XEP-0378: OTR Discovery

Sam Whited
mailto:sam@samwhited.com
xmpp:sam@samwhited.com
https://blog.samwhited.com/

2017-09-11
Version 0.1

Status	Type	Short Name
Deferred	Standards Track	OTR-DISCO

This document provides a mechanism by which OTR encryption support can be discovered in XMPP, without relying on OTRs protocol agnostic discovery mechanism.

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 Discovering support 1

3 Security Considerations 1

4 IANA Considerations 1

5 XMPP Registrar Considerations 2

1 Introduction

The Off-the-Record messaging protocol (OTR) is widely layered on top of XMPP to provide end-to-end encryption. Current use of the protocol is described in Current Off-the-Record Messaging Usage (XEP-0364) [1]. OTR provides its own discovery mechanism in which it sends messages with special whitespace characters to indicate support. While this works when initializing a session, there is no way to query a client for support and to know in advance that a particular version of OTR is supported. This specification aims to solve that by providing an in-band mechanism for discovering OTR support in XMPP.
It should be noted that newer, more secure encryption protocols exist for XMPP, and that new implementations of OTR are discouraged. This protocol is primarily intended to solve issues with existing implementations of OTR.

2 Discovering support

If an entity supports OTR it MUST advertise the fact by returning a feature of 'urn:xmpp:otr:0' (see Namespace Versioning regarding the possibility of incrementing the version number) in response to a Service Discovery (XEP-0030) [2] information request. This indicates support for OTRv3 as defined by Off-the-Record Messaging Protocol version 3 [3].

Listing 1: Disco response

```
<feature var='urn:xmpp:otr:0' />
```

If older versions of OTR are required, they may be discovered out of band using OTRs built in mechanism which is beyond the scope of this document.

3 Security Considerations

Because OTR support is advertised outside of any end-to-end encrypted stream, it may be subject to downgrade attacks (eg. the server operator may remove OTR from the features list).

4 IANA Considerations

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

[1] XEP-0364: Current Off-the-Record Messaging Usage <https://xmpp.org/extensions/xep-0364.html>.
[2] XEP-0030: Service Discovery <https://xmpp.org/extensions/xep-0030.html>.
[3] Off-the-Record Messaging Protocol (OTR) version 3 <https://otr.cypherpunks.ca/Protocol-v3-4.0.0.html> (Accessed 2015-08-30).

5 XMPP Registrar Considerations

This specification defines the following XML namespaces:

- urn:xmpp:otr:0

The XMPP Registrar [4] shall include the foregoing namespaces in its disco features registry as defined in Service Discovery (XEP-0030) [5].

```
<var>
        <name>urn:xmpp:otr:0</name>
        <desc>Indicates support for Off-the-Record Messaging (OTR)
            version 3</desc>
        <doc>XEP-0378</doc>
</var>
```

[4] 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/>.

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