



A76XX Series_MQTT(S) _Application Note

LTE Module

SIMCom Wireless Solutions Limited

SIMCom Headquarters Building, Building 3, No. 289 Linhong
Road, Changning District, Shanghai P.R.China

Tel: 86-21-31575100
support@simcom.com
www.simcom.com

Document Title:	A76XXSeries_MQTT(S)_Application Note
Version:	1.02
Date:	2021.11.08
Status:	Released

GENERAL NOTES

SIMCOM OFFERS THIS INFORMATION AS A SERVICE TO ITS CUSTOMERS, TO SUPPORT APPLICATION AND ENGINEERING EFFORTS THAT USE THE PRODUCTS DESIGNED BY SIMCOM. THE INFORMATION PROVIDED IS BASED UPON REQUIREMENTS SPECIFICALLY PROVIDED TO SIMCOM BY THE CUSTOMERS. SIMCOM HAS NOT UNDERTAKEN ANY INDEPENDENT SEARCH FOR ADDITIONAL RELEVANT INFORMATION, INCLUDING ANY INFORMATION THAT MAY BE IN THE CUSTOMER'S POSSESSION. FURTHERMORE, SYSTEM VALIDATION OF THIS PRODUCT DESIGNED BY SIMCOM WITHIN A LARGER ELECTRONIC SYSTEM REMAINS THE RESPONSIBILITY OF THE CUSTOMER OR THE CUSTOMER'S SYSTEM INTEGRATOR. ALL SPECIFICATIONS SUPPLIED HEREIN ARE SUBJECT TO CHANGE.

COPYRIGHT

THIS DOCUMENT CONTAINS PROPRIETARY TECHNICAL INFORMATION WHICH IS THE PROPERTY OF SIMCOM WIRELESS SOLUTIONS LIMITED COPYING, TO OTHERS AND USING THIS DOCUMENT, ARE FORBIDDEN WITHOUT EXPRESS AUTHORITY BY SIMCOM. OFFENDERS ARE LIABLE TO THE PAYMENT OF INDEMNIFICATIONS. ALL RIGHTS RESERVED BY SIMCOM IN THE PROPRIETARY TECHNICAL INFORMATION, INCLUDING BUT NOT LIMITED TO REGISTRATION GRANTING OF A PATENT , A UTILITY MODEL OR DESIGN. ALL SPECIFICATION SUPPLIED HEREIN ARE SUBJECT TO CHANGE WITHOUT NOTICE AT ANY TIME.

SIMCom Wireless Solutions Limited

SIMCom Headquarters Building, Building 3, No. 289 Linhong Road, Changning District, Shanghai
P.R.China
Tel: +86 21 31575100
Email: simcom@simcom.com

For more information, please visit:

<https://www.simcom.com/download/list-863-en.html>

For technical support, or to report documentation errors, please visit:

<https://www.simcom.com/ask/> or email to: support@simcom.com

Copyright © 2021SIMCom Wireless Solutions Limited All Rights Reserved.

About Document

Version History

Revision	Date	Chapter	Description
V1.00	2020.06.19	All	New version
V1.01	2021.07.02	All	Add support on A7678 Series
V1.02	2021.11.08	Scope	Scope description is updated

SIMCOM
Confidential

Scope

Based on module AT command manual, this document will introduce MQTT(S) application process. Developers could understand and develop application quickly and efficiently based on this document. This document applies to A1803S Series, A1603 Series, A1601 Series and A1802 Series.

