OneMO | 中国移动 China Mobile

# SSL用户手册

OneMO_1207

版本：V5.3.0
发布日期：2024/1/10

China Mobile IoT Co., Ltd.
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。

**OneMO官网：** onemo10086.com

**邮箱：** SmartModule@cmiot.chinamobile.com

**客户服务热线：400-110-0866**

中国移动 China Mobile OneMO 1207

# 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或网络性能，同时也取决于用户预先安装的各种软件。由于当地网络运营商、ISP，或当地网络设置等原因，可能也会造成本手册中描述的全部或部分产品及其附件特性和功能未包含在您的购买或使用范围之内。

## 责任限制

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的、特殊的或连带的损失承担任何责任。

在适用法律允许的范围内，在任何情况下，中移物联网有限公司均不对用户因使用本手册内容和本手册中描述的产品而引起的任何特殊的、间接的、附带的或后果性的损坏、利润损失、数据丢失、声誉和预期的节省而负责。

因使用本手册中所述的产品而引起的中移物联网有限公司对用户的最大赔偿（除在涉及#身伤害的情况中根据适用法律规定的损害赔偿外），不应超过用户为购买此产品而支付的金额。

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。

## 商标声明

中国移动 China Mobile 为中国移动注册商标。

本手册和本手册描述的产品中出现的其他商标、产品名称、服务名称和公司名称，均为其各自所有者的财产。

## 进出口法规

出口、转口或进口本手册中描述的产品（包括但不限于产品软件和技术数据），用户应遵守相关进出口法律和法规。

## 隐私保护

关于我们如何保护用户的个人信息等隐私情况，请查看相关隐私政策。

## 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。

本手册中描述的产品，可能包含中移物联网有限公司及其存在的许可人享有版权的软件，除非获得相关权利人的许可，否则，非经本公司书面同意，任何单位和个人不得擅自摘抄、复制本手册内容的部分或全部，并以任何形式传播。

中国移动 China Mobile OneMO 12017

# 关于文档

## 修订记录

| 版本 | 描述 |
| --- | --- |
| V1.0.0 | 初版 |
| V2.0.0 | 新增ML307A相关内容 |
| V3.0.0 | 新增ML302A相关内容 |
| V4.0.0 | 新增ML305U相关内容 |
| V5.0.0 | 新增ML305A相关内容 |
| V5.0.1 | 更新手册适用范围，新增ML307A-DL型号信息。 |
| V5.0.2 | 更新手册适用范围，新增ML305A-DL型号信息。 |
| V5.0.3 | 新增ML305M相关内容；<br>更新“AT+MSSLKEYWR 写入SSL私钥”中命令描述和*<length>*参数描述。 |
| V5.1.0 | 新增ML307R相关内容 |
| V5.2.0 | 新增MN326相关内容 |
| V5.3.0 | 新增ML307G相关内容 |

OneMO 120 China Mobile

# 目录

服务与支持 ii
文档声明 iii
关于文档 v
1. 引言 7
1.1. 适用型号 7
2. AT命令概述 8
2.1. AT命令语法 9
2.2. AT命令响应 10
3. SSL协议AT命令 11
3.1. AT+MSSLCFG 配置SSL Context参数 11
3.2. AT+MSSLCERTWR 写入SSL证书 19
3.3. AT+MSSLKEYWR 写入SSL私钥 21
3.4. AT+MSSLCERTRD 读取SSL证书 23
3.5. AT+MSSLLIST 列出已存在证书及密钥名称 24
3.6. AT+MSSLRM 删除SSL证书 26
3.7. AT+MSSLPSK 配置PSK预共享密钥 27
3.8. AT+MSSLCHECK 校验证书或密钥正确性 28
3.9. AT+MSSLCIPHER 查询密码套件 30
4. 示例 31
4.1. 示例 31
5. 附录 33
5.1. 密码套件算法 33
5.2. 错误码 41

# 1. 引言

本文档针对本公司产品功能内容和相关操作进行详细说明，以供客户参考。如有未尽细节，请咨询中移物联网技术支持。

## 1.1. 适用型号

Table 1. 适用模组

| 模组系列 | 模组子型号 |
| --- | --- |
| MN316 | MN316-DBRS/MN316-DLVS |
| MN316-S | MN316-S-DLVS |
| MN326 | MN326-X |
| ML302A | ML302A-DCLM/ML302A-DSLM/ML302A-GCLM/ML302A-GSLM |
| ML302S | ML302S-DNLM |
| ML305A | ML305A-DC/ML305A-DS/ML305A-DL |
| ML307A | ML307A-DCLN/ML307A-DSLN/ML307A-GCLN/ML307A-GSLN/ML307A-DL |
| ML307S | ML307S-DNLM |
| ML305U | ML305U-DBLN |
| ML305M | ML305M-DSLM |
| ML307R | ML307R-DC/ML307R-DL |
| ML307G | ML307G-DL |

# 2. AT命令概述

本章主要介绍AT命令定义及其语法格式。

AT命令是从TE（Terminal Equipment，终端设备）或DTE（Data Terminal Equipment，数据终端设备）向TA（Terminal Adaptor，终端适配器）或DCE（Data Circuit Terminal Equipment，数据电路终端设备）发送的特定格式的字符串。TE通过TA发送AT命令来控制MS（Mobile Station，移动台）的功能，与网络业务进行交互。用户可以通过AT命令进行呼叫、短消息、电话本、数据业务、补充业务、传真等方面的控制。

中国移动 China Mobile OneMO 12017

## 2.1. AT命令语法

AT命令必须以“AT”或“at”开头，以回车符<CR>结尾；命令后面跟随结构为“<CR><LF>response<CR><LF>”的响应。为便于阅读，文档中将省略<CR><LF>，仅展示响应内容。

中移物联网模组实现的AT命令集包含3GPP TS 27.005、3GPP TS 27.007、ITU-TV.25ter标准命令集和中移物联网自定义的扩展命令集。

AT命令根据语法结构可归为基础语法、S参数语法和扩展语法3类。

### 基础语法

该类AT命令格式为“AT<x><n>”或“AT&<x><n>”；其中“<x>”是命令，“<n>”是命令参数。

比如命令“ATE<n>”，该命令根据“<n>”值确定DCE是否需要将接收到的字符反馈给DTE。“<n>”是可选项，如果不带该值则使用缺省值。

### S参数语法

该类AT命令格式为“ATS<n>=<m>”，其中“<n>”是要设置S寄存器索引，“<m>”是设置值。

### 扩展语法

该类AT命令有多种操作模式。

Table 2. AT命令及响应类型

| 类型 | 命令 | 响应描述 |
| --- | --- | --- |
| 测试命令 | AT+<CMD>=? | 返回参数列表及参数值范围 |
| 读取命令 | AT+<CMD>? | 返回参数当前值 |
| 配置命令 | AT+<CMD>=<p1>[,<p2[,<p3>[…]]] | 设置参数值 |
| 执行命令 | AT+<CMD> | 执行具体操作 |

其中：

- <…>尖括号中是参数，实际输入时不包含尖括号；
- […]方括号中的参数是可选参数。

## 2.2. AT命令响应

Table 3. AT命令响应类型

| 响应 | 释义描述 |
| --- | --- |
| ERROR | AT命令格式错误或其他错误 |
| +CME ERROR: <err>或者+CMS ERROR: <err>或者+CIS ERROR: <err> | 启用了扩展错误报告（+CMEE），其中<err>表示错误码或详细错误信息 |
| OK | AT命令执行成功 |

Note:

