中国移动
China Mobile

ML302

SSL TCP 用户手册

4G 系列

版本：V1.0.0

日期：2019 年 9 月

中移物联网有限公司
iot.10086.cn

服务与支持

如果您有任何关于模组产品及产品手册的评论、疑问、想法，或者任何无法从本手册中找到答案的疑问，请通过以下方式联系我们。

中移物联网有限公司

网址： iot.10086.cn

邮箱： SmartModule@cmiot.chinamobile.com

客户服务热线： 400-110-0866

微信公众号： OneMO2019

文档声明

注意

本手册描述的产品及其附件特性和功能，取决于当地网络设计。因此，本手册中描述的全部或部分产品及其附件特性和功能可能未包含在您的购买或使用范围之内。

免责声明

除非合同另有约定，中移物联网有限公司对本文档内容不做任何明示或暗示的声明或保证，并且不对特定目的适销性及适用性或者任何间接、特殊或连带的损失承担任何责任。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。公司保留随时修改本手册中任何信息的权利，无需进行提前通知且不承担任何责任。

操作系统更新声明

操作系统仅支持官方升级；如用户自己刷非官方系统，导致安全风险和损失由用户负责。

固件包完整性风险声明

固件仅支持官方升级；如用户自己刷非官方固件，导致安全风险和损失由用户负责。

版权所有©中移物联网有限公司。保留一切权利。

关于文档

修订记录

版本	日期	作者	描述
V1.0.0	2019/09/25	喻炎森	初版

目录

1 文档概述

1.1 概述

该文档描述了中移物联网公司 ML302 SSL 加密协议的相关命令，用于指导使用 SSL 加密协议。在某些情况下，为了确保通信隐私，服务器和客户机之间的通信应该以加密的方式进行。这样可以防止在通信过程中窃听、篡改或伪造数据。使用 SSL 加密协议进行数据连接可以有效保障数据传输的安全。

文档详细描述了 TCPIP 连接使用 SSL 加密的相关指令。

ML302 支持的 SSL 协议版本如下。

SSL 协议版本
SSL3.0
TLS1.0
TLS1.1
TLS1.2

ML302 支持的加密套件如下。

加密套件	
0x0035	TLS_RSA_WITH_AES_256_CBC_SHA
0X0005	TLS_RSA_WITH_RC4_128_SHA
0X0004	TLS_RSA_WITH_RC4_128_MD5
0X000A	TLS_RSA_WITH_3DES_EDE_CBC_SHA
0X002F	TLS_RSA_WITH_AES_128_CBC_SHA
0X003D	TLS_RSA_WITH_AES_256_CBC_SHA256

2 指令详解

2.1 AT+QSSLCFG SSL 配置

AT+QSSLCFG	
语法	
测试命令 AT+QSSLCFG=?	**响应：** +QSSLCFG: “type”,(0-5),“value” OK
查询上下文的设置 AT+QSSLCFG=”ctxindex”, < ctxindex>	**响应：** +QSSLCFG: <ctxindex>,<sslversion>,<seclevel>, ciphersuite>,<cacert>,<clientcertname>,<clientkeyname> OK ERROR
配置 SSL 版本 AT+QSSLCFG=”sslversion”, ctxindex>，[<sslversion>]	**响应：** OK ERROR **如果省略第三个参数，则查询“sslversion”值** +QSSLCFG: ”sslversion”,<sslversion> OK
配置密码套件 AT+QSSLCFG=”ciphersuite”, <ctxindex>，[<list of supported <ciphersuite>s>]	**响应：** OK ERROR **如果省略第三个参数，则查询“ciphersuite”值** +QSSLCFG: ” ciphersuite”,< ciphersuite > OK
配置认证等级 AT+QSSLCFG=”seclevel”, <ctxindex>，[<seclevel>]	**响应：** OK ERROR **如果省略第三个参数，则查询“seclevel”值** +QSSLCFG: ”seclevel”,< seclevel > OK
配置根证书的路径 AT+QSSLCFG=”cacert”, <ctxindex>[<cacertname>]	**响应：** OK ERROR **如果省略第三个参数，则查询“cacertname”值** +QSSLCFG: ”cacert”,<cacertname> OK