SIMCom
Confidential

SIMCom
Confidential

Contents

About Document	1
Version History.....	1
Scope.....	2
Contents	4
1 Introduction	5
1.1 Purpose of the document.....	5
1.2 Related documents.....	5
1.3 Conventions and abbreviations.....	5
1.4 The process of Using MQTT(S) AT Command.....	6
1.5 Error Handling.....	7
2 AT Commands for MQTT(S)	8
2.1 Overview of AT Commands for MQTT(S).....	8
3 MQTT(S)Examples	9
3.1 Access to MQTT server not SSL/TLS.....	9
3.2 Connect to SSL/TLS MQTT server (not verify server).....	12
3.3 Access to SSL/TLS MQTT server (only verify the server).....	13
3.4 Access to SSL/TLS MQTT server (verify server and client).....	16
3.5 Access to MQTT server without checking UTF8 coding.....	18
4 Appendix	20
4.1 Summary of Error Codes.....	20

1 Introduction

1.1 Purpose of the document

Based on module AT command manual, this document will introduce MQTTS application process.

Developers could understand and develop application quickly and efficiently based on this document.

1.2 Related documents

[1] A76XXSeries_AT Command Manual

1.3 Conventions and abbreviations

In this document, the GSM engines are referred to as following term:

ME (Mobile Equipment);

MS (Mobile Station);

TA (Terminal Adapter);

DCE (Data Communication Equipment) or facsimile DCE (FAX modem, FAX board);

In application, controlling device controls the GSM engine by sending AT Command via its serial interface.

The controlling device at the other end of the serial line is referred to as following term:

TE (Terminal Equipment);

DTE (Data Terminal Equipment) or plainly "the application" which is running on an embedded system;

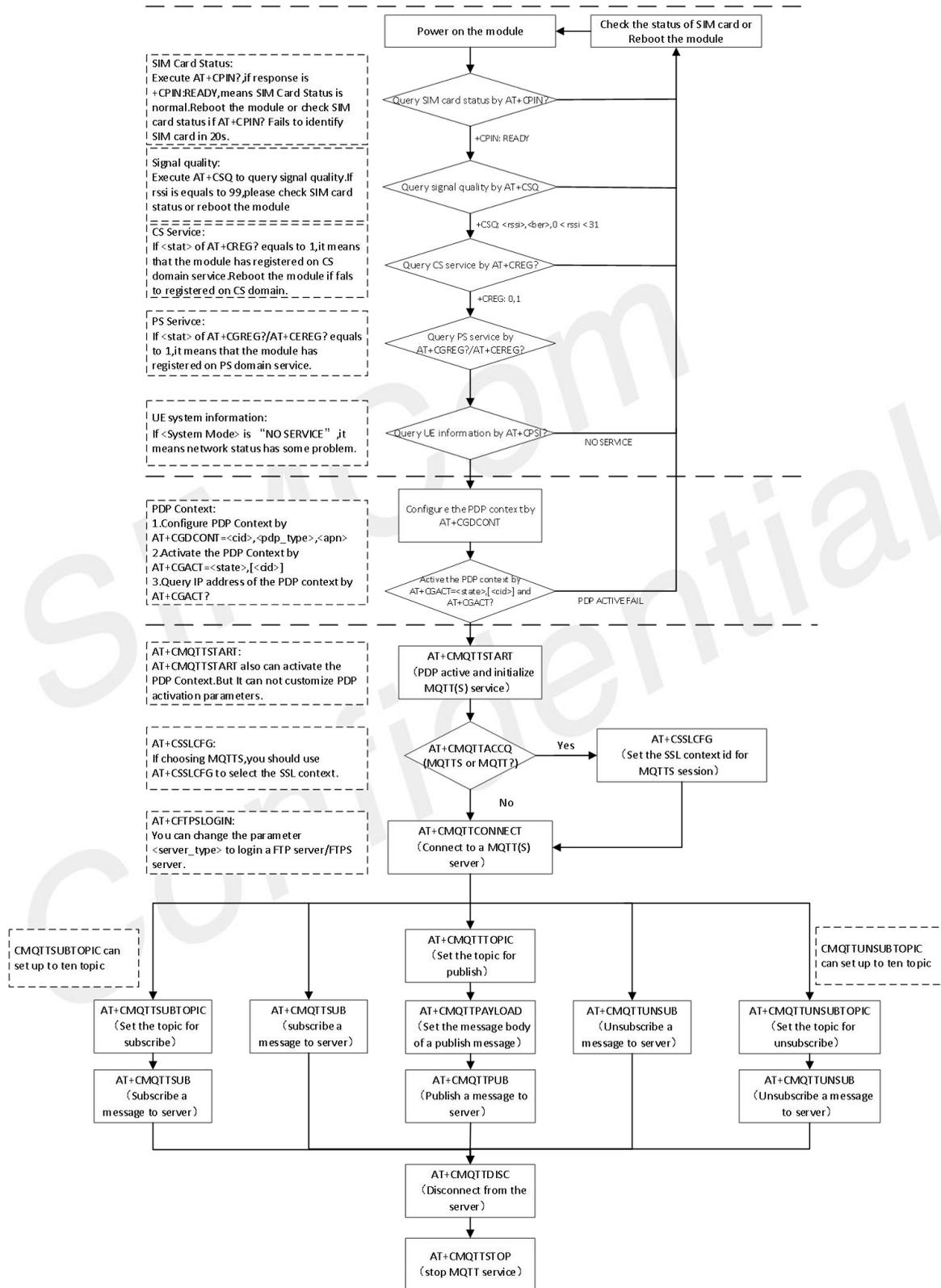
Other Conventions:

MQTT(Message Queuing Telemetry Transport);

SSL(Secure Sockets Layer);

PDP(Packet Data Protocol);

1.4 The process of Using MQTT(S) AT Command



1.5 Error Handling

For more details, please refer to A76XXSeries_AT Command Manual.

SIMCom
Confidential

2 AT Commands for MQTT(S)

2.1 Overview of AT Commands for MQTT(S)

Command	Description
AT+CMQTTSTART	Start MQTT service
AT+CMQTTSTOP	Stop MQTT service
AT+CMQTTACCQ	Acquire a client
AT+CMQTTREL	Release a client
AT+CMQTTSSLCFG	Set the SSL context (only for SSL/TLS MQTT)
AT+CMQTTWILLTOPIC	Input the topic of will message
AT+CMQTTWILLMSG	Input the will message
AT+CMQTTCONNECT	Connect to MQTT server
AT+CMQTTDISC	Disconnect from server
AT+CMQTTTOPIC	Input the topic of publish message
AT+CMQTTPAYLOAD	Input the publish message
AT+CMQTT PUB	Publish a message to server
AT+CMQTTSUBTOPIC	Input the topic of subscribe message
AT+CMQTTSUB	Subscribe a message to server
AT+CMQTTUNSUBTOPIC	Input the topic of unsubscribe message
AT+CMQTTUNSUB	Unsubscribe a message to server
AT+CMQTTCFG	Configure the MQTT Context

For detail information, please refer to “A76XXSeries_AT Command Manual”.

3 MQTT(S)Examples

Before all MQTT(S) related operations, we should ensure the following:

Ensure network is available:

AT+CSQ

+CSQ: 23,0

OK

AT+CREG?

+CREG: 0,1

OK

AT+CGREG?

+CGREG: 0,1

OK

AT+CPSI?

+CPSI:

LTE,Online,460-00,0x333C,39589680,308,EUT

RAN-BAND3,1350,5,0,0,54,0,22

OK

//In WCDMA/GSW,you need to continue to execute the following instructions

AT+CGDCONT=cid,"ip","APN"

OK

AT+CGACT=1,cid

OK

AT+CGACT?

