

# LTE Standard(A)系列

# SSL 应用指导

**LTE Standard 模块系列**

版本：1.2

日期：2022-08-05

状态：受控文件



上海移远通信技术股份有限公司（以下简称“移远通信”）始终以为客户提供最及时、最全面的服务为宗旨。如需任何帮助，请随时联系我司上海总部，联系方式如下：

上海移远通信技术股份有限公司  
上海市闵行区田林路 1016 号科技绿洲 3 期（B 区）5 号楼 邮编：200233  
电话：+86 21 5108 6236 邮箱：[info@quectel.com](mailto:info@quectel.com)

或联系我司当地办事处，详情请登录：<http://www.quectel.com/cn/support/sales.htm>。

如需技术支持或反馈我司技术文档中的问题，请随时登陆网址：  
<http://www.quectel.com/cn/support/technical.htm> 或发送邮件至：[support@quectel.com](mailto:support@quectel.com)。

## 前言

移远通信提供该文档内容以支持客户的产品设计。客户须按照文档中提供的规范、参数来设计产品。同时，您理解并同意，移远通信提供的参考设计仅作为示例。您同意在设计您目标产品时使用您独立的分析、评估和判断。在使用本文档所指导的任何硬软件或服务之前，请仔细阅读本声明。您在此承认并同意，尽管移远通信采取了商业范围内的合理努力来提供尽可能好的体验，但本文档和其所涉及服务是在“可用”基础上提供给您的。移远通信可在未事先通知的情况下，自行决定随时增加、修改或重述本文档。

## 使用和披露限制

### 许可协议

除非移远通信特别授权，否则我司所提供硬软件、材料和文档的接收方须对接收的内容保密，不得将其用于除本项目的实施与开展以外的任何其他目的。

### 版权声明

移远通信产品和本协议项下的第三方产品可能包含受移远通信或第三方材料、硬软件和文档版权保护的相关资料。除非事先得到书面同意，否则您不得获取、使用、向第三方披露我司所提供的文档和信息，或对此类受版权保护的资料进行复制、转载、抄袭、出版、展示、翻译、分发、合并、修改，或创造其衍生作品。移远通信或第三方对受版权保护的资料拥有专有权，不授予或转让任何专利、版权、商标或服务商标权的许可。为避免歧义，除了正常的非独家、免版税的产品使用许可，任何形式的购买都不可被视为授予许可。对于任何违反保密义务、未经授权使用或以其他非法形式恶意使用所述文档和信息的违法侵权行为，移远通信有权追究法律责任。

### 商标

除另行规定，本文档中的任何内容均不授予在广告、宣传或其他方面使用移远通信或第三方的任何商标、商号及名称，或其缩略语，或其仿冒品的权利。

### 第三方权利

您理解本文档可能涉及一个或多个属于第三方的硬软件和文档（“第三方材料”）。您对此类第三方材料的使用应受本文档的所有限制和义务约束。

移远通信针对第三方材料不做任何明示或暗示的保证或陈述，包括但不限于任何暗示或法定的适销性或特定用途的适用性、平静受益权、系统集成、信息准确性以及与许可技术或被许可人使用许可技术相关的不侵犯任何第三方知识产权的保证。本协议中的任何内容都不构成移远通信对任何移远通信产品或任何其他软硬件、设备、工具、信息或产品的开发、增强、修改、分销、营销、销售、提供销售或以其他方式维持生产的陈述或保证。此外，移远通信免除因交易过程、使用或贸易而产生的任何和所有保证。

## 隐私声明

为实现移远通信产品功能，特定设备数据将会上传至移远通信或第三方服务器（包括运营商、芯片供应商或您指定的服务器）。移远通信严格遵守相关法律法规，仅为实现产品功能之目的或在适用法律允许的情况下保留、使用、披露或以其他方式处理相关数据。当您与第三方进行数据交互前，请自行了解其隐私保护和数据安全政策。

