INTERNATIONAL STANDARD

ISO/IEC 20922

First edition
2016-06-15

Information technology — Message Queuing Telemetry Transport (MQTT) v3.1.1

Technologies de l'information — Transport par télémesure des messages en file d'attente (MQTT) v3.1.1

Reference number
ISO/IEC 20922:2016(E)

© ISO/IEC 2016



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2016

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

© ISO/IEC 2016 – All rights reserved

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT), see the following URL: Foreword — Supplementary information.

ISO/IEC 20922:2016 was prepared by the OASIS Message Queuing Telemetry Transport (MQTT) Technical Committee and was adopted, under the PAS procedure, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in parallel with its approval by the national bodies of ISO and IEC.

© ISO/IEC 2016 – All rights reserved

MQTT Version 3.1.1

OASIS Standard

29 October 2014

Specification URIs

This version:

http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.doc (Authoritative)
http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html
http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.pdf

Previous version:

http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/cos01/mqtt-v3.1.1-cos01.doc (Authoritative)
http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/cos01/mqtt-v3.1.1-cos01.html
http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/cos01/mqtt-v3.1.1-cos01.pdf

Latest version:

http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/mqtt-v3.1.1.doc (Authoritative)
http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/mqtt-v3.1.1.html
http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/mqtt-v3.1.1.pdf

Technical Committee:

OASIS Message Queuing Telemetry Transport (MQTT) TC

Chairs:

Raphael J Cohn (raphael.cohn@stormmq.com), Individual
Richard J Coppen (coppen@uk.ibm.com), IBM

Editors:

Andrew Banks (Andrew_Banks@uk.ibm.com), IBM
Rahul Gupta (rahul.gupta@us.ibm.com), IBM

Related work:

This specification is related to:

- *MQTT and the NIST Cybersecurity Framework Version 1.0*. Edited by Geoff Brown and Louis-Philippe Lamoureux. Latest version: http://docs.oasis-open.org/mqtt/mqtt-nist-cybersecurity/v1.0/mqtt-nist-cybersecurity-v1.0.html.

Abstract:

MQTT is a Client Server publish/subscribe messaging transport protocol. It is light weight, open, simple, and designed so as to be easy to implement. These characteristics make it ideal for use in many situations, including constrained environments such as for communication in Machine to Machine (M2M) and Internet of Things (IoT) contexts where a small code footprint is required and/or network bandwidth is at a premium.

The protocol runs over TCP/IP, or over other network protocols that provide ordered, lossless, bi-directional connections. Its features include:

- Use of the publish/subscribe message pattern which provides one-to-many message distribution and decoupling of applications.
- A messaging transport that is agnostic to the content of the payload.
- Three qualities of service for message delivery:

Copyright © OASIS Open 2014. All Rights Reserved.

© ISO/IEC 2016 – All rights reserved

- "At most once", where messages are delivered according to the best efforts of the operating environment. Message loss can occur. This level could be used, for example, with ambient sensor data where it does not matter if an individual reading is lost as the next one will be published soon after.
- "At least once", where messages are assured to arrive but duplicates can occur.
- "Exactly once", where message are assured to arrive exactly once. This level could be used, for example, with billing systems where duplicate or lost messages could lead to incorrect charges being applied.

- A small transport overhead and protocol exchanges minimized to reduce network traffic.
- A mechanism to notify interested parties when an abnormal disconnection occurs.

Status:

This document was last revised or approved by the membership of OASIS on the above date. The level of approval is also listed above. Check the "Latest version" location noted above for possible later revisions of this document. Any other numbered Versions and other technical work produced by the Technical Committee (TC) are listed at https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=mqtt#technical.

TC members should send comments on this specification to the TC's email list. Others should send comments to the TC's public comment list, after subscribing to it by following the instructions at the "Send A Comment" button on the TC's web page at https://www.oasis-open.org/committees/mqtt/.

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the Technical Committee web page (https://www.oasis-open.org/committees/mqtt/ipr.php).

Citation format:

When referencing this specification the following citation format should be used:

[mqtt-v3.1.1]

MQTT Version 3.1.1. Edited by Andrew Banks and Rahul Gupta. 29 October 2014. OASIS Standard. http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html. Latest version: http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/mqtt-v3.1.1.html.