+CGACT: 1,1

OK

3.1 Access to MQTT server not SSL/TLS

Following commands shows how to communicate with a MQTT server.

```
// start MQTT service, activate PDP context
```

```
AT+CMQTTSTART
```

```
OK
```

```
+CMQTTSTART: 0
```

```
// Acquire one client which will connect to a MQTT server not SSL/TLS
```

```
AT+CMQTTACCQ=0,"client test0"
```

```
OK
```

```
// Set the will topic for the CONNECT message
```

```
AT+CMQTTWILLTOPIC=0,10
```

```
>
```

```
OK
```

```
// Set the will message for the CONNECT message
```

```
AT+CMQTTWILLMSG=0,6,1
```

```
>
```

```
OK
```

```
// Connect to a MQTT server
```

```
AT+CMQTTCONNECT=0,"tcp://test.mosquitto.  
org:1883",60,1
```

```
OK
```

```
+CMQTTCONNECT: 0,0
```

```
// Subscribe one topic from the server
```

```
AT+CMQTTSUB=0,9,1
```

```
>
```

```
OK
```

```
+CMQTTSUB: 0,0
```

```
// Set the topic for the PUBLISH message
```

```
AT+CMQTTTOPIC=0,9
```

```
>
```

```
OK
```

```
// Set the payload for the PUBLISH message
```

```
AT+CMQTTPAYLOAD=0,60
```

```
>
```

```
OK
```

```
// Publish a message
```

AT+CMQTTPUB=0,1,60

OK

+CMQTTPUB: 0,0

//receive publish message from server

+CMQTTRXSTART: 0,9,60

+CMQTTRXTOPIC: 0,9

simcommsg

+CMQTTRXPAYLOAD: 0,60

012345678901234567890123456789012345678

901234567890123456789

+CMQTTRXEND: 0

// Set one topic for the SUBSCRIBE message

AT+CMQTTSUBTOPIC=0,9,1

>

OK

// Subscribe a message

AT+CMQTTSUB=0

OK

+CMQTTSUB: 0,0

// Unsubscribe one topic from the server

AT+CMQTTUNSUB=0,9,0

>

OK

+CMQTTUNSUB: 0,0

// Disconnect from server

AT+CMQTTDISC=0,120

OK

+CMQTTDISC: 0,0

//Release the client

AT+CMQTTREL=0

OK

//stop MQTT Service

AT+CMQTTSTOP

OK

+CMQTTSTOP: 0

3.2 Connect to SSL/TLS MQTT server (not verify server)

Following commands shows how to access to a MQTT server without verifying the server. It needs to configure the authentication mode to 0, and then it will connect to the server successfully.

```
// start MQTT service, activate PDP context
AT+CMQTTSTART
OK

+CMQTTSTART: 0
// Acquire one client which will connect to a SSL/TLS MQTT server
AT+CMQTTACCQ=0,"client test0",1
OK
// Set the will topic for the CONNECT message
AT+CMQTTWILLTOPIC=0,10
>

OK
// Set the will message for the CONNECT message
AT+CMQTTWILLMSG=0,6,1
>

OK
// Connect to a MQTT server
AT+CMQTTCONNECT=0,"tcp://test.mosquitto.org:8883",60,1
OK

+CMQTTCONNECT: 0,0
// Set the topic for the PUBLISH message
AT+CMQTTTOPIC=0,13
>

OK
// Set the payload for the PUBLISH message
AT+CMQTTPAYLOAD=0,60
>

OK
// Publish a message
AT+CMQTTTPUB=0,1,60
OK

+CMQTTTPUB: 0,0
```

```
// Set one topic for the SUBSCRIBE message
```

```
AT+CMQTTSUBTOPIC=0,9,1
```

```
>
```

```
OK
```

```
// Subscribe a message
```

```
AT+CMQTTSUB=0
```

```
OK
```

```
+CMQTTSUB: 0,0
```

```
// Subscribe one topic from the server
```

```
AT+CMQTTSUB=0,9,1
```

```
>
```

```
OK
```

```
+CMQTTSUB: 0,0
```

```
// Unsubscribe one topic from the server
```

```
AT+CMQTTUNSUB=0,9,0
```

```
>
```

```
OK
```

```
+CMQTTUNSUB: 0,0
```

```
// Disconnect from server
```

```
AT+CMQTTDISC=0,120
```

```
OK
```

```
+CMQTTDISC: 0,0
```

```
//Release the client
```

```
AT+CMQTTREL=0
```

```
OK
```

```
//stop MQTT Service
```

```
AT+CMQTTSTOP
```

```
OK
```

```
+CMQTTSTOP: 0
```