AT+QSSLCFG	
语法 （接上页）	
配置客户端证书的路径 AT+QSSLCFG="clientcert", <ctxindex>，[<clientcertname>]	**响应：** OK ERROR **如果省略第三个参数，则查询"clientcertname"值** +QSSLCFG: "clientcert",< clientcertname> OK
配置客户端密钥的路径 AT+QSSLCFG="clientkey", <ctxindex>，[<clientkeyname>]	**响应：** OK ERROR **如果省略第三个参数，则查询"clientcertname"值** +QSSLCFG: "clientcert",< clientcertname> OK
配置是否忽略 RTC 时间 AT+QSSLCFG="ignorertctime" [,<ignorertctime>]	**响应：** OK ERROR **如果省略第二个参数，则查询"ignorertctime"值** +QSSLCFG: "ignorertctime",<ignorertctime > OK
配置是否使能 HTTPS 命令 AT+QSSLCFG="https" [,<httpsenable>]	**响应：** OK ERROR **如果省略第二个参数，则查询"https"值** +QSSLCFG: "https",<httpsenable > OK
配置 HTTPS 使用的 SSL 上下文 ID 号 AT+QSSLCFG="httpsctxi" [,<httpsctxindex>]	**响应：** OK ERROR **如果省略第二个参数，则查询"httpsctxi"值** +QSSLCFG: "httpsctxi",<httpsctxindex> OK
最大响应时间	300s
命令描述	
此 at 命令用于配置 SSL 版本、密码套件、安全级别、CA 证书、客户端证书、客户端密钥、rtc 时间忽略、http/https。这些参数是在握手过程中使用。	
参数描述	
<ctxindex>	
SSL 上下文 id	

AT+QSSLCFG	
参数描述	
<sslversion> ssl 支持版本	
0	SSL3.0
1	TLS1.0
2	TLS1.1
3	TLS1.2
4	全部支持
<ciphersuite> 字符串，配置密码套件	
0X0035	TLS_RSA_WITH_AES_256_CBC_SHA
0X002F	TLS_RSA_WITH_AES_128_CBC_SHA
0X0005	TLS_RSA_WITH_RC4_128_SHA
0X0004	TLS_RSA_WITH_RC4_128_MD5
0X000A	TLS_RSA_WITH_3DES_EDE_CBC_SHA
0X003D	TLS_RSA_WITH_AES_256_CBC_SHA256
0XFFFF	支持如上所有加密套件（默认）
<seclevel> 认证等级	
0	无身份验证
1	服务器什么验证
2	服务器和客户端双向验证
<cacertname>	
字符串，服务器 CA 证书路径。	
<clientcertname>	
字符串，客户端证书路径	
<clientkeyname>	
字符串，客户端密钥路径	
<ignorertctime> 是否忽略 RTC 时间	
0	不忽略
1	忽略
<httpsenable> 使能 HTTPS	
0	关闭 HTTPS
1	使能 HTTPS
<httpsctxindex> HTTPS 使用的 SSL 上下文 ID	
0-5	SSL 上下文 ID 范围
备注	
如果没有设置身份验证，则不需要安全数据。如果已设置服务器身份验证，则需要配置服务器 CA 证书。如果设置了服务器和客户端身份验证，则需要配置客户端证书、服务器 CA 证书和客户端私钥。 服务器 CA 证书路径为"/caCrt.pem", 客户端证书路径为" /clientCrt.pem"，客户端密钥路径为" /privateKey.pem"	
示例	
AT+QSSLCFG="seclevel",0,2 OK	