Copyright © OASIS Open 2014. All Rights Reserved.

© ISO/IEC 2016 – All rights reserved

Notices

Copyright © OASIS Open 2014. All Rights Reserved.

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The name "OASIS" is a trademark of OASIS, the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see https://www.oasis-open.org/policies-guidelines/trademark for above guidance.

© ISO/IEC 2016 – All rights reserved

Table of Contents

1 Introduction 9
1.1 Organization of MQTT 9
1.2 Terminology 9
1.3 Normative references 10
1.4 Non normative references 11
1.5 Data representations 13
1.5.1 Bits 13
1.5.2 Integer data values 13
1.5.3 UTF-8 encoded strings 13
1.6 Editing conventions 15
2 MQTT Control Packet format 16
2.1 Structure of an MQTT Control Packet 16
2.2 Fixed header 16
2.2.1 MQTT Control Packet type 16
2.2.2 Flags 17
2.2.3 Remaining Length 18
2.3 Variable header 19
2.3.1 Packet Identifier 20
2.4 Payload 21
3 MQTT Control Packets 23
3.1 CONNECT – Client requests a connection to a Server 23
3.1.1 Fixed header 23
3.1.2 Variable header 23
3.1.3 Payload 29
3.1.4 Response 30
3.2 CONNACK – Acknowledge connection request 31
3.2.1 Fixed header 31
3.2.2 Variable header 31
3.2.3 Payload 33
3.3 PUBLISH – Publish message 33
3.3.1 Fixed header 33
3.3.2 Variable header 35
3.3.3 Payload 36
3.3.4 Response 36
3.3.5 Actions 36
3.4 PUBACK – Publish acknowledgement 37
3.4.1 Fixed header 37
3.4.2 Variable header 37
3.4.3 Payload 37
3.4.4 Actions 37
3.5 PUBREC – Publish received (QoS 2 publish received, part 1) 37
3.5.1 Fixed header 38
3.5.2 Variable header 38

Copyright © OASIS Open 2014. All Rights Reserved.

© ISO/IEC 2016 – All rights reserved

3.5.3 Payload 38
3.5.4 Actions 38
3.6 PUBREL – Publish release (QoS 2 publish received, part 2) 38
3.6.1 Fixed header 38
3.6.2 Variable header 39
3.6.3 Payload 39
3.6.4 Actions 39
3.7 PUBCOMP – Publish complete (QoS 2 publish received, part 3) 39
3.7.1 Fixed header 39
3.7.2 Variable header 40
3.7.3 Payload 40
3.7.4 Actions 40
3.8 SUBSCRIBE - Subscribe to topics 40
3.8.1 Fixed header 40
3.8.2 Variable header 40
3.8.3 Payload 41
3.8.4 Response 42
3.9 SUBACK – Subscribe acknowledgement 43
3.9.1 Fixed header 44
3.9.2 Variable header 44
3.9.3 Payload 44
3.10 UNSUBSCRIBE – Unsubscribe from topics 45
3.10.1 Fixed header 45
3.10.2 Variable header 45
3.10.3 Payload 46
3.10.4 Response 46
3.11 UNSUBACK – Unsubscribe acknowledgement 47
3.11.1 Fixed header 47
3.11.2 Variable header 47
3.11.3 Payload 48
3.12 PINGREQ – PING request 48
3.12.1 Fixed header 48
3.12.2 Variable header 48
3.12.3 Payload 48
3.12.4 Response 48
3.13 PINGRESP – PING response 48
3.13.1 Fixed header 48
3.13.2 Variable header 49
3.13.3 Payload 49
3.14 DISCONNECT – Disconnect notification 49
3.14.1 Fixed header 49
3.14.2 Variable header 49
3.14.3 Payload 49
3.14.4 Response 49
4 Operational behavior 51

Copyright © OASIS Open 2014. All Rights Reserved.