3.3 Access to SSL/TLS MQTT server (only verify the server)

Following commands shows how to access to a SSL/TLS MQTT server with verifying the server. It needs to configure the authentication mode to 1 and the right server root CA, and then it will connect to the server

successfully.

```
// Set the SSL version of the first SSL context
AT+CSSLCFG="sslversion",0,4
OK
// Set the authentication mode(verify server) of the first SSL context
AT+CSSLCFG="authmode",0,1
OK
// Set the server root CA of the first SSL context
AT+CSSLCFG="cacert",0,"server_ca.pem"
OK
// start MQTT service, activate PDP context
AT+CMQTTSTART
OK

+CMQTTSTART: 0
// Acquire one client which will connect to a SSL/TLS MQTT server
AT+CMQTTACCQ=0,"client test0",1
OK
// Set the first SSL context to be used in the SSL connection
AT+CMQTTSSLCFG=0,0
OK
// Set the will topic for the CONNECT message
AT+CMQTTWILLTOPIC=0,10
>

OK
// Set the will message for the CONNECT message
AT+CMQTTWILLMSG=0,6,1
>

OK
// Connect to a MQTT server, input the right server and port
AT+CMQTTCONNECT=0,"tcp://mqttp_server:port",60,1
OK

+CMQTTCONNECT: 0,0
// Set the topic for the PUBLISH message
AT+CMQTTTOPIC=0,13
>

OK
// Set the payload for the PUBLISH message
AT+CMQTTPAYLOAD=0,60
```

```
>

OK
// Publish a message
AT+CMQTTPUB=0,1,60
OK

+CMQTTPUB: 0,0
// Set one topic for the SUBSCRIBE message
AT+CMQTTSUBTOPIC=0,9,1
>

OK
// Subscribe a message
AT+CMQTTSUB=0
OK

+CMQTTSUB: 0,0
// Subscribe one topic from the server
AT+CMQTTSUB=0,9,1
>

OK

+CMQTTSUB: 0,0
// Unsubscribe one topic from the server
AT+CMQTTUNSUB=0,9,0
>

OK

+CMQTTUNSUB: 0,0
// Disconnect from server
AT+CMQTTDISC=0,120
OK

+CMQTTDISC: 0,0
//Release the client
AT+CMQTTREL=0
OK
//stop MQTT Service
AT+CMQTTSTOP
OK

+CMQTTSTOP: 0
```