AT命令响应结果中，冒号“:”后均存在空格，用以分隔响应头与参数列表。

手册描述中错误响应用+ CME ERROR: <err>或者+CMS ERROR: <err>或者+CIS ERROR: <err>表示，实际返回情况参考AT+CMEE命令。

中国移动 China Mobile OneMO 1207

# 3. SSL协议AT命令

本章详细描述了SSL协议相关的AT命令和命令格式。

## 3.1. AT+MSSLCFG 配置SSL Context参数

本命令用于配置SSL Context参数操作。

| AT+MSSLCFG | |
|---|---|
| 语法 | 响应 |
| 测试命令<br>**AT+MSSLCFG=?** | 成功<br>*+MSSLCFG: (list of support<cmd>s)*<br>*OK*<br>错误<br>*+CME ERROR: <err>* |
| 设置命令（配置认证方式）<br>**AT +MSSLCFG="auth"[,<ssl_id>[ ,<cert_verify>]]** | 成功<br>仅配置参数***"auth"***，读取所有ssl id配置：<br>*+MSSLCFG: "auth",0,<cert_verify>*<br>*+MSSLCFG: "auth",1,<cert_verify>*<br>*.....*<br>*OK*<br>配置参数***"auth"***与***<ssl_id>***，读取指定ssl id配置：<br>*+MSSLCFG: "auth",<ssl_id>,<cert_verify>*<br>*OK*<br>配置完整参数：<br>*OK*<br>错误<br>*+CME ERROR: <err>* |
| 设置命令（配置证书及密钥）<br>**AT +MSSLCFG="cert"[,<ssl_id>[, <srv_cert>,<cli_cert>,<prv_k ey>]]** | 成功<br>仅配置参数***"cert"***，读取所有ssl id配置：<br>*+MSSLCFG: "cert",0,<srv_cert>,<cli_cert>,<prv_key>*<br>*+MSSLCFG: "cert",1,<srv_cert>,<cli_cert>,<prv_key>*<br>*.....*<br>*OK* |

| AT+MSSLCFG | |
|---|---|
| | 配置参数*"cert"*与*<ssl_id>*，读取指定ssl id配置：<br>`+MSSLCFG: "cert",<ssl_id>,<srv_cert>,<cli_cert>,<prv_key>`<br>`OK`<br>配置完整参数：<br>`OK`<br>错误<br>`+CME ERROR: <err>` |
| 设置命令（配置PSK）<br>**AT +MSSLCFG="psk"[,<ssl_id>[,<pskid>]]** | 成功<br>配置参数*"psk"*，读取所有ssl id配置：<br>`+MSSLCFG: "psk",0,<pskid>`<br>`+MSSLCFG: "psk",1,<pskid>`<br>`.....`<br>`OK`<br>配置参数*"psk"*与*<ssl_id>*，读取指定ssl id配置：<br>`+MSSLCFG: "psk",<ssl_id>,<pskid>`<br>`OK`<br>配置完整参数：<br>`OK`<br>错误<br>`+CME ERROR: <err>` |
| 设置命令（配置输入数据编码格式）<br>**AT +MSSLCFG="encoding"[,<ssl_id>[,<input_format>]]** | 成功<br>配置参数*"encoding"*，读取所有ssl id配置：<br>`+MSSLCFG: "encoding",0,<input_format>`<br>`+MSSLCFG: "encoding",1,<input_format>`<br>`.....`<br>`OK`<br>配置参数*"encoding"*与*<ssl_id>*，读取指定ssl id配置：<br>`+MSSLCFG: "encoding",<ssl_id>,<input_format>`<br>`OK`<br>配置完整参数：<br>`OK`<br>错误 |

| AT+MSSLCFG | |
|---|---|
| | *+CME ERROR: <err>* |
| 设置命令（配置SSL协商超时时间）<br>**AT +MSSLCFG="negotime"[,<ssl_id>[,<negotiate_timeout>]]** | 成功<br>配置参数***"negotime"***，读取所有ssl id配置：<br>*+MSSLCFG: "negotime",0,<negotiate_timeout>*<br>*+MSSLCFG: "negotime",1,<negotiate_timeout>*<br>*.....*<br>*OK*<br>配置参数***"negotime"***与***<ssl_id>***，读取指定ssl id配置：<br>*+MSSLCFG: "negotime",<ssl_id>,<negotiate_timeout>*<br>*OK*<br>配置完整参数：<br>*OK*<br>错误<br>*+CME ERROR: <err>* |
| 设置命令（配置SSL指定版本）<br>**AT +MSSLCFG="version"[,<ssl_id>[,<ssl_version>]]** | 成功<br>配置参数***"version"***，读取所有ssl id配置：<br>*+MSSLCFG: "version",0,<ssl_version>*<br>*+MSSLCFG: "version",1,<ssl_version>*<br>*.....*<br>*OK*<br>配置参数***"version"***与***<ssl_id>***，读取指定ssl id配置：<br>*+MSSLCFG: "version",<ssl_id>,<ssl_version>*<br>*OK*<br>配置完整参数：<br>*OK*<br>错误<br>*+CME ERROR: <err>* |
| 设置命令（配置SSL指定加密套件）<br>**AT +MSSLCFG="ciphersuite"[,<ssl_id>[,<cipher_suite>]]** | 成功<br>配置参数***"ciphersuite"***，读取所有ssl id配置：<br>*+MSSLCFG: "ciphersuite",0,<cipher_suite>*<br>*+MSSLCFG: "ciphersuite",1,<cipher_suite>*<br>*.....*<br>*OK* |

| AT+MSSLCFG | |
|---|---|
| | 配置参数*"ciphersuite"*与*<ssl_id>*，读取指定ssl id配置：<br>`+MSSLCFG: "ciphersuite",<ssl_id>,<cipher_suite>`<br>`OK`<br>配置完整参数：<br>`OK`<br>错误<br>`+CME ERROR: <err>` |
| 设置命令（配置SSL会话恢复功能打开/关闭）<br>**AT+MSSLCFG="session"[,<ssl_id>[,<session_enable>]]** | 成功<br>配置参数*"session"*，读取所有ssl id配置：<br>`+MSSLCFG: "session",0,<session_enable>`<br>`+MSSLCFG: "session",1,<session_enable>`<br>`.....`<br>`OK`<br>配置参数*"session"*与*<ssl_id>*，读取指定ssl id配置：<br>`+MSSLCFG: "session",<ssl_id>,<session_enable>`<br>`OK`<br>配置完整参数：<br>`OK`<br>错误<br>`+CME ERROR: <err>` |
| 设置命令（配置SSL是否忽略证书时间戳）<br>**AT+MSSLCFG="ignorestamp"[,<ssl_id>[,<ignore_stamp>]]** | 成功<br>配置参数*"ignorestamp"*，读取所有ssl id配置：<br>`+MSSLCFG: "ignorestamp",0,<ignore_stamp>`<br>`+MSSLCFG: "ignorestamp",1,<ignore_stamp>`<br>`.....`<br>`OK`<br>配置参数*"ignorestamp"*与*<ssl_id>*，读取指定ssl id配置：<br>`+MSSLCFG: "ignorestamp",<ssl_id>,<ignore_stamp>`<br>`OK`<br>配置完整参数：<br>`OK`<br>错误 |

| AT+MSSLCFG | |
|---|---|
| | *+CME ERROR: <err>* |
| 设置命令（配置SSL是否忽略证书认证结果）<br>**AT +MSSLCFG="ignoreverify"[,<ssl_id>[,<ignore_verify>]]** | 成功<br>配置参数***"ignoreverify"***，读取所有ssl id配置：<br>*+MSSLCFG: "ignoreverify",0,<ignore_verify>*<br>*+MSSLCFG: "ignoreverify",1,<ignore_verify>*<br>*.....*<br>*OK*<br>配置参数***"ignoreverify"***与***<ssl_id>***，读取指定ssl id配置：<br>*+MSSLCFG: "ignoreverify",<ssl_id>,<ignore_verify>*<br>*OK*<br>配置完整参数：<br>*OK*<br>错误<br>*+CME ERROR: <err>* |