## 免责声明

- 1) 移远通信不承担任何因未能遵守有关操作或设计规范而造成损害的责任。
- 2) 移远通信不承担因本文档中的任何因不准确、遗漏、或使用本文档中的信息而产生的任何责任。
- 3) 移远通信尽力确保开发中功能的完整性、准确性、及时性，但不排除上述功能错误或遗漏的可能。除非另有协议规定，否则移远通信对开发中功能的使用不做任何暗示或法定的保证。在适用法律允许的最大范围内，移远通信不对任何因使用开发中功能而遭受的损害承担责任，无论此类损害是否可以预见。
- 4) 移远通信对第三方网站及第三方资源的信息、内容、广告、商业报价、产品、服务和材料的可访问性、安全性、准确性、可用性、合法性和完整性不承担任何法律责任。

版权所有 ©上海移远通信技术股份有限公司 2022，保留一切权利。

**Copyright © Quectel Wireless Solutions Co., Ltd. 2022.**

# 文档历史

## 修订记录

| 版本  | 日期         | 作者                      | 变更表述   |
|-----|------------|-------------------------|--|
| -   | 2020-08-31 | Luffy LIU               | 文档创建   |
| 1.0 | 2021-04-16 | Luffy LIU               | 受控版本   |
| 1.1 | 2022-03-02 | Luffy LIU/<br>Larson LI | 1. 增加文档适用模块 EC200A 系列、EC800N-CN 和 EG915N-EU。<br>2. 删除 EG912Y-CN 模块。                    |
| 1.2 | 2022-08-05 | Luffy LIU/<br>Larson LI | 1. 新增适用模块 EC200M-CN、EC600M-CN、EC800M-CN、EG915N-LA 和 EG912N-EN。<br>2. 删除适用模块 EC200T 系列。 |

# 目录

|  |           |
|--|-----------|
| 文档历史 .....                                     | 3         |
| 目录 .....                                       | 4         |
| 表格索引 .....                                     | 6         |
| <b>1 引言 .....</b>                              | <b>7</b>  |
| 1.1. 适用模块 .....                                | 7         |
| 1.2. SSL 版本和加密套件 .....                         | 8         |
| 1.3. SSL 功能使用流程 .....                          | 10        |
| 1.4. 数据访问模式说明 .....                            | 10        |
| 1.5. 证书有效性验证 .....                             | 11        |
| 1.6. 服务器名称指示 .....                             | 11        |
| <b>2 SSL AT 命令详解 .....</b>                     | <b>12</b> |
| 2.1. AT 命令说明 .....                             | 12        |
| 2.1.1. 定义 .....                                | 12        |
| 2.1.2. AT 命令语句 .....                           | 12        |
| 2.1.3. AT 示例声明 .....                           | 13        |
| 2.2. SSL 相关 AT 命令描述 .....                      | 13        |
| 2.2.1. AT+QSSLCFG 配置 SSL 上下文的参数 .....          | 13        |
| 2.2.2. AT+QSSLOPEN 打开 SSL Socket 连接远程服务器 ..... | 19        |
| 2.2.3. AT+QSSLSEND 通过 SSL 连接发送数据 .....         | 21        |
| 2.2.4. AT+QSSLRECV 通过 SSL 连接接收数据 .....         | 22        |
| 2.2.5. AT+QSSLCLOSE 关闭 SSL 连接 .....            | 23        |
| 2.2.6. AT+QSSLSTATE 查询 Socket 连接状态 .....       | 23        |
| 2.3. URC 详解 .....                              | 25        |
| 2.3.1. +QSSLURC: "recv" 通知主机接收数据 .....         | 25        |
| 2.3.2. +QSSLURC: "closed" 通知异常断开连接 .....       | 25        |
| <b>3 举例 .....</b>                              | <b>26</b> |
| 3.1. 配置并激活 PDP 上下文 .....                       | 26        |
| 3.1.1. 配置 PDP 上下文 .....                        | 26        |
| 3.1.2. 激活 PDP 上下文 .....                        | 26        |
| 3.1.3. 去激活 PDP 上下文 .....                       | 26        |
| 3.2. 配置 SSL 上下文 .....                          | 26        |
| 3.3. SSL 客户端在缓存模式下工作 .....                     | 27        |
| 3.3.1. 建立 SSL 连接并进入缓存模式 .....                  | 27        |
| 3.3.2. 缓存模式下发送数据 .....                         | 27        |
| 3.3.2.1. 发送不定长数据 .....                         | 27        |
| 3.3.2.2. 发送定长数据 .....                          | 27        |
| 3.3.3. 缓存模式下接收数据 .....                         | 27        |
| 3.3.4. 关闭 SSL 连接 .....                         | 28        |
| 3.4. SSL 客户端在直吐模式下工作 .....                     | 28        |
| 3.4.1. 建立 SSL 连接并进入直吐模式 .....                  | 28        |

