl:1'>
    <not-authorized xmlns='urn:ietf:params:xml:ns:xmpp-sasl'/>
</failure>
```

After the ISR authentication has failed, the initiating entity could continue with normal authentication (Extensible SASL Profile (XEP-0388) [25], ...).

6 Security Considerations

Any ISR data SHALL NOT be part of TLS 1.3 0-RTT early data. (TODO: Shall we weaken this requirement to allow early data?. It would be technically possible if the sender does not add additional data, for example Stanzas, after the ISR/XEP-0388 data at the end of the early data. And if the receiver does ensure that the existence of such additional data is causing an ISR failure.)
It is of vital importance that the Instant Stream Resumption Token is generated by a cryptographically secure random generator. See RFC 4086 [26] for more information about Randomness Requirements for Security.

[23] XEP-0388: Extensible SASL Profile <https://xmpp.org/extensions/xep-0388.html>.
[24] This is to prevent brute force attacks.
[25] XEP-0388: Extensible SASL Profile <https://xmpp.org/extensions/xep-0388.html>.
[26] RFC 4086: Randomness Requirements for Security <http://tools.ietf.org/html/rfc4086>.

7 IANA Considerations

This document requires no interaction with the Internet Assigned Numbers Authority (IANA) [27].

8 XMPP Registrar Considerations

The XMPP Registrar [28] includes 'https://xmpp.org/extensions/isr/0' in its registry of protocol namespaces (see <https://xmpp.org/registrar/namespaces.html>).

9 XML Schema

TODO: Add after the XEP leaves the 'experimental' state.

10 Acknowledgements

Thanks to Jonas Wielicki, Thijs Alkemade, Dave Cridland, Maxime Buquet, Alexander Würstlein, Sam Whited and Ivan Vučica for their feedback.

[27] 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 <http://www.iana.org/>.

[28] 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/>.