## 命令描述

设置SSL相关操作需要的配置选项，包含配置SSL认证方式、证书及密钥、PSK、输入数据编码格式、SSL协商超时时间、SSL指定版本、SSL指定加密套件、打开或关闭会话恢复功能、是否忽略证书时间戳、是否忽略证书认证结果等功能。当仅输入配置选项字符串时，查询该选项当前的配置。[1]

## 参数描述

***<cmd>*** 字符串，命令类型。

***auth***

配置认证方式

***cert***

配置证书及密钥

***psk***

配置PSK

***encoding***

配置输入数据编码格式

***negotime***

配置SSL协商超时时间

***version***

配置SSL指定版本

***ciphersuite***

配置SSL指定加密套件

1. 需在建立 SSL 连接前进行证书输入和相应模式配置，否则将无法生效。

**AT+MSSLCFG**

***session***

配置SSL会话恢复功能打开/关闭

***ignorestamp***

配置SSL是否忽略证书时间戳

***ignoreverify***

配置SSL是否忽略证书认证结果

*<ssl_id>* 整型，SSL连接ID，范围：0~5。[2]

*<cert_verify>* 整型，证书认证方式，默认值0。

***0***

无身份认证，默认值。

***1***

单向认证

***2***

双向认证

*<pskid>* 字符串型，预共享密钥id，不超过64字节。[3]

*<input_format>* 整型，输入数据编码格式，默认值2。[4]

***0***

ascii字符串

***1***

Hex格式字符串

***2***

转义字符串，默认值。

*<negotiate_timeout>* 整型，SSL协商超时时间，范围：10~300，默认值300，单位：s。

*<srv_cert>* 字符串型，受信任CA 证书名称，不超过64字节。

*<cli_cert>* 字符串型，客户端证书名称，不超过64字节。

*<prv_key>* 字符串型，客户端密钥名称，不超过64字节。

*<ssl_version>* 整型，指定SSL版本，默认值255。

***0***

SSL 3.0

***1***

TLS 1.0

***2***

2. NB系列支持范围0~4。
3. 4G 系列不支持该参数。
4. MN316/MN326/ML302S/ML307S/ML302A/ML305A/ML307A/ML305U/ML305M/ML307G/ML307R：只支持2转义字符串。

**AT+MSSLCFG**

TLS 1.1

***3***

TLS 1.2

***255***

全部

*<cipher_suite>* 十六进制字符串，指定加密套件，默认值0。

***0***

支持所有加密套件

其他

参考附录

*<session_enable>* 整型，是否开启会话恢复功能，默认值1。

***0***

关闭

***1***

开启

*<ignore_stamp>* 整型，是否忽略证书时间戳，默认值1。

***0***

不忽略

***1***

忽略

*<ignore_verify>* 整型，是否忽略证书认证结果，默认值0。

***0***

不忽略

***1***

忽略

示例

配置pskid

```
AT+MSSLCFG="psk",1,"1"
OK
```

查询ssl id1的加密套件

```
AT+MSSLCFG="ciphersuite",1
+MSSLCFG: "ciphersuite",1,0x01
OK
```

设置ssl id1的加密套件

**AT+MSSLCFG**

```
AT+MSSLCFG="ciphersuite",1,2D
OK
```

查询所有ssl id的输入数据编码格式

```
AT+MSSLCFG="encoding"
+MSSLCFG: "encoding",0,2
+MSSLCFG: "encoding",1,2
+MSSLCFG: "encoding",2,2
+MSSLCFG: "encoding",3,2
+MSSLCFG: "encoding",4,2
OK
```

Note: MN316/MN326从深睡眠唤醒后，SSL所有配置需要重新设置，包括写入的证书；最多同时建立两路SSL连接。

中国移动 China Mobile OneMO 1207

## 3.2. AT+MSSLCERTWR 写入SSL证书

本命令用于写入SSL证书。

| AT+MSSLCERTWR | |
|---|---|
| 语法 | 响应 |
| 测试命令<br>**AT+MSSLCERTWR=?** | 成功<br>*OK*<br>错误<br>*+CME ERROR: <err>* |
| 设置命令<br>**AT+MSSLCERTWR=<cert_name>,<remain_length>,<length>[,<data>]** | 成功<br>***<data>***不设置，输入数据达指定长度时结束输入：<br>>(输入指定*length*长度的证书文件内容)<br>*OK*<br>所有参数均设置：<br>*OK*<br>错误<br>*+CME ERROR: <err>* |
| 命令描述 | |
| 配置SSL证书，包含配置证书名称，证书剩余待写入长度，本次写入证书长度。[5] | |
| 参数描述 | |
| ***<cert_name>*** 字符串型，证书名称，不超过64字节。 | |
| ***<remain_length>*** 整型，剩余待写入的数据长度。<br>***0***<br>剩余待写入长度为0，表示本包为最后一包。<br>其他<br>剩余待写入长度，还需再次写入。 | |
| ***<length>***<br>整型，当前输入证书数据长度，单个证书最多写入8K（8192字节）数据。数据模式下不可设置为0，命令中直接输入数据时，设置为0，不对数据长度进行校验，设置大于0，将对输入数据的长度进行校验（ascii字符串和带转义的字符串输入模式下：校验实际命令中输入字符串长度是否与指定长度相等；Hex字符串输入模式下：校验实际命令中输入字符串长度是否是指定长度的两倍）。 | |
| ***<data>*** 字符串型，写入的证书内容，必须为PEM格式。 | |