© ISO/IEC 2016 – All rights reserved

4.1 Storing state 51
4.1.1 Non normative example 51
4.2 Network Connections 52
4.3 Quality of Service levels and protocol flows 52
4.3.1 QoS 0: At most once delivery 52
4.3.2 QoS 1: At least once delivery 53
4.3.3 QoS 2: Exactly once delivery 54
4.4 Message delivery retry 55
4.5 Message receipt 56
4.6 Message ordering 56
4.7 Topic Names and Topic Filters 57
4.7.1 Topic wildcards 57
4.7.2 Topics beginning with $ 58
4.7.3 Topic semantic and usage 58
4.8 Handling errors 59
5 Security 60
5.1 Introduction 60
5.2 MQTT solutions: security and certification 60
5.3 Lightweight cryptography and constrained devices 61
5.4 Implementation notes 61
5.4.1 Authentication of Clients by the Server 61
5.4.2 Authorization of Clients by the Server 61
5.4.3 Authentication of the Server by the Client 61
5.4.4 Integrity of Application Messages and Control Packets 62
5.4.5 Privacy of Application Messages and Control Packets 62
5.4.6 Non-repudiation of message transmission 62
5.4.7 Detecting compromise of Clients and Servers 62
5.4.8 Detecting abnormal behaviors 63
5.4.9 Other security considerations 63
5.4.10 Use of SOCKS 64
5.4.11 Security profiles 64
6 Using WebSocket as a network transport 65
6.1 IANA Considerations 65
7 Conformance 66
7.1 Conformance Targets 66
7.1.1 MQTT Server 66
7.1.2 MQTT Client 66
Appendix A. Acknowledgements (non normative) 68
Appendix B. Mandatory normative statements (non normative) 70
Appendix C. Revision history (non normative) 80

Copyright © OASIS Open 2014. All Rights Reserved.

© ISO/IEC 2016 – All rights reserved

Table of Figures and Tables

Figure 1.1 Structure of UTF-8 encoded strings 13
Figure 1.2 UTF-8 encoded string non normative example....14
Figure 2.1 – Structure of an MQTT Control Packet 16
Figure 2.2 - Fixed header format....16
Table 2.1 - Control packet types 16
Table 2.2 - Flag Bits....17
Table 2.4 Size of Remaining Length field....18
Figure 2.3 - Packet Identifier bytes....20
Table 2.5 - Control Packets that contain a Packet Identifier....20
Table 2.6 - Control Packets that contain a Payload 21
Figure 3.1 – CONNECT Packet fixed header....23
Figure 3.2 - Protocol Name bytes....23
Figure 3.3 - Protocol Level byte 24
Figure 3.4 - Connect Flag bits....24
Figure 3.5 Keep Alive bytes 27
Figure 3.6 - Variable header non normative example 28
Figure 3.7 - Password bytes 30
Figure 3.8 – CONNACK Packet fixed header 31
Figure 3.9 – CONNACK Packet variable header....31
Table 3.1 – Connect Return code values 32
Figure 3.10 – PUBLISH Packet fixed header 33
Table 3.2 - QoS definitions....34
Table 3.3 - Publish Packet non normative example 35
Figure 3.11 - Publish Packet variable header non normative example 35
Table 3.4 - Expected Publish Packet response....36
Figure 3.12 - PUBACK Packet fixed header 37
Figure 3.13 – PUBACK Packet variable header....37
Figure 3.14 – PUBREC Packet fixed header 38
Figure 3.15 – PUBREC Packet variable header 38
Figure 3.16 – PUBREL Packet fixed header....38
Figure 3.17 – PUBREL Packet variable header 39
Figure 3.18 – PUBCOMP Packet fixed header 39
Figure 3.19 – PUBCOMP Packet variable header 40
Figure 3.20 – SUBSCRIBE Packet fixed header....40
Figure 3.21 - Variable header with a Packet Identifier of 10, Non normative example....41
Figure 3.22 – SUBSCRIBE Packet payload format....41
Table 3.5 - Payload non normative example....42
Figure 3.23 - Payload byte format non normative example....42
Figure 3.24 – SUBACK Packet fixed header....44
Figure 3.25 – SUBACK Packet variable header....44
Figure 3.26 – SUBACK Packet payload format....44
Table 3.6 - Payload non normative example....45
Figure 3.27 - Payload byte format non normative example....45
Figure 3.28 – UNSUBSCRIBE Packet Fixed header 45
Figure 3.29 – UNSUBSCRIBE Packet variable header....45
Table3.7 - Payload non normative example....46
Figure 3.30 - Payload byte format non normative example....46

Copyright © OASIS Open 2014. All Rights Reserved.