3.4 Access to SSL/TLS MQTT server (verify server and client)

Following commands shows how to access to a SSL/TLS MQTT server with verifying the server and client. It needs to configure the authentication mode to 2, the right server root CA, the right client certificate and key, and then it will connect to the server successfully.

```
// Set the SSL version of the first SSL context
AT+CSSLCFG="sslversion",0,4
OK
// Set the authentication mode(verify server and client) of the first SSL context
AT+CSSLCFG="authmode",0,2
OK
// Set the server root CA of the first SSL context
AT+CSSLCFG="cacert",0,"ca_cert.pem"
OK
// Set the client certificate of the first SSL context
AT+CSSLCFG="clientcert",0,"cert.pem"
OK
// Set the client key of the first SSL context
AT+CSSLCFG="clientkey",0,"key_cert.pem"
OK
// start MQTT service, activate PDP context
AT+CMQTTSTART
OK

+CMQTTSTART: 0
// Acquire one client which will connect to a SSL/TLS MQTT server
AT+CMQTTACCQ=0,"client test0",1
OK
// Set the first SSL context to be used in the SSL connection
AT+CMQTTSSLCFG=0,0
OK
// Set the will topic for the CONNECT message
AT+CMQTTWILLTOPIC=0,10
>

OK
// Set the will message for the CONNECT message
AT+CMQTTWILLMSG=0,6,1
>

OK
```

```
// Connect to a MQTT server
AT+CMQTTCONNECT=0,"tcp://hooleeping.co
m:8883",60,1
OK

+CMQTTCONNECT: 0,0
// Set the topic for the PUBLISH message
AT+CMQTTTOPIC=0,13
>

OK
// Set the payload for the PUBLISH message
AT+CMQTTPAYLOAD=0,60
>

OK
// Publish a message
AT+CMQTTPUB=0,1,60
OK

+CMQTTPUB: 0,0
// Set one topic for the SUBSCRIBE message
AT+CMQTTSUBTOPIC=0,9,1
>

OK
// Subscribe a message
AT+CMQTTSUB=0
OK

+CMQTTSUB: 0,0
// Subscribe one topic from the server
AT+CMQTTSUB=0,9,1
>

OK

+CMQTTSUB: 0,0
// Unsubscribe one topic from the server
AT+CMQTTUNSUB=0,9,0
>

OK

+CMQTTUNSUB: 0,0
// Disconnect from server
```

```
AT+CMQTTDISC=0,120
```

```
OK
```

```
+CMQTTDISC: 0,0
```

```
//Release the client
```

```
AT+CMQTTREL=0
```

```
OK
```

```
//stop MQTT Service
```

```
AT+CMQTTSTOP
```

```
OK
```

```
+CMQTTSTOP: 0
```

3.5 Access to MQTT server without checking UTF8 coding

Following commands shows how to communicate with a MQTT server without checking UTF8 coding.

```
// start MQTT service, activate PDP context
```

```
AT+CMQTTSTART
```

```
OK
```

```
+CMQTTSTART: 0
```

```
// Acquire one client which will connect to a MQTT server not SSL/TLS
```

```
AT+CMQTTACCQ=0,"client test0"
```

```
OK
```

```
// Configure not checking UTF8 coding
```

```
AT+CMQTTCFG="checkUTF8",0,0
```

```
OK
```

```
// Connect to a MQTT server
```

```
AT+CMQTTCONNECT=0,"tcp://198.41.30.241:1  
883",60,1
```

```
OK
```

```
+CMQTTCONNECT: 0,0
```

```
// Subscribe one topic which is not UTF8 coding string.
```

```
//The data can input by hexadecimal format.
```

```
AT+CMQTTSUB=0,9,1
```

```
>
```

```
OK
```

+CMQTTSUB: 0,0

// Set the topic for the PUBLISH message

AT+CMQTTTOPIC=0,9

>

OK

// Publish a message

AT+CMQTTPUB=0,1,60

OK

+CMQTTPUB: 0,0

//receive publish message from server

+CMQTTRXSTART: 0,9,0

+CMQTTRXTOPIC: 0,9

盼盼盼盼?

+CMQTTRXEND: 0

// Disconnect from server

AT+CMQTTDISC=0,120

OK

+CMQTTDISC: 0,0

//Release the client

AT+CMQTTREL=0

OK

//stop MQTT Service

AT+CMQTTSTOP

OK

+CMQTTSTOP: 0

4 Appendix

4.1 Summary of Error Codes

Code of <err>	Meaning
0	operation succeeded
1	failed
2	bad UTF-8 string
3	sock connect fail
4	sock create fail
5	sock close fail
6	message receive fail
7	network open fail
8	network close fail
9	network not opened
10	client index error
11	no connection
12	invalid parameter
13	not supported operation
14	client is busy
15	require connection fail
16	sock sending fail
17	timeout
18	topic is empty
19	client is used
20	client not acquired
21	client not released
22	length out of range
23	network is opened
24	packet fail
25	DNS error
26	socket is closed by server
27	connection refused: unaccepted protocol version
28	connection refused: identifier rejected

29	connection refused: server unavailable
30	connection refused: bad user name or password
31	connection refused: not authorized
32	handshake fail
33	not set certificate
34	Open session failed
35	Disconnect from server failed

SIMCom
Confidential