5. 对同一证书文件进行写操作时将删除之前存在的证书文件；**AT+MSSLCFG="encoding"**配置为转义字符输入时，证书中的换行需用\r\n替换。

## AT+MSSLCERTWR

### 示例

配置SSL证书

```
AT+MSSLCERTWR="baidu.cer",0,1261
>
-----BEGIN CERTIFICATE-----
MIIDdTCCAl2gAwIBAgILBAAAAAABFUtaw5QwDQYJKoZIhvcNAQEFBQAwVzELMAkG
A1UEBhMCQkUxGTAXBgNVBAoTEEdsb2JhbFNpZ24gbnYtc2ExEDAOBgNVBAsTB1Jv
b3QgQ0ExGzAZBgNVBAMTEkdsb2JhbFNpZ24gUm9vdCBDQTAeFw05ODA5MDExMjAw
MDBaFw0yODAxMjgxMjAwMDBaMFcxCzAJBgNVBAYTAkJFMRkwFwYDVQQKExBHbG9i
YWxTaWduIG52LXNhMRAwDgYDVQQLEwdSb290IENBMRswGQYDVQQDExJHbG9iYWxT
aWduIFJvb3QgQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDaDuaZ
jc6j40+Kfvvxi4Mla+pIH/EqsLmVEQS98GPR4mdmzxzdzxtIK+6NiY6arymAZavp
xy0Sy6scTHAHoT0KMM0VjU/43dSMUBUc71DuxC73/OlS8pF94G3VNTCOXkNz8kHp
1Wrjsok6Vjk4bwY8iGlbKk3Fp1S4bInMm/k8yuX9ifUSPJJ4ltbcdG6TRGHRjcdG
snUOhugZitVtbNV4FpWi6cgKOOvyJBNPc1STE4U6G7weNLWLBYy5d4ux2x8gkasJ
U26Qzns3dLlwR5EiUWMWea6xrkEmCMgZK9FGqkjWZCrXgzT/LCrBbBlDSgeF59N8
9iFo7+ryUp9/k5DPAgMBAAGjQjBAMA4GA1UdDwEB/wQEAwIBBjAPBgNVHRMBAf8E
BTADAQH/MB0GA1UdDgQWBBRge2YaRQ2XyolQL30EzTSo//z9SzANBgkqhkiG9w0B
AQUFAAOCAQEA1nPnfE920I2/7LqivjTFKDK1fPxsnCwrvQmeU79rXqoRSLblCKOz
yj1hTdNGCbM+w6DjY1Ub8rrvrTnhQ7k4o+YviiY776BQVvnGCv04zcQLcFGUl5gE
38NflNUVyRRBnMRddWQVDf9VMOyGj/8N7yy5Y0b2qvzfvGn9LhJIZJrglfCm7ymP
AbEVtQwdpf5pLGkkeB6zpxxxYu7KyJesF12KwvhHhm4qxFYxldBniYUr+WymXUad
DKqC5JlR3XC321Y9YeRq4VzW9v493kHMB65jUr9TU/Qr6cf9tveCX4XSQRjbgbME
HMUfpIBvFSDJ3gyICh3WZlXi/EjJKSZp4A==
-----END CERTIFICATE-----
OK
```

Note: MN316/MN326：不支持>下的数据输入模式，只能在AT命令中直接输入数据。

# 3.3. AT+MSSLKEYWR 写入SSL私钥

本命令用于写入SSL私钥。

| AT+MSSLKEYWR | |
|---|---|
| 语法 | 响应 |
| 测试命令<br>**AT+MSSLKEYWR=?** | 成功<br>*OK*<br>错误<br>*+CME ERROR: <err>* |
| 设置命令<br>**AT+MSSLKEYWR=<key_name>,<remain_length>,<length>[,<data>]** | 成功<br>***<data>***不设置，输入数据达指定长度时结束输入：<br>>(输入指定*length*长度的私钥文件内容)<br>*OK*<br>所有参数均设置：<br>*OK*<br>错误<br>*+CME ERROR: <err>* |

**命令描述**

写入SSL私钥，包含配置私钥名称，私钥剩余待写入长度，本次写入私钥长度。[6]

**参数描述**

***<key_name>*** 字符串型，私钥名称，不超过64字节。

***<remain_length>*** 整型，剩余待写入的数据长度。

***0***

剩余待写入长度为0，表示本包为最后一包。

其他

剩余待写入长度，还需再次写入。

***<length>***

整型，当前输入私钥数据长度，单个私钥最多写入8K（8192字节）数据。数据模式下不可设置为0，命令中直接输入数据时，设置为0，不对数据长度进行校验，设置大于0，将对输入数据的长度进行校验（ascii字符串和带转义的字符串输入模式下：校验实际命令中输入字符串长度是否与指定长度相等；Hex字符串输入模式下：校验实际命令中输入字符串长度是否是指定长度的两倍）。

***<data>*** 字符串型，写入的私钥内容，私钥内容必须为PEM格式。

6. 对同一私钥文件进行写操作时将删除之前存在的私钥文件；**AT+MSSLCFG="encoding"**配置为转义字符输入时，私钥中的换行需用\r\n替换。

## AT+MSSLKEYWR

### 示例

写入SSL私钥

```
AT+MSSLKEYWR="test.key",0,1674
>
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAiMdJCQi3trZSSRAPW+L5Up53R/gFLuj2wN+DWLujkuXprLEO
E5QzNCA+jcA1YeIbHDmKxv/mTalRmchL77T6Qjdx21W11PJh47/DKW18VaWjU0dr
FiHPuUZiN3NUKjacQIow2yEN3K3x/hOr7dpWkyrv6ZHKHbuz+1V97IXt0CFMqqh6
8gTHsJct8ycKOgt1yl/ZBq7s+gwAAiwF3entQ0RxVStW+1xSKPylRZlZlULMu0Tt
qHhf3fc1oYFCmylJUIFF7Sq6AI14BGIV23DCgfGTUihDmERZrcnIU+eIHQiV8nMH
bqi1Uh/BjOaeY0L5xwPjyx2WrZiYyq3SEtry0QIDAQABAoIBAADi78N9+bjWripY
jwzsp+qD6eh+wEPZUS4XVMHYt3rugAj1Pc7dLUbHdbhT+FSZ00ynx9E529uBfyyk
um9DiEKxGs0N3WeTqZRBDCoC0mU4tVoHErfaQL8l6GGNHwzF/VXCv4XQDUeyneik
Zn8cZOa/xr3ICtwN+SDmITKM/KlWZ3x5wWO47vFbaDK8OHPRfwL4CdCxjBHlQ/eE
p2+g3GWe43XWPfhLe7h+/sl5xHaoLbl9wsIzxK2DwBXiKsaqikEbTkc5qTFjtbAB
C2hbDmHEyGewpT2dTfZKwtQGvgF8ja0qmOc1z8PB8m2Y5fUwUw89bU5WbEE61WUq
bFkGlxUCgYEAvv59fg/jc75w644TwUnmLTR72z3KZI1qxiYaO1Kd0wc60nzPHnwi
8Ecyld4dZ73Q5HUl1OG/5Pz/Orpr97wRN/CP/Td0NbTls7hjn3C39z49m6jf05KH
xZaQx/CT6ZuQaI8j1Qp/wbW8AxxEE4sFsv511Oq/doBMWyKpg2aak50CgYEAt1Tu
WKitqMCq0lst/gc67svMZjb4Q3LoIIaQFgOCVLVPou2iZuIYrRUKOoPt5KCp4T2K
rh6Mjf6yAXOpw4NxUQXNMOJZmTWthCFc/XvFKC/dcxT8icg7tCBuHjMRTU3AZ2qt
oRqmoZnZ6c7poPEU5WhH0KNbNQdstjK/vcChV8UCgYEAt8FHYZrNvdUS9T5reUKt
Jv7gzw2DBP0eJmgQQtT4rUi+ajbUWsMaJkyJubDKX747FSl0dL2Bj0FuGcW0DNQv
SL+0+O16bBV0J50WlBaxmDmUsodmWTsYT5zNzN+En3QhGsfktJp2UhuUOPXf9WGC
6TRyj5gO/2buj5wotRhpTe0CgYBA5MFRhLOjzj8plrlO+AQ2TtFVRRPv3BaqnLcX
87olff1ocLFRtaqCabYrLFPi37QCVKRoKcwa3xLnTKfE2xwbT/Bn41dP0h5PbPfb
ihoptXevqrgRlVz8z5Xq/qybLnByquI26pYdEbZ++ozcOTnqUlVJVumMBcrHW4Nf
iXYS+QKBgAVP/tJo5INN39snrFZltr/ihbdMYBKZ7LdJfYMdUggVdpteOAbtNwyV
5hiy8dA0N5VStwqPBUlOpRNH+LJWuKlLAsYc+z3Apjebn/9egpPG82J2iwLCxjUg
MgrkGgKYoZljkmH4MKKdBI4OBGFij3aazJsYe9HJKHoLcMON3Q46
-----END RSA PRIVATE KEY-----
OK
```