|        |                            |    |
|--------|----------------------------|----|
| 3.4.2. | 直吐模式下发送数据 .....            | 28 |
| 3.4.3. | 直吐模式下接收数据 .....            | 29 |
| 3.4.4. | 关闭 SSL 连接 .....            | 29 |
| 3.5.   | SSL 客户端在透传模式下工作 .....      | 29 |
| 3.5.1. | 建立 SSL 连接并在透传模式下发送数据 ..... | 29 |
| 3.5.2. | 建立 SSL 连接并在透传模式下接收数据 ..... | 29 |
| 3.5.3. | 关闭 SSL 连接 .....            | 29 |
| 4      | SSL 连接失败原因的排查 .....        | 30 |
| 5      | 结果码 .....                  | 31 |
| 6      | 附录 参考文档及术语缩写 .....         | 33 |

表格索引

表 1: 适用模块 ..... 7

表 2: SSL 版本 ..... 8

表 3: 支持的 SSL 加密套件 ..... 8

表 4: AT 命令类型 ..... 12

表 5: 结果码 ..... 31

表 6: 参考文档 ..... 33

表 7: 术语缩写 ..... 33

# 1 引言

本文档介绍如何使用移远通信 LTE Standard(A)系列模块的 SSL 功能。

SSL (Secure Sockets Layer, 安全套接层) 是为网络通信提供安全及数据完整性的一种安全协议。

为确保通信的私密性, 在某些情况下, 服务器和客户端之间的通信应采用加密方式, 以防止在通信过程中数据被窃听、篡改或伪造。SSL 功能可以满足上述要求。

## 1.1. 适用模块

表 1: 适用模块

| 模块系列            | 模块        |
|-----------------|-----------|
| LTE Standard(A) | EC200A 系列 |
|                 | EC200M-CN |
|                 | EC200N-CN |
|                 | EC200S 系列 |
|                 | EC600M-CN |
|                 | EC600N-CN |
|                 | EC600S-CN |
|                 | EC800M-CN |
|                 | EC800N-CN |
|                 | EG912N-EN |
|                 | EG912Y-EU |
|                 | EG915N 系列 |



## 1.2. SSL 版本和加密套件

下表为移远通信 LTE Standard(A)系列模块支持的 SSL 版本。

表 2: SSL 版本

| SSL 版本  |
|---------|
| SSL 3.0 |
| TLS 1.2 |
| TLS 1.1 |
| TLS 1.0 |

下表为移远通信 LTE Standard(A)系列模块支持的 SSL 加密套件。默认支持所有加密套件。有关加密套件的详细说明，请参考 *RFC 2246-The TLS Protocol Version 1.0*。

表 3: 支持的 SSL 加密套件

| 加密套件代码 | 加密套件名称                                |
|--------|---------------------------------------|
| 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       |
| 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   |
| 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          |
| 0XC011 | TLS_ECDHE_RSA_WITH_RC4_128_SHA                |
| 0XC012 | TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA           |
| 0XC013 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA            |
| 0XC014 | TLS_ECDHE_RSA_WITH_AES_256_CBC_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             |
| 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          |
| 0XC02F | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256         |
| 0XC030 | MBEDTLS_TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 |
| 0XFFFF | 支持以上所有加密套件                                    |