2.2 AT+QSECWRITE 添加证书或者密钥

AT+QSECWRITE	
语法	
测试命令 AT+QSECWRITE=?	**响应：** +QSECWRITE:(0~2) OK
配置命令 AT+QSECWRITE=<crtflag>	**响应：** **正常：** > 写入数据，ctrl+z 退出 +QSECWRITE: <uploadsize>,<chacksum> OK **错误：** ERROR/+CME ERROR: <err>
最大响应时间	1000ms
命令描述	
此命令用于将用户证书、用户密钥和 CA 证书添加到文件。证书和密钥将以加密的方式存储在这些存储库中。证书和密钥保存后，主机无法从中读取数据，而只能查询它们的校验和。请注意，在添加证书或密钥之前，如果它已经存在，请先删除。	
参数描述	
<crtflag>	
0	设置 CA 证书
1	设置客户端证书
2	设置客户端密钥
<uploadsize>	
写入的数据长度	
<checksum>	
校验和	
备注	
校验和计算方式如下： – 校验和为 16 为十六进制数，读取数据按两字节作为一个单位进行异或运算，末尾为单字节时最后补 0x00。 Chacksum=(data[0]<<8 | data[1]) XOR (data[2]<<8 | data[3]) XOR ... (data[2x-1]<<8 | data[2x]) – 当为单数个数据时： Chacksum=(data[0]<<8 | data[1]) XOR (data[2]<<8 | data[3]) XOR ... (data[x]<<8 | 0x00)	
示例	
AT+QSECWRITE=0 > <Input the data> +QSECWRITE: 1388,384a OK	

2.3 AT+QSECREAD 查询证书或者密钥的校验和

AT+QSECREAD	
语法	
测试命令 AT+QSECREAD=?	**响应：** +QSECREAD: (0~2) OK
配置命令 AT+QSECREAD=<crtflag>	**响应：** +QSECREAD: <good>,<checksum> OK ERROR/+CME ERROR: <err>
最大响应时间	300ms
命令描述	
此命令查询证书或者密钥的校验和。通过 qsecwrite 上传证书或密钥时，将同时存储证书或密钥的校验和。在执行 qsecread 之后，qsecread 将再次计算证书或密钥的校验和，然后将此校验和与 qsecwrite 存储的校验和进行比较，如果它们是相同的，证书或密钥是正确的，否则证书或密钥是错误的。	
参数描述	
<crtflag>	
0	设置 CA 证书
1	设置客户端证书
2	设置客户端密钥
<good> 指示证书或密钥是否正确。	
0	错误
1	正确
<checksum>	
校验和	
示例	
AT+QSECREAD=0 +QSECREAD: 1,553f OK	

2.4 AT+QSECDEL 删除证书或密钥

AT+QSECDEL	
语法	
测试命令 AT+QSECDEL=?	**响应：** +QSECDEL:(0~2) OK
配置命令 AT+QSECDEL=<crtflag>	**响应：** OK ERROR/+CME ERROR: <err>
最大响应时间	300ms
命令描述	
此命令用来删除指定的证书或密钥。	
参数描述	
<crtflag>	
0	设置 CA 证书
1	设置客户端证书
2	设置客户端密钥
示例	
AT+QSECDEL=0 OK	