Note: MN316/MN326：不支持>下的数据输入模式，只能在AT命令中直接输入数据。

# 3.4. AT+MSSLCERTRD 读取SSL证书

本命令用于读取SSL证书。

| AT+MSSLCERTRD | |
|---|---|
| 语法 | 响应 |
| 设置命令<br>**AT+MSSLCERTRD=<cert_name>** | 成功<br>*+MSSLCERTRD: <length>,<data>*<br>*OK*<br>错误<br>*+CME ERROR: <err>* |
| 命令描述 | |
| 通过配置的证书名称字符串，读取存储的证书内容，其中包含证书文件的数据长度以及数据内容。[7] | |
| 参数描述 | |
| ***<cert_name>*** 字符串型，证书名称，不超过64字节。 | |
| ***<length>*** 整型，当前读取的证书数据长度。 | |
| ***<data>*** 字符串型，读取的证书内容。 | |
| 示例 | |

读取SSL证书

```
AT+MSSLCERTRD="baidu.cer"
+MSSLCERTRD: 1261,-----BEGIN CERTIFICATE-----
MIIDdTCCAl2gAwIBAgILBAAAAAABFUtaw5QwDQYJKoZIhvcNAQEFBQAwVzELMAkG
A1UEBhMCQkUxGTAXBgNVBAoTEEdsb2JhbFNpZ24gbnYtc2ExEDAOBgNVBAsTB1Jv
b3QgQ0ExGzAZBgNVBAMTEkdsb2JhbFNpZ24gUm9vdCBDQTAeFw05ODA5MDExMjAw
MDBaFw0yODAxMjgxMjAwMDBaMFcxCzAJBgNVBAYTAkJFMRkwFwYDVQQKExBHbG9i
YWxTaWduIG52LXNhMRAwDgYDVQQLEwdSb290IENBMRswGQYDVQQDExJHbG9iYWxT
aWduIFJvb3QgQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDaDuaZ
jc6j40+Kfvvxi4Mla+pIH/EqsLmVEQS98GPR4mdmzxzdzxtIK+6NiY6arymAZavp
xy0Sy6scTHAHoT0KMM0VjU/43dSMUBUc71DuxC73/OlS8pF94G3VNTCOXkNz8kHp
1Wrjsok6Vjk4bwY8iGlbKk3Fp1S4bInMm/k8yuX9ifUSPJJ4ltbcdG6TRGHRjcdG
snUOhugZitVtbNV4FpWi6cgKOOvyJBNPc1STE4U6G7weNLWLBYy5d4ux2x8gkasJ
U26Qzns3dLlwR5EiUWMWea6xrkEmCMgZK9FGqkjWZCrXgzT/LCrBbBlDSgeF59N8
9iFo7+ryUp9/k5DPAgMBAAGjQjBAMA4GA1UdDwEB/wQEAwIBBjAPBgNVHRMBAf8E
BTADAQH/MB0GA1UdDgQWBBRge2YaRQ2XyolQL30EzTSo//z9SzANBgkqhkiG9w0B
AQUFAAOCAQEA1nPnfE920I2/7LqivjTFKDK1fPxsnCwrvQmeU79rXqoRSLblCKOz
yj1hTdNGCbM+w6DjY1Ub8rrvrTnhQ7k4o+YviiY776BQVvnGCv04zcQLcFGUl5gE
38NflNUVyRRBnMRddWQVDf9VMOyGj/8N7yy5Y0b2qvzfvGn9LhJIZJrglfCm7ymP
AbEVtQwdpf5pLGkkeB6zpxxxYu7KyJesF12KwvhHhm4qxFYxldBniYUr+WymXUad
DKqC5JlR3XC321Y9YeRq4VzW9v493kHMB65jUr9TU/Qr6cf9tveCX4XSQRjbgbME
HMUfpIBvFSDJ3gyICh3WZlXi/EjJKSZp4A==
-----END CERTIFICATE-----
OK
```

7. 客户端私钥无法被该命令读取。

# 3.5. AT+MSSLLIST 列出已存在证书及密钥名称

本命令用于列举出模组中保存的证书与密钥名称。

| AT+MSSLLIST | |
|---|---|
| 语法 | 响应 |
| 设置命令<br>**AT+MSSLLIST=<ca_type>** | 成功<br>*[+MSSLLIST: <cert_name>,<len>*<br>*[+MSSLLIST: <cert_name>,<len>*<br>*[.....]]]*<br>*OK*<br>错误<br>*+CME ERROR: <err>* |

**命令描述**

根据配置的证书类型列出模组文件系统中保存的证书及密钥名称，文件系统中存在证书或密钥文件时一次列举证书或密钥名称以及文件数据长度，当不存在任何证书或密钥则直接返回OK。

**参数描述**

***<ca_type>*** 整型，需要查询的证书类型。

***1***

公钥证书

***2***

私钥

***3***

PSK

***<cert_name>*** 字符串型，证书名称，不超过64字节 。

***<len>*** 整型，证书长度。

**示例**

查询存储的公钥证书

```
AT+MSSLLIST=1
+MSSLLIST: "baidu.cer",1261
+MSSLLIST: "test.cer",1824
OK
```

查询存储的私钥

```
AT+MSSLLIST=2
+MSSLLIST: "test.key",1674
OK
```

查询存储的PSK（不存在PSK文件）

**AT+MSSLLIST**

**AT+MSSLLIST=3**

*OK*

中国移动 China Mobile OneMO 120

## 3.6. AT+MSSLRM 删除SSL证书

本命令用于删除模组中存储的SSL证书或密钥。

| AT+MSSLRM | |
|---|---|
| 语法 | 响应 |
| 设置命令<br>**AT+MSSLRM=<cert_name>** | 成功<br>*OK*<br>错误<br>*+CME ERROR: <err>* |
| 命令描述 | |
| 该命令将删除相应证书或密钥，请在无连接使用的情况下进行删除操作，否则可能导致连接失败。 | |
| 参数描述 | |
| ***<cert_name>*** 字符串型，证书或密钥名称，不超过64字节。 | |
| 示例 | |
| 删除SSL证书<br>**AT+MSSLRM="baidu.cer"**<br>*OK* | |

OneMO 1207 China Mobile

# 3.7. AT+MSSLPSK 配置PSK预共享密钥

本命令用于配置PSK预共享密钥操作。

| AT+MSSLPSK | |
|---|---|
| 语法 | 响应 |
| 设置命令<br>**AT+MSSLPSK=<pskid>,<psk>** | 成功<br>*OK*<br>错误<br>*+CME ERROR: <err>* |
| 命令描述 | |
| 配置命令将新增一条PSK记录，已存在的PSK列表通过**AT+MSSLLIST**命令查看；通过**AT+MSSLCFG**命令将PSK与SSL ID进行绑定，供上层应用协议调用。 | |
| 参数描述 | |
| ***<pskid>*** 字符串型，预共享密钥id，不超过64字节。 | |
| ***<psk>*** 字符串型，预共享密钥，单个密钥最多写入8K（8192字节）数据。 | |
| 示例 | |
| 配置PSK预共享密钥<br>**AT+MSSLPSK="123","2345"**<br>*OK* | |