### 1.3. SSL 功能使用流程

**步骤 1:** 通过 **AT+QICSGP** 配置 PDP 上下文的<APN>、<username>、<password>和其他参数。详细信息请参考文档 [1]。

**步骤 2:** 通过 **AT+QIACT** 激活 PDP 上下文。成功激活上下文后，可通过 **AT+QIACT?**查询分配的 IP 地址。详细信息请参考文档 [1]。

**步骤 3:** 通过 **AT+QSSLCFG** 配置指定 SSL 上下文的 SSL 版本、加密套件、受信任 CA 证书路径及身份验证模式。

**步骤 4:** 通过 **AT+QSSLOPEN** 打开 SSL socket 连接远程服务器。

**步骤 5:** SSL 连接成功建立后，将通过该连接收发数据。每个模式下数据收发的详情请参考第 1.4 章。

**步骤 6:** 通过 **AT+QSSLCLOSE** 关闭 SSL 连接。

**步骤 7:** 通过 **AT+QIDEACT** 去激活 PDP 上下文。详细信息请参考文档 [1]。

### 1.4. 数据访问模式说明

SSL 连接支持以下 3 种数据访问模式：

- 缓存模式
- 直吐模式
- 透传模式

当使用 **AT+QSSLOPEN** 打开 SSL 连接时，可以通过<access\_mode>来指定数据访问模式；SSL 连接成功创建后，可以通过 **AT+QISWTMD** 切换数据访问模式。关于 **AT+QISWTMD** 的详细信息，可参考文档 [1]。

1. 缓存模式下，可以通过 **AT+QSSLSEND** 发送数据。从网络接收数据时，模块将上报 URC：**+QSSLURC: "recv",<clientID>**，之后用户可以通过 **AT+QSSLRECV** 来读取缓存数据。
2. 直吐模式下，可以通过 **AT+QSSLSEND** 发送数据。从网络接收数据时，数据会以如下格式直接输出到 UART/ USB modem/ USB AT 口：**+QSSLURC: "recv",<clientID>,<currentrecvlength><CR><LF><data>**。
3. 透传模式下，相应端口会进入独占模式，从网络接收到的数据会从 COM 口直接输出。**+++**或者 **DTR**（需先执行 **AT&D1**）可用于退出透传模式。若服务器异常断开 SSL 连接，将上报结果码 **NO CARRIER**。关于 **AT&D** 的详细信息，可参考文档 [3]。

## ● 退出透传模式

用户可以通过+++或者 DTR（需先执行 AT&D1）两种方式退出透传模式，为了防止+++被当成数据发送，实际操作过程中必须注意以下几点：

- 1) +++输入前 1 秒或更长时间内不能输入其它任何数据；
- 2) 必须在 1 秒内输入+++，并且不能输入其它任何数据；
- 3) +++输入后 1 秒内不能输入其它任何数据；
- 4) 通过+++或者 DTR（需先执行 AT&D1）方式使模块退出透传模式，直到模块返回 OK。

## ● 切换到透传模式

- 1) 通过执行 AT+QISWTMD: 执行命令时，指定<access\_mode>为 2，返回 CONNECT，表示成功切换到透传模式。
- 2) 通过执行 ATO: 退出透传模式后，可通过 ATO 再切换回至透传模式；若返回 CONNECT，则表示成功切换至透传模式。若连接访问模式前模块未进入过透传模式，执行 ATO 则会返回 NO CARRIER。关于 ATO 的详细信息，可参考文档 [3]。

## 1.5. 证书有效性验证

检查证书是否在有效期内，必须对证书进行解析，并将本地时间与证书的“不早于”时间和“不晚于”时间相比较。如果本地时间早于“不早于”的时间或晚于“不晚于”的时间，则证书将被视为已过期。

若需要进行证书有效性验证（通过 AT+QSSLCFG 设置<ignore\_ltime>=0），为避免验证失败，应使用 AT+CCLK 将模块本地时间配置在证书有效期内。关于 AT+CCLK 的详细信息，可参考文档 [3]。

## 1.6. 服务器名称指示

客户端期望 SNI（服务器名称指示）提供服务器主机名称信息，以增强与基于单个 IP 地址的多个虚拟服务器的安全连接。该功能仅适用于 TLS 协议。

## 2 SSL AT 命令详解

### 2.1. AT 命令说明

#### 2.1.1. 定义

- **<CR>** 回车符。
- **<LF>** 换行符。
- **<...>** 参数名称。实际命令中不包含尖括号。
- **[...]** 可选参数或 TA 信息响应的可选部分。实际命令中不包含方括号。若无特别说明，配置命令中的可选参数被省略时，将默认使用其之前已设置的值或其默认值。
- 下划线 参数的默认设置。