© ISO/IEC 2016 – All rights reserved

Figure 3.31 – UNSUBACK Packet fixed header....47
Figure 3.32 – UNSUBACK Packet variable header....47
Figure 3.33 – PINGREQ Packet fixed header....48
Figure 3.34 – PINGRESP Packet fixed header....48
Figure 3.35 – DISCONNECT Packet fixed header....49
Figure 4.1 – QoS 0 protocol flow diagram, non normative example....52
Figure 4.2 – QoS 1 protocol flow diagram, non normative example....53
Figure 4.3 – QoS 2 protocol flow diagram, non normative example....54
Figure 6.1 - IANA WebSocket Identifier....65

Copyright © OASIS Open 2014. All Rights Reserved.

© ISO/IEC 2016 – All rights reserved

1 Introduction

1.1 Organization of MQTT

This specification is split into seven chapters:

- Chapter 1 - Introduction
- Chapter 2 - MQTT Control Packet format
- Chapter 3 - MQTT Control Packets
- Chapter 4 - Operational behavior
- Chapter 5 - Security
- Chapter 6 - Using WebSocket as a network transport
- Chapter 7 - Conformance Targets

1.2 Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted as described in IETF RFC 2119 [RFC2119].

Network Connection:

A construct provided by the underlying transport protocol that is being used by MQTT.

- It connects the Client to the Server.
- It provides the means to send an ordered, lossless, stream of bytes in both directions.

For examples see Section 4.2.

Application Message:

The data carried by the MQTT protocol across the network for the application. When Application Messages are transported by MQTT they have an associated Quality of Service and a Topic Name.

Client:

A program or device that uses MQTT. A Client always establishes the Network Connection to the Server. It can

- Publish Application Messages that other Clients might be interested in.
- Subscribe to request Application Messages that it is interested in receiving.
- Unsubscribe to remove a request for Application Messages.
- Disconnect from the Server.

Server:

A program or device that acts as an intermediary between Clients which publish Application Messages and Clients which have made Subscriptions. A Server

- Accepts Network Connections from Clients.
- Accepts Application Messages published by Clients.

Copyright © OASIS Open 2014. All Rights Reserved.

© ISO/IEC 2016 – All rights reserved

- Processes Subscribe and Unsubscribe requests from Clients.
- Forwards Application Messages that match Client Subscriptions.

Subscription:
A Subscription comprises a Topic Filter and a maximum QoS. A Subscription is associated with a single Session. A Session can contain more than one Subscription. Each Subscription within a session has a different Topic Filter.

Topic Name:
The label attached to an Application Message which is matched against the Subscriptions known to the Server. The Server sends a copy of the Application Message to each Client that has a matching Subscription.

Topic Filter:
An expression contained in a Subscription, to indicate an interest in one or more topics. A Topic Filter can include wildcard characters.

Session:
A stateful interaction between a Client and a Server. Some Sessions last only as long as the Network Connection, others can span multiple consecutive Network Connections between a Client and a Server.

MQTT Control Packet:
A packet of information that is sent across the Network Connection. The MQTT specification defines fourteen different types of Control Packet, one of which (the PUBLISH packet) is used to convey Application Messages.

1.3 Normative references

[RFC2119]

Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
http://www.ietf.org/rfc/rfc2119.txt

[RFC3629]

Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, November 2003
http://www.ietf.org/rfc/rfc3629.txt

[RFC5246]

Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

http://www.ietf.org/rfc/rfc5246.txt

[RFC6455]

Fette, I. and A. Melnikov, "The WebSocket Protocol", RFC 6455, December 2011.

http://www.ietf.org/rfc/rfc6455.txt

Copyright © OASIS Open 2014. All Rights Reserved.