Note: ML302S/ML307S/ML302A/ML305A/ML307A/ML305U/ML305M/ML307G/ML307R暂不支持该命令。

# 3.8. AT+MSSLCHECK 校验证书或密钥正确性

本命令用于校验证书或密钥。

| AT+MSSLCHECK | |
|---|---|
| 语法 | 响应 |
| 测试命令<br>**AT+MSSLCHECK=?** | 成功<br>*+MSSLCHECK: ,(list of support<verify_alg>s)*<br>*OK*<br>错误<br>*+CME ERROR: <err>* |
| 设置命令<br>**AT+MSSLCHECK=<cert_name>[,<verify_alg>]** | 成功<br>*+MSSLCHECK: <check_code>*<br>*OK*<br>错误<br>*+CME ERROR: <err>* |
| 命令描述 | |
| 通过配置需要校验的证书或者密钥名称字符串与校验用加密算法，返回对应的校验码，可通过校验码判断证书或密钥正确性。 | |
| 参数描述 | |
| ***<cert_name>*** 字符串型，证书名称，密钥名称或预共享密钥id。 | |
| ***<verify_alg>*** 整型，校验用加密算法，默认值0。[8]<br>***0***<br>MD5<br>***1***<br>SHA<br>***2***<br>SHA256<br>***3***<br>CRC | |
| ***<check_code>*** 字符串型，证书或密钥对应校验码。 | |
| 示例 | |
| 校验客户端密钥 | |

8. MN316/MN326/ML302S/ML307S/ML302A/ML305A/ML307A/ML307G/ML305U/ML305M/ML307R:只支持 MD5 校验。

### AT+MSSLCHECK

**AT+MSSLCHECK="test.key"**

*+MSSLCHECK: 9e5e120bc7827646a0c4b007ec3e1453*

*OK*

中国移动 China Mobile OneMO 120

## 3.9. AT+MSSLCIPHER 查询密码套件

本命令用于查看模组支持的所有密码套件。

| AT+MSSLCIPHER | |
|---|---|
| 语法 | 响应 |
| 测试命令<br>**AT+MSSLCIPHER=?** | 成功<br>*+MSSLCIPHER: (list of support<cipalgID>s)*<br>*OK*<br>错误<br>*+CME ERROR: <err>* |
| 参数描述 | |
| ***<cipalgID>*** 整型，密码套件支持列表，0x0~0xFFFF，详情见附录。 | |
| 示例 | |
| 测试命令，查询模组支持的密码套件<br>**AT+MSSLCIPHER=?**<br>*+MSSLCIPHER: (0x01,0x16,0x3D)*<br>*OK* | |

Note: ML302S/ML307S暂不支持该命令。

# 4. 示例

本章主要介绍SSL命令在相关业务场景中的使用流程。

## 4.1. 示例

本节主要介绍SSL配置与建立TCP SSL连接相关的操作流程。

### 无身份认证SSL连接建立

```
AT+MSSLCFG="auth",0,0 //配置ssl id0认证方式为无身份验证
OK
AT+MIPCFG="ssl",0,1,0 //配置TCP通道0连接绑定ssl id0并以SSL方式建立连接
OK
AT+MIPOPEN=0,"TCP","www.iottest.work",443,,0 //建立目标连接地址为www.iottest.work的连接
OK
+MIPOPEN: 0,0
```

### 服务器认证SSL连接建立

```
AT+MSSLCFG="auth",1,1 //配置ssl id1认证方式为单向认证
OK
AT+MSSLCERTWR=”test.cer”,0,854 //写入根证书
>(键入根证书)
OK
AT+MSSLCFG="cert",1,"test.cer" //配置ssl id1的根证书为test.cer
OK
AT+MIPCFG="ssl",1,1,1 //配置TCP通道1连接绑定ssl id1并以SSL方式建立连接
OK
AT+MIPOPEN=1,"TCP","www.iottest.work",443,,0 //建立目标连接地址为www.iottest.work的连接
OK
+MIPOPEN: 1,0
```

### 服务器和客户端双向认证SSL连接建立

```
AT+MSSLCFG=”auth”,2,2 //配置ssl id2认证方式为双向认证
OK
AT+MSSLCERTWR=”test.cer”,0,854 //写入根证书
>(键入根证书)
OK
AT+MSSLCERTWR=”test.clientcer”,0,854 //写入客户端证书
>(键入客户端证书)
OK
AT+MSSLKEYWR=”test.key”,0,886 //写入客户端密钥
>(键入客户端密钥)
OK
AT+MSSLCFG="cert",2,"test.cer","test.clientcer","test.key"
//配置ssl id2的根证书、客户端证书与客户端密钥。
```

OneMO_1207

*OK*

**AT+MIPCFG="ssl",2,1,2** *//配置TCP通道2连接绑定ssl id2并以SSL方式建立连接*

*OK*

**AT+MIPOPEN=2,"TCP","www.iottest.work",443,,0** *//建立目标连接地址为www.iottest.work的连接*

*OK*

*+MIPOPEN: 2,0*

中国移动 China Mobile OneMO 120

# 5. 附录

本章主要介绍SSL命令在相关业务场景中的使用流程。

## 5.1. 密码套件算法

本节描述了支持的加密套件算法列表，各型号实际支持套件以AT+MSSLCIPHER=?指令查询结果为准。

| <cipalgID> | 加密套件算法 |
|---|---|
| 0x01 | TLS_RSA_WITH_NULL_MD5 |
| 0x02 | TLS_RSA_WITH_NULL_SHA |
| 0x04 | TLS_RSA_WITH_RC4_128_MD5 |
| 0x05 | TLS_RSA_WITH_RC4_128_SHA |
| 0x09 | TLS_RSA_WITH_DES_CBC_SHA |
| 0x0A | TLS_RSA_WITH_3DES_EDE_CBC_SHA |
| 0x15 | TLS_DHE_RSA_WITH_DES_CBC_SHA |
| 0x16 | TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA |
| 0x2C | TLS_PSK_WITH_NULL_SHA |
| 0x2D | TLS_DHE_PSK_WITH_NULL_SHA |
| 0x2E | TLS_RSA_PSK_WITH_NULL_SHA |
| 0x2F | TLS_RSA_WITH_AES_128_CBC_SHA |
| 0x33 | TLS_DHE_RSA_WITH_AES_128_CBC_SHA |
| 0x35 | TLS_RSA_WITH_AES_256_CBC_SHA |
| 0x39 | TLS_DHE_RSA_WITH_AES_256_CBC_SHA |
| 0x3B | TLS_RSA_WITH_NULL_SHA256 |
| 0x3C | TLS_RSA_WITH_AES_128_CBC_SHA256 |
| 0x3D | TLS_RSA_WITH_AES_256_CBC_SHA256 |
| 0x41 | TLS_RSA_WITH_CAMELLIA_128_CBC_SHA |
| 0x45 | TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA |
| 0x67 | TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 |
| 0x6B | TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 |

