



XMPP

XEP-0170: Recommended Order of Stream Feature Negotiation

Peter Saint-Andre
<mailto:xsf@stpeter.im>
<xmpp:peter@jabber.org>
<http://stpeter.im/>

2007-01-04
Version 1.0

Status	Type	Short Name
Active	Informational	N/A

This document specifies a recommended order for negotiation of XMPP stream features.

Legal

Copyright

This XMPP Extension Protocol is copyright © 1999 – 2018 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	Client-to-Server Recommendations	1
2.1	Standard XMPP Features	1
2.2	Stream Compression	1
2.3	In-Band Registration	2
3	Server-to-Server Recommendations	2
3.1	Standard XMPP Features	2
3.2	Dialback	3
3.3	Stream Compression	3
4	Security Considerations	3
5	IANA Considerations	4
6	XMPP Registrar Considerations	4

1 Introduction

During its formalization of the core Jabber protocols, the IETF's XMPP WG introduced the concept of XML stream features. While the order in which features shall be negotiated is clearly defined for the features specified in [RFC 3920](#)¹ and [RFC 3921](#)², the number of possible features is open-ended (which is why the [XMPP Registrar](#)³ maintains a registry of stream features). This document specifies the recommended order for negotiation of various stream features.

2 Client-to-Server Recommendations

2.1 Standard XMPP Features

The XMPP RFCs define an ordering for the features defined therein, namely:

1. TLS
2. SASL
3. Resource binding

That order **MUST** be followed if no other stream features are negotiated.

2.2 Stream Compression

[Stream Compression \(XEP-0138\)](#)⁴ is negotiated when it is not possible to set up TLS compression for whatever reason. It seems safest to negotiate stream compression after negotiation of both TLS (to safely complete the negotiation) and SASL (to prevent certain denial-of-service attacks caused by consumption of server resources for compression before the connecting entity is authenticated). Therefore the following order is **RECOMMENDED**:

1. TLS
2. SASL
3. Stream compression
4. Resource binding

¹RFC 3920: Extensible Messaging and Presence Protocol (XMPP): Core <<http://tools.ietf.org/html/rfc3920>>.

²RFC 3921: Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence <<http://tools.ietf.org/html/rfc3921>>.

³The 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/>>.

⁴XEP-0138: Stream Compression <<https://xmpp.org/extensions/xep-0138.html>>.

2.3 In-Band Registration

The [In-Band Registration \(XEP-0077\)](#)⁵ protocol can be used to establish an account before logging in. That step would be completed before SASL because an entity cannot authenticate if it does not first create an account. Therefore the following order is RECOMMENDED:

1. TLS
2. In-band registration
3. SASL
4. Resource binding

If both stream compression and in-band registration are negotiated, the following order is RECOMMENDED:

1. TLS
2. In-band registration
3. SASL
4. Stream compression
5. Resource binding

3 Server-to-Server Recommendations

3.1 Standard XMPP Features

The XMPP RFCs define an ordering for the features defined therein, namely:

1. TLS
2. SASL

That order **MUST** be followed if no other stream features are negotiated.

⁵XEP-0077: In-Band Registration <<https://xmpp.org/extensions/xep-0077.html>>.

3.2 Dialback

RFC 3920 requires SASL negotiation after TLS negotiation. When the certificate presented by the initiating entity makes reference to a trusted root certification authority, SASL negotiation provides meaningful authentication. In that case, the order shown above is recommended. However, it is possible that the initiating entity will present a self-signed certificate or a certificate whose associated root certification authority is not trusted by the receiving entity. In this situation, service provisioning policies at the receiving entity may dictate the use of server dialback in order to provide a stronger level of trust for the server-to-server stream (where such trust is essentially trust in the underlying Domain Name System), even though server dialback explicitly does not provide authentication. In this case, the following order is RECOMMENDED:

1. TLS
2. Dialback

3.3 Stream Compression

[Stream Compression \(XEP-0138\)](#)⁶ is negotiated when it is not possible to set up TLS compression for whatever reason. It seems safest to negotiate stream compression after negotiation of both TLS (to safely complete the negotiation) and SASL (to prevent certain denial-of-service attacks). Therefore the following order is RECOMMENDED:

1. TLS
2. SASL
3. Stream compression

If stream compression is negotiated in addition to TLS and dialback, it is RECOMMENDED to negotiate it after both TLS and dialback:

1. TLS
2. Dialback
3. Stream compression

4 Security Considerations

The order of negotiated stream features has security implications and may be security-critical. In particular, TLS MUST be negotiated first.

⁶XEP-0138: Stream Compression <<https://xmpp.org/extensions/xep-0138.html>>.

5 IANA Considerations

This document requires no interaction with the [Internet Assigned Numbers Authority \(IANA\)](#)⁷.

6 XMPP Registrar Considerations

This document requires no interaction with the XMPP Registrar.

⁷The 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/>.