2.5 AT+QSSLOPEN 建立加密连接

AT+QSSLOPEN	
语法	
测试命令 AT+QSSLOPEN=?	**响应:** +QSSLOPEN: <ssid>,<ctxindex>,<ipaddr/domain e>,<port>,<connectmode>[,<timeout>] OK
查询命令 AT+QSSLOPEN?	**响应:** OK
配置命令 AT+QSSLOPEN=<ssid>, <ctxindex>,<ipaddr/domainname>, <port>,<connectmode>[,<timeout>]	**响应:** **成功:** OK **失败:** ERROR/+CME ERROR: <err> **执行结果将上报 URC:** +QSSLOPEN: <ssid>,<connectcode>
命令描述	
此命令通过 TCP 方式建立一条加密连接用于后续数据收发。	
参数描述	
<ssid> 连接序号	
0-5	连接序号范围
<ctxindex> SSL 上下文 ID	
0-5	SSL 上下文 ID 范围
<ipaddr/domainname>	
字符串，服务器地址	
<port>	
端口号	
<connectmode> 传输模式	
0	非透传
1	透出
<timeout> 超时时间	
10-300（s，默认 90s)	超时时间范围
<connectcode> 返回结果码	
0	成功
-1	错误
-2	Socket 已被占用
示例	
AT+QSSLOPEN=0,0,"www.iottest.work",443,0 OK +QSSLOPEN: 0,0	

2.6 AT+QSSLCLOSE 关闭加密连接

AT+QSSLCLOSE	
语法	
测试命令 AT+QSSLCLOSE=?	**响应：** +QSSLCLOSE: (0-5)[,(0,1)] OK
查询命令 AT+QSSLCLOSE?	**响应：** OK
配置命令 AT+QSSLCLOSE=<ssid>[,<closetype>]	**响应：** **成功：** CLOSE OK **失败：** ERROR/+CME ERROR: <err>
命令描述	
此命令用来关闭指定的加密连接。	
参数描述	
<ssid> 连接序号	
0-5	连接序号范围
<closetype> 保留参数	
0-1	保留参数范围
示例	
AT+QSSLCLOSE=0 OK 0,CLOSE OK	

2.7 AT+QSSLSEND 通过加密连接发送数据

AT+QSSLSEND	
语法	
测试命令 AT+QSSLSEND=?	**响应** + QSSLSEND: (0-5) OK
查询命令 AT+ QSSLSEND?	**响应** OK
配置命令 AT+QSSLSEND=<ssid>	**响应：** **成功：** > 输入数据，发送“CTRL+Z”发送，或者通过“ESC”取消发送 **发送成功：** SEND OK **发送失败：** SEND FAIL **失败：** ERROR/+CME ERROR: <err>
命令描述	
此命令通过指定一条已建立的加密连接发送数据。输入命令后出现‘>’，此时在 sendbox 中输入要发送的数据，按 CTRL+Z 发送。	
参数描述	
<ssid> 连接序号	
0-5	连接序号范围
示例	
AT+QSSLSEND=0 ><input send data><CTRL+Z> SEND OK	//向 ssid 为 0 的加密连接发送数据

2.8 AT+QSSLRECV 通过加密连接获取数据

该命令用于获取数据，当模组收到网络数据时将上报"+QSSLURC: "recv",<cid>,<ssid>",此时可使用该命令读取数据。

AT+QSSLRECV	
语法	
测试命令 AT+ QSSLRECV =?	**响应：** + QSSLRECV: (0,1),(0-5),(1,1500) OK
查询命令 AT+ QSSLRECV?	**响应：** OK
配置命令 AT+QSSLRECV=<cid><ssid>,<length>	**响应：** **成功：** +QSSLRECV: <ipaddr>:<port>,TCP,<actuallength> <CR><LF><data> OK **如果无数据，直接返回** OK **失败：** ERROR/+CME ERROR: <err>
命令描述	
该命令用于获取数据，当模组收到网络数据时将上报"+QSSLURC: "recv",<cid>,<ssid>",此时可使用该命令读取数据。	
参数描述	
<cid> 保留参数，对命令无影响	
0-1	保留参数范围
<ssid> 连接序号	
0-5	激活协议栈
<length> 接收长度	
（1-1460）	接收长度范围
示例	
AT+QSSLRECV=1,0,1460 +QSSLRECV: 106.12.79.254:443,TCP,434 <This is the recv data> OK	