| <cipalgID> | 加密套件算法 |
| --- | --- |
| 0x84 | TLS_RSA_WITH_CAMELLIA_256_CBC_SHA |
| 0x88 | TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA |
| 0x8A | TLS_PSK_WITH_RC4_128_SHA |
| 0x8B | TLS_PSK_WITH_3DES_EDE_CBC_SHA |
| 0x8C | TLS_PSK_WITH_AES_128_CBC_SHA |
| 0x8D | TLS_PSK_WITH_AES_256_CBC_SHA |
| 0x8E | TLS_DHE_PSK_WITH_RC4_128_SHA |
| 0x8F | TLS_DHE_PSK_WITH_3DES_EDE_CBC_SHA |
| 0x90 | TLS_DHE_PSK_WITH_AES_128_CBC_SHA |
| 0x91 | TLS_DHE_PSK_WITH_AES_256_CBC_SHA |
| 0x92 | TLS_RSA_PSK_WITH_RC4_128_SHA |
| 0x93 | TLS_RSA_PSK_WITH_3DES_EDE_CBC_SHA |
| 0x94 | TLS_RSA_PSK_WITH_AES_128_CBC_SHA |
| 0x95 | TLS_RSA_PSK_WITH_AES_256_CBC_SHA |
| 0x9C | TLS_RSA_WITH_AES_128_GCM_SHA256 |
| 0x9D | TLS_RSA_WITH_AES_256_GCM_SHA384 |
| 0x9E | TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 |
| 0x9F | TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 |
| 0xA8 | TLS_PSK_WITH_AES_128_GCM_SHA256 |
| 0xA9 | TLS_PSK_WITH_AES_256_GCM_SHA384 |
| 0xAA | TLS_DHE_PSK_WITH_AES_128_GCM_SHA256 |
| 0xAB | TLS_DHE_PSK_WITH_AES_256_GCM_SHA384 |
| 0xAC | TLS_RSA_PSK_WITH_AES_128_GCM_SHA256 |
| 0xAD | TLS_RSA_PSK_WITH_AES_256_GCM_SHA384 |
| 0xAE | TLS_PSK_WITH_AES_128_CBC_SHA256 |
| 0xAF | TLS_PSK_WITH_AES_256_CBC_SHA384 |
| 0xB0 | TLS_PSK_WITH_NULL_SHA256 |
| 0xB1 | TLS_PSK_WITH_NULL_SHA384 |
| 0xB2 | TLS_DHE_PSK_WITH_AES_128_CBC_SHA256 |

| <cipalgID> | 加密套件算法 |
| --- | --- |
| 0xB3 | TLS_DHE_PSK_WITH_AES_256_CBC_SHA384 |
| 0xB4 | TLS_DHE_PSK_WITH_NULL_SHA256 |
| 0xB5 | TLS_DHE_PSK_WITH_NULL_SHA384 |
| 0xB6 | TLS_RSA_PSK_WITH_AES_128_CBC_SHA256 |
| 0xB7 | TLS_RSA_PSK_WITH_AES_256_CBC_SHA384 |
| 0xB8 | TLS_RSA_PSK_WITH_NULL_SHA256 |
| 0xB9 | TLS_RSA_PSK_WITH_NULL_SHA384 |
| 0xBA | TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256 |
| 0xBE | TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 |
| 0xC0 | TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256 |
| 0xC4 | TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256 |
| 0xC001 | TLS_ECDH_ECDSA_WITH_NULL_SHA |
| 0xC002 | TLS_ECDH_ECDSA_WITH_RC4_128_SHA |
| 0xC003 | TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA |
| 0xC004 | TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA |
| 0xC005 | TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA |
| 0xC006 | TLS_ECDHE_ECDSA_WITH_NULL_SHA |
| 0xC007 | TLS_ECDHE_ECDSA_WITH_RC4_128_SHA |
| 0xC008 | TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA |
| 0xC009 | TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA |
| 0xC00A | TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA |
| 0xC00B | TLS_ECDH_RSA_WITH_NULL_SHA |
| 0xC00C | TLS_ECDH_RSA_WITH_RC4_128_SHA |
| 0xC00D | TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA |
| 0xC00E | TLS_ECDH_RSA_WITH_AES_128_CBC_SHA |
| 0xC00F | TLS_ECDH_RSA_WITH_AES_256_CBC_SHA |
| 0xC010 | TLS_ECDHE_RSA_WITH_NULL_SHA |
| 0xC011 | TLS_ECDHE_RSA_WITH_RC4_128_SHA |
| 0xC012 | TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA |

| <cipalgID> | 加密套件算法 |
| --- | --- |
| 0xC013 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA |
| 0xC014 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA |
| 0xC023 | TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 |
| 0xC024 | TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 |
| 0xC025 | TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 |
| 0xC026 | TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 |
| 0xC027 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 |
| 0xC028 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 |
| 0xC029 | TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 |
| 0xC02A | TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 |
| 0xC02B | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 |
| 0xC02C | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 |
| 0xC02D | TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 |
| 0xC02E | TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 |
| 0xC02F | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 |
| 0xC030 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 |
| 0xC031 | TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 |
| 0xC032 | TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 |
| 0xC033 | TLS_ECDHE_PSK_WITH_RC4_128_SHA |
| 0xC034 | TLS_ECDHE_PSK_WITH_3DES_EDE_CBC_SHA |
| 0xC035 | TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA |
| 0xC036 | TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA |
| 0xC037 | TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256 |
| 0xC038 | TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384 |
| 0xC039 | TLS_ECDHE_PSK_WITH_NULL_SHA |
| 0xC03A | TLS_ECDHE_PSK_WITH_NULL_SHA256 |
| 0xC03B | TLS_ECDHE_PSK_WITH_NULL_SHA384 |
| 0xC03C | TLS_RSA_WITH_ARIA_128_CBC_SHA256 |
| 0xC03D | TLS_RSA_WITH_ARIA_256_CBC_SHA384 |

| <cipalgID> | 加密套件算法 |
| --- | --- |
| 0xC044 | TLS_DHE_RSA_WITH_ARIA_128_CBC_SHA256 |
| 0xC045 | TLS_DHE_RSA_WITH_ARIA_256_CBC_SHA384 |
| 0xC048 | TLS_ECDHE_ECDSA_WITH_ARIA_128_CBC_SHA256 |
| 0xC049 | TLS_ECDHE_ECDSA_WITH_ARIA_256_CBC_SHA384 |
| 0xC04A | TLS_ECDH_ECDSA_WITH_ARIA_128_CBC_SHA256 |
| 0xC04B | TLS_ECDH_ECDSA_WITH_ARIA_256_CBC_SHA384 |
| 0xC04C | TLS_ECDHE_RSA_WITH_ARIA_128_CBC_SHA256 |
| 0xC04D | TLS_ECDHE_RSA_WITH_ARIA_256_CBC_SHA384 |
| 0xC04E | TLS_ECDH_RSA_WITH_ARIA_128_CBC_SHA256 |
| 0xC04F | TLS_ECDH_RSA_WITH_ARIA_256_CBC_SHA384 |
| 0xC050 | TLS_RSA_WITH_ARIA_128_GCM_SHA256 |
| 0xC051 | TLS_RSA_WITH_ARIA_256_GCM_SHA384 |
| 0xC052 | TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256 |
| 0xC053 | TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384 |
| 0xC05C | TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256 |
| 0xC05D | TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384 |
| 0xC05E | TLS_ECDH_ECDSA_WITH_ARIA_128_GCM_SHA256 |
| 0xC05F | TLS_ECDH_ECDSA_WITH_ARIA_256_GCM_SHA384 |
| 0xC060 | TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256 |
| 0xC061 | TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384 |
| 0xC062 | TLS_ECDH_RSA_WITH_ARIA_128_GCM_SHA256 |
| 0xC063 | TLS_ECDH_RSA_WITH_ARIA_256_GCM_SHA384 |
| 0xC064 | TLS_PSK_WITH_ARIA_128_CBC_SHA256 |
| 0xC065 | TLS_PSK_WITH_ARIA_256_CBC_SHA384 |
| 0xC066 | TLS_DHE_PSK_WITH_ARIA_128_CBC_SHA256 |
| 0xC067 | TLS_DHE_PSK_WITH_ARIA_256_CBC_SHA384 |
| 0xC068 | TLS_RSA_PSK_WITH_ARIA_128_CBC_SHA256 |
| 0xC069 | TLS_RSA_PSK_WITH_ARIA_256_CBC_SHA384 |
| 0xC06A | TLS_PSK_WITH_ARIA_128_GCM_SHA256 |