© ISO/IEC 2016 – All rights reserved

[Unicode]

The Unicode Consortium. The Unicode Standard.

http://www.unicode.org/versions/latest/

1.4 Non normative references

[RFC793]

Postel, J. Transmission Control Protocol. STD 7, IETF RFC 793, September 1981.
http://www.ietf.org/rfc/rfc793.txt

[AES]

Advanced Encryption Standard (AES) (FIPS PUB 197).
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[DES]

Data Encryption Standard (DES).
http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

[FIPS1402]

Security Requirements for Cryptographic Modules (FIPS PUB 140-2)

http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[IEEE 802.1AR]

IEEE Standard for Local and metropolitan area networks - Secure Device Identity
http://standards.ieee.org/findstds/standard/802.1AR-2009.html

[ISO29192]

ISO/IEC 29192-1:2012 Information technology -- Security techniques -- Lightweight cryptography -- Part 1: General
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56425

[MQTT NIST]

MQTT supplemental publication, MQTT and the NIST Framework for Improving Critical Infrastructure Cybersecurity
http://docs.oasis-open.org/mqtt/mqtt-nist-cybersecurity/v1.0/mqtt-nist-cybersecurity-v1.0.html

[MQTTV31]

MQTT V3.1 Protocol Specification.

http://public.dhe.ibm.com/software/dw/webservices/ws-mqtt/mqtt-v3r1.html

[NISTCSF]

Improving Critical Infrastructure Cybersecurity Executive Order 13636
http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf

Copyright © OASIS Open 2014. All Rights Reserved.

© ISO/IEC 2016 – All rights reserved

115

116 **[NIST7628]**

117 *NISTIR 7628 Guidelines for Smart Grid Cyber Security*
118 http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf

119

120 **[NSAB]**

121 *NSA Suite B Cryptography*
122 http://www.nsa.gov/ia/programs/suiteb_cryptography/

123

124 **[PCIDSS]**

125 *PCI-DSS Payment Card Industry Data Security Standard*
126 https://www.pcisecuritystandards.org/security_standards/

127

128 **[RFC1928]**

129 *Leech, M., Ganis, M., Lee, Y., Kuris, R., Koblas, D., and L. Jones, "SOCKS Protocol Version 5", RFC*
130 *1928, March 1996.*

131 http://www.ietf.org/rfc/rfc1928.txt

132

133 **[RFC4511]**

134 *Sermersheim, J., Ed., "Lightweight Directory Access Protocol (LDAP): The Protocol", RFC 4511, June*
135 *2006.*

136 http://www.ietf.org/rfc/rfc4511.txt

137

138 **[RFC5077]**

139 *Salowey, J., Zhou, H., Eronen, P., and H. Tschofenig, "Transport Layer Security (TLS) Session*
140 *Resumption without Server-Side State", RFC 5077, January 2008.*

141 http://www.ietf.org/rfc/rfc5077.txt

142

143 **[RFC5280]**

144 *Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key*
145 *Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.*

146 http://www.ietf.org/rfc/rfc5280.txt

147

148 **[RFC6066]**

149 Eastlake 3rd, D., "Transport Layer Security (TLS) Extensions: Extension Definitions", RFC 6066, January
150 2011.

151 http://www.ietf.org/rfc/rfc6066.txt

152

153 **[RFC6749]**

154 *Hardt, D., Ed., "The OAuth 2.0 Authorization Framework", RFC 6749, October 2012.*

Copyright © OASIS Open 2014. All Rights Reserved.

© ISO/IEC 2016 – All rights reserved

155 http://www.ietf.org/rfc/rfc6749.txt
156
157 [RFC6960]
158 *Santesson, S., Myers, M., Ankney, R., Malpani, A., Galperin, S., and C. Adams, "X.509 Internet Public*
159 *Key Infrastructure Online Certificate Status Protocol - OCSP", RFC 6960, June 2013.*
160 http://www.ietf.org/rfc/rfc6960.txt
161
162 [SARBANES]
163 *Sarbanes-Oxley Act of 2002.*
164 http://www.gpo.gov/fdsys/pkg/PLAW-107publ204/html/PLAW-107publ204.htm
165
166 [USEUSAFEHARB]
167 *U.S.-EU Safe Harbor*
168 http://export.gov/safeharbor/eu/eg_main_018365.asp

169 # 1.5 Data representations

170 ## 1.5.1 Bits

171 Bits in a byte are labeled 7 through 0. Bit number 7 is the most significant bit, the least significant bit is
172 assigned bit number 0.