2.9 AT+QSSLSTATE 查询连接状态

AT+QSSLSTATE	
语法	
测试命令 AT+ QSSLSTATE =?	**响应：** OK
查询命令 AT+ QSSLSTATE?	**响应：** OK
执行命令 AT+QSSLSTATE	**响应：** **成功：** +QSSLSTATE: <state> +QSSLSTATE: <socketindex>,<connectiontype>,<ipadd>,<port>, <socketstatus>,<sslconnectionflag> ... OK **失败：** ERROR/+CME ERROR: <err>
命令描述	
此命令用于查询所有连接状态。	
参数描述	
<state> 字符串参数；表明连接状态	
"IP INITIAL"	初始化
"IP START"	启动任务
"IP CONFIG"	配置场景
"IP IND"	激活 GPRS/CSD 场景中
"IP GPRSACT"	接收场景配置
"IP STATUS"	获得本地 IP 地址（参考 AT+QILOCIP 命令）
"IP PROCESSING"	数据阶段
"PDP DEACT"	GPRS/CSD 场景异常关闭
<socketindex>	
连接序号，范围为 0-5。	
<connectiontype> 连接类型	
"TCP"	TCP 连接
"UDP"	UDP 连接
<ipadd>	
远程连接或接入 IP 地址。	
<port>	
远程连接或接入端口号。	

AT+QSSLSTATE	
参数描述	
<socketstatus> 字符串参数；表明接入连接状态。	
“INITIAL” “CONNECTING” “CONNECTED” “REMOTE CLOSING” “CLOSING” “CLOSED”	
<sslconnectionflag> 加密连接标志	
0	普通连接
1	加密连接
示例	
AT+QSSLSTATE +QSSLSTATE: 0,"TCP","106.12.79.254",443,"CONNECTED",1 +QSSLSTATE: 1,"TCP","",0,"INITIAL",1 +QSSLSTATE: 2,"TCP","",0,"INITIAL",1 +QSSLSTATE: 3,"TCP","",0,"INITIAL",1 +QSSLSTATE: 4,"TCP","",0,"INITIAL",1 +QSSLSTATE: 5,"TCP","",0,"INITIAL",1 OK	

2.10 +QSSLURC URC 上报

+QSSLURC 为特定情况下的主动上报信息，用于提示模组收到数据或者连接非主动断开的情况。

+QSSLURC	
语法	
+QSSLURC: "recv",<cid>,<ssid>	接收到数据
+QSSLURC: "close",<ssid>	连接非主动断开
命令描述	
+QSSLURC 为特定情况下的主动上报信息，用于提示模组收到数据或者连接非主动断开的情况。	
参数描述	
<cid> 保留参数，对命令无影响	
0-1	保留参数范围
<ssid> 连接序号	
0-5	连接序号范围

3 示例

AT+CGDCONT=1,"IP","CMNET"
OK
AT+CGACT=1,1
+CGACT: 1, 1, 10.127.79.43
OK
AT+QSSLCFG="seclevel",0,0
OK
AT+QSSLOPEN=0,0,"www.iottest.work",443,0
OK
+QSSLOPEN: 0,0
AT+QSSLSEND=0
> GET https://www.iottest.work/test.html HTTP/1.1
Host: www.iottest.work
Connection: keep-alive
SEND OK
OK
+QSSLURC,"recv",1,0
AT+QSSLRECV=1,0,1460
+QSSLRECV: 106.12.79.254:443,TCP,434
HTTP/1.1 200 OK
Date: Sat, 12 Oct 2019 01:05:55 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
Last-Modified: Fri, 22 Feb 2019 07:38:30 GMT
ETag: "72-58276ad682560"
Accept-Ranges: bytes
Content-Length: 114
Keep-Alive: timeout=300, max=200
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
<html>
<head>
<title>
IOTTEST
</title>
</head>
<body>
Hello!This is an IOT test webpage!
</body>
</html>
OK
AT+QSSLCLOSE=0
OK
0,CLOSE OK