| <cipalgID> | 加密套件算法 |
| --- | --- |
| 0xC06B | TLS_PSK_WITH_ARIA_256_GCM_SHA384 |
| 0xC06C | TLS_DHE_PSK_WITH_ARIA_128_GCM_SHA256 |
| 0xC06D | TLS_DHE_PSK_WITH_ARIA_256_GCM_SHA384 |
| 0xC06E | TLS_RSA_PSK_WITH_ARIA_128_GCM_SHA256 |
| 0xC06F | TLS_RSA_PSK_WITH_ARIA_256_GCM_SHA384 |
| 0xC070 | TLS_ECDHE_PSK_WITH_ARIA_128_CBC_SHA256 |
| 0xC071 | TLS_ECDHE_PSK_WITH_ARIA_256_CBC_SHA384 |
| 0xC072 | TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256 |
| 0xC073 | TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384 |
| 0xC074 | TLS_ECDH_ECDSA_WITH_CAMELLIA_128_CBC_SHA256 |
| 0xC075 | TLS_ECDH_ECDSA_WITH_CAMELLIA_256_CBC_SHA384 |
| 0xC076 | TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 |
| 0xC077 | TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384 |
| 0xC078 | TLS_ECDH_RSA_WITH_CAMELLIA_128_CBC_SHA256 |
| 0xC079 | TLS_ECDH_RSA_WITH_CAMELLIA_256_CBC_SHA384 |
| 0xC07A | TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256 |
| 0xC07B | TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384 |
| 0xC07C | TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256 |
| 0xC07D | TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384 |
| 0xC086 | TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256 |
| 0xC087 | TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384 |
| 0xC088 | TLS_ECDH_ECDSA_WITH_CAMELLIA_128_GCM_SHA256 |
| 0xC089 | TLS_ECDH_ECDSA_WITH_CAMELLIA_256_GCM_SHA384 |
| 0xC08A | TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256 |
| 0xC08B | TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384 |
| 0xC08C | TLS_ECDH_RSA_WITH_CAMELLIA_128_GCM_SHA256 |
| 0xC08D | TLS_ECDH_RSA_WITH_CAMELLIA_256_GCM_SHA384 |
| 0xC08E | TLS_PSK_WITH_CAMELLIA_128_GCM_SHA256 |
| 0xC08F | TLS_PSK_WITH_CAMELLIA_256_GCM_SHA384 |

| <cipalgID> | 加密套件算法 |
| --- | --- |
| 0xC090 | TLS_DHE_PSK_WITH_CAMELLIA_128_GCM_SHA256 |
| 0xC091 | TLS_DHE_PSK_WITH_CAMELLIA_256_GCM_SHA384 |
| 0xC092 | TLS_RSA_PSK_WITH_CAMELLIA_128_GCM_SHA256 |
| 0xC093 | TLS_RSA_PSK_WITH_CAMELLIA_256_GCM_SHA384 |
| 0xC094 | TLS_PSK_WITH_CAMELLIA_128_CBC_SHA256 |
| 0xC095 | TLS_PSK_WITH_CAMELLIA_256_CBC_SHA384 |
| 0xC096 | TLS_DHE_PSK_WITH_CAMELLIA_128_CBC_SHA256 |
| 0xC097 | TLS_DHE_PSK_WITH_CAMELLIA_256_CBC_SHA384 |
| 0xC098 | TLS_RSA_PSK_WITH_CAMELLIA_128_CBC_SHA256 |
| 0xC099 | TLS_RSA_PSK_WITH_CAMELLIA_256_CBC_SHA384 |
| 0xC09A | TLS_ECDHE_PSK_WITH_CAMELLIA_128_CBC_SHA256 |
| 0xC09B | TLS_ECDHE_PSK_WITH_CAMELLIA_256_CBC_SHA384 |
| 0xC09C | TLS_RSA_WITH_AES_128_CCM |
| 0xC09D | TLS_RSA_WITH_AES_256_CCM |
| 0xC09E | TLS_DHE_RSA_WITH_AES_128_CCM |
| 0xC09F | TLS_DHE_RSA_WITH_AES_256_CCM |
| 0xC0A0 | TLS_RSA_WITH_AES_128_CCM_8 |
| 0xC0A1 | TLS_RSA_WITH_AES_256_CCM_8 |
| 0xC0A2 | TLS_DHE_RSA_WITH_AES_128_CCM_8 |
| 0xC0A3 | TLS_DHE_RSA_WITH_AES_256_CCM_8 |
| 0xC0A4 | TLS_PSK_WITH_AES_128_CCM |
| 0xC0A5 | TLS_PSK_WITH_AES_256_CCM |
| 0xC0A6 | TLS_DHE_PSK_WITH_AES_128_CCM |
| 0xC0A7 | TLS_DHE_PSK_WITH_AES_256_CCM |
| 0xC0A8 | TLS_PSK_WITH_AES_128_CCM_8 |
| 0xC0A9 | TLS_PSK_WITH_AES_256_CCM_8 |
| 0xC0AA | TLS_DHE_PSK_WITH_AES_128_CCM_8 |
| 0xC0AB | TLS_DHE_PSK_WITH_AES_256_CCM_8 |
| 0xC0AC | TLS_ECDHE_ECDSA_WITH_AES_128_CCM |

| <cipalgID> | 加密套件算法 |
| --- | --- |
| 0xC0AD | TLS_ECDHE_ECDSA_WITH_AES_256_CCM |
| 0xC0AE | TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 |
| 0xC0AF | TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8 |
| 0xC0FF | TLS_ECJPAKE_WITH_AES_128_CCM_8 |
| 0xCCA8 | TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 |
| 0xCCA9 | TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 |
| 0xCCAA | TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 |
| 0xCCAB | TLS_PSK_WITH_CHACHA20_POLY1305_SHA256 |
| 0xCCAC | TLS_ECDHE_PSK_WITH_CHACHA20_POLY1305_SHA256 |
| 0xCCAD | TLS_DHE_PSK_WITH_CHACHA20_POLY1305_SHA256 |
| 0xCCAE | TLS_RSA_PSK_WITH_CHACHA20_POLY1305_SHA256 |

中国移动 China Mobile OneMO 1207

## 5.2. 错误码

本章为SSL命令相关的错误码。

| 错误码 | 说明 |
| --- | --- |
| 50 | 参数错误 |
| 750 | SSL/TLS/DTLS 未知错误 |
| 751 | SSL/TLS/DTLS 初始化资源错误 |
| 752 | SSL/TLS/DTLS 服务器证书验证失败 |
| 753 | SSL/TLS/DTLS 协商超时 |
| 754 | SSL/TLS/DTLS 协商失败 |
| 760 | CERTS/KEYS 未知错误 |
| 761 | CERTS/KEYS 无效（格式/内容错误） |
| 762 | CERTS/KEYS 不存在 |
| 763 | CERTS/KEYS 已存在同名的证书或密钥 |
| 764 | CERTS/KEYS 写入错误 |
| 765 | CERTS/KEYS 其他证书/密钥正在写入中 |
| 766 | CERTS/KEYS 读取错误 |
| 767 | CERTS/KEYS 删除错误 |
| 768 | CERTS/KEYS 过大 |
| 769 | CERTS/KEYS 加载失败 |

OneMO 120 移动 China Mobile