173 ## 1.5.2 Integer data values

174 Integer data values are 16 bits in big-endian order: the high order byte precedes the lower order byte.
175 This means that a 16-bit word is presented on the network as Most Significant Byte (MSB), followed by
176 Least Significant Byte (LSB).

177 ## 1.5.3 UTF-8 encoded strings

178 Text fields in the Control Packets described later are encoded as UTF-8 strings. UTF-8 [RFC3629] is an
179 efficient encoding of Unicode [Unicode] characters that optimizes the encoding of ASCII characters in
180 support of text-based communications.
181
182 Each of these strings is prefixed with a two byte length field that gives the number of bytes in a UTF-8
183 encoded string itself, as illustrated in Figure 1.1 Structure of UTF-8 encoded strings below. Consequently
184 there is a limit on the size of a string that can be passed in one of these UTF-8 encoded string
185 components; you cannot use a string that would encode to more than 65535 bytes.
186
187 Unless stated otherwise all UTF-8 encoded strings can have any length in the range 0 to 65535 bytes.

188 **Figure 1.1 Structure of UTF-8 encoded strings**

Bit	7	6	5	4	3	2	1	0
byte 1	String length MSB							
byte 2	String length LSB							
byte 3 ….	UTF-8 Encoded Character Data, if length > 0.							

Copyright © OASIS Open 2014. All Rights Reserved.

© ISO/IEC 2016 – All rights reserved

The character data in a UTF-8 encoded string MUST be well-formed UTF-8 as defined by the Unicode specification [Unicode] and restated in RFC 3629 [RFC3629]. In particular this data MUST NOT include encodings of code points between U+D800 and U+DFFF. If a Server or Client receives a Control Packet containing ill-formed UTF-8 it MUST close the Network Connection [MQTT-1.5.3-1].

A UTF-8 encoded string MUST NOT include an encoding of the null character U+0000. If a receiver (Server or Client) receives a Control Packet containing U+0000 it MUST close the Network Connection [MQTT-1.5.3-2].

The data SHOULD NOT include encodings of the Unicode [Unicode] code points listed below. If a receiver (Server or Client) receives a Control Packet containing any of them it MAY close the Network Connection:

U+0001..U+001F control characters
U+007F..U+009F control characters

Code points defined in the Unicode specification [Unicode] to be non-characters (for example U+0FFFF)

A UTF-8 encoded sequence 0xEF 0xBB 0xBF is always to be interpreted to mean U+FEFF ("ZERO WIDTH NO-BREAK SPACE") wherever it appears in a string and MUST NOT be skipped over or stripped off by a packet receiver [MQTT-1.5.3-3].

1.5.3.1 Non normative example

For example, the string A☐ which is LATIN CAPITAL Letter A followed by the code point U+2A6D4 (which represents a CJK IDEOGRAPH EXTENSION B character) is encoded as follows:

Figure 1.2 UTF-8 encoded string non normative example

Bit	7	6	5	4	3	2	1	0
byte 1	String Length MSB (0x00)							
	0	0	0	0	0	0	0	0
byte 2	String Length LSB (0x05)							
	0	0	0	0	0	1	0	1
byte 3	'A' (0x41)							
	0	1	0	0	0	0	0	1
byte 4	(0xF0)							
	1	1	1	1	0	0	0	0
byte 5	(0xAA)							
	1	0	1	0	1	0	1	0
byte 6	(0x9B)							
	1	0	0	1	1	0	1	1

Copyright © OASIS Open 2014. All Rights Reserved.

© ISO/IEC 2016 – All rights reserved

byte 7	(0x94)							
	1	0	0	1	0	1	0	0

217

218 1.6 Editing conventions

219 Text highlighted in Yellow within this specification identifies conformance statements. Each conformance
220 statement has been assigned a reference in the format [MQTT-x.x.x-y].

Copyright © OASIS Open 2014. All Rights Reserved.

© ISO/IEC 2016 – All rights reserved