XEP-0467: XMPP over QUIC

Travis Burtrum
mailto:travis@burtrum.org
xmpp:travis@burtrum.org
https://moparisthebest.com/

2022-07-13
Version 0.1.0

Status	Type	Short Name
Experimental	Standards Track	NOT_YET_ASSIGNED

This specification defines a procedure to make both c2s and s2s XMPP connections over the QUIC protocol instead of TCP+TLS.

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 Requirements 1

3 Use Cases 2

4 Security Considerations 2

5 IANA Considerations 2

6 XMPP Registrar Considerations 3

1 Introduction

XMPP Core [1] specifies the use of STARTTLS to connect to an XMPP server. SRV records for XMPP over TLS (XEP-0368) [2] extends that to skip STARTTLS by doing Direct TLS. This XEP defines how to negotiate a XMPP connection over QUIC (RFC 9000 [3]), which provides identical security and authentication to TCP+TLS, along with a number of other desirable properties, such as connection migration across IP changes, and multiple independent bidirectional streams in one session, among others.

2 Requirements

QUIC session negotiation is virtually identical to TLS. This document specifies that the following additional rules apply:

1. While other forms of discovery like Discovering Alternative XMPP Connection Methods (XEP-0156) [4] can discover QUIC connections, we also define UDP port 443 as the default port to attempt a XMPP-over-QUIC connection on if those are not available, yes this is the reserved port for HTTPS, no we don't care because SNI and ALPN are required so there will be no mishaps.
2. TLS certificates MUST be validated the same way as for STARTTLS. (i.e., as specified in XMPP Core [5]).
3. STARTTLS MUST NOT be used over QUIC connections.
4. Client or server MUST set SNI TLS extension to the JID's domain part, and MUST use TLS Encrypted Client Hello [6] if available.
5. Client or server MUST set the ALPN (RFC 7301 [7]) TLS extension, and MUST use TLS Encrypted Client Hello [8] if available.
6. The ALPN protocol MUST be '**xmpp-client**' when negotiating an c2s connection.
7. The ALPN protocol MUST be '**xmpp-server**' when negotiating an s2s connection.

[1] RFC 6120: Extensible Messaging and Presence Protocol (XMPP): Core <http://tools.ietf.org/html/rfc6120>.
[2] XEP-0368: SRV records for XMPP over TLS <https://xmpp.org/extensions/xep-0368.html>.
[3] RFC 9000: QUIC: A UDP-Based Multiplexed and Secure Transport <http://tools.ietf.org/html/rfc9000>.
[4] XEP-0156: Discovering Alternative XMPP Connection Methods <https://xmpp.org/extensions/xep-0156.html>.
[5] RFC 6120: Extensible Messaging and Presence Protocol (XMPP): Core <http://tools.ietf.org/html/rfc6120>.
[6] TLS Encrypted Client Hello <http://tools.ietf.org/html/draft-ietf-tls-esni/>.
[7] RFC 7301: Transport Layer Security (TLS) Application-Layer Protocol Negotiation Extension <https://tools.ietf.org/html/rfc7301>.
[8] TLS Encrypted Client Hello <http://tools.ietf.org/html/draft-ietf-tls-esni/>.

8. The client or server MUST use QUIC Connection Migration which allows for a single QUIC session and therefore multiple XMPP connections to migrate between IPs without reconnecting. Use of Stream Management (XEP-0198) [9] is therefore optional but encouraged if reconnection might occur over another transport like TLS or WebSocket.

9. QUIC supports uni-directional and bi-directional streams, but XMPP MUST only use bi-directional streams. Multiple bi-directional MAY be opened in one session and MUST be treated as a seperate connections with the same security and authentication as negotiated in the initial TLS handshake. This means clients can log into multiple accounts, or the same account multiple times over one QUIC session, or servers can open multiple s2s connections over one QUIC session where one of the servers can prove control over multiple domains, for example if the certificate covered multiple domain names.

3 Use Cases

Perhaps the most compelling benefit of QUIC over TCP+TLS is connection migration especially for mobile devices which swap between mobile and WiFi often. Multiple connections per QUIC session is also helpful for clients with multiple accounts or servers with multiple streams to each other. The handshake and especially 0-rtt mode will be faster than STARTTLS, and in theory, QUIC in general should be faster than TLS, though perhaps not enough to matter for XMPP.

4 Security Considerations

QUIC provides AT LEAST the same level of security as STARTTLS and Direct TLS, and far more privacy with TLS Encrypted Client Hello [10] (which can and should be used with Direct TLS, but this isn't a MUST). QUIC provides more security than STARTTLS if RFC 7590 [11] is not followed, as it isn't subject to STARTTLS stripping. All security setup and certificate validation code SHOULD be shared between the QUIC, STARTTLS and Direct TLS logic as well.

5 IANA Considerations

ALPN (RFC 7301 [12]) requires registration of new Protocol IDs. This document re-uses the two Protocol IDs specified in SRV records for XMPP over TLS (XEP-0368) [13], but the ALPN registry (currently located here) should be updated to additionally point to this document.

[9] XEP-0198: Stream Management <https://xmpp.org/extensions/xep-0198.html>.
[10] TLS Encrypted Client Hello <http://tools.ietf.org/html/draft-ietf-tls-esni/>.
[11] RFC 7590: Use of Transport Layer Security (TLS) in the Extensible Messaging and Presence Protocol (XMPP) <http://tools.ietf.org/html/rfc7590>.
[12] RFC 7301: Transport Layer Security (TLS) Application-Layer Protocol Negotiation Extension <https://tools.ietf.org/html/rfc7301>.
[13] XEP-0368: SRV records for XMPP over TLS <https://xmpp.org/extensions/xep-0368.html>.

IANA requires registration of port numbers too (currently located here) but UDP 443 is already assigned to HTTPS, which also requires ALPN, so I think no registration is required.

6 XMPP Registrar Considerations

This document requires no interaction with the XMPP Registrar [14].

[14] 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/>.