#### 2.1.2. AT 命令语句

前缀 **AT** 或 **at** 必须加在每个命令行的开头。输入**<CR>**将终止命令行。通常，命令后面跟随形式为**<CR><LF><response><CR><LF>**的响应。在本文档中表现命令和响应的表格中，省略了**<CR><LF>**，仅显示命令和响应。

表 4: AT 命令类型

| AT 命令类型 | 语句  | 描述                               |
|---------|---|----------------------------------|
| 测试命令    | <b>AT+&lt;cmd&gt;=?</b>   | 测试是否存在相应的命令，并返回有关其参数的类型、值或范围的信息。 |
| 查询命令    | <b>AT+&lt;cmd&gt;?</b>  | 查询相应命令的当前参数值。                    |
| 设置命令    | <b>AT+&lt;cmd&gt;=&lt;p1&gt;[,&lt;p2&gt;[,&lt;p3&gt;[...]]]</b> | 设置用户可定义的参数值。                     |
| 执行命令    | <b>AT+&lt;cmd&gt;</b>   | 返回特定的参数信息或执行特定的操作。               |

### 2.1.3. AT 示例声明

本文中的示例仅为方便用户了解 AT 命令的使用方法，不构成移远通信对终端流程设计的建议或意见，也不代表模块应被设置成相应示例中的状态。某些 AT 命令存在多个示例，这些示例之间不存在承接关系或连续性。

## 2.2. SSL 相关 AT 命令描述

### 2.2.1. AT+QSSLCFG 配置 SSL 上下文的参数

该命令用于配置 SSL 上下文的 SSL 版本、加密套件、受信任 CA 证书路径、身份验证模式、客户端证书和客户端密钥路径等 SSL 配置。这些参数将在握手过程中使用。

<SSL\_ctxID>是 SSL 上下文的索引。模块最多支持 6 个 SSL 上下文。可以基于一个 SSL 上下文建立多个 SSL 连接。SSL 版本和加密套件的设置存储在 SSL 上下文中，并将应用于与该 SSL 上下文关联的新 SSL 连接。

#### AT+QSSLCFG 配置 SSL 上下文的参数

测试命令

AT+QSSLCFG=?

响应

+QSSLCFG: "sslversion", (支持的<SSL\_ctxID>范围), (支持的<SSL\_version>范围)  
 +QSSLCFG: "ciphersuite", (支持的<SSL\_ctxID>范围), (支持的<cipher\_suites>列表)  
 +QSSLCFG: "cacert", (支持的<SSL\_ctxID>范围), <cacertpath>  
 +QSSLCFG: "cacertex", (支持的<SSL\_ctxID>范围), <cacertpath>  
 +QSSLCFG: "clientcert", (支持的<SSL\_ctxID>范围), <client\_cert\_path>  
 +QSSLCFG: "clientkey", (支持的<SSL\_ctxID>范围), <client\_key\_path>  
 +QSSLCFG: "seclevel", (支持的<SSL\_ctxID>范围), (支持的<seclevel>范围)  
 +QSSLCFG: "ignorelocaltime", (支持的<SSL\_ctxID>范围), (支持的<ignore\_ltime>列表)  
 +QSSLCFG: "negotiatetime", (支持的<SSL\_ctxID>范围), (支持的<negotiate\_time>范围)  
 +QSSLCFG: "sni", (支持的<SSL\_ctxID>范围), (支持的<SNI>列表)  
 +QSSLCFG: "closetimemode", (支持的<SSL\_ctxID>范围), (支持的<close\_time\_mode>列表)  
 +QSSLCFG: "ignoremulticertchainverify", (支持的<SSL\_c

|   |  |
|---|--|
|   | txID>范围),(支持的<ignore_multicertchain_verify>列表)<br><b>+QSSLCFG: "ignoreinvalidcertsign",</b> (支持的<SSL_ctxID>范围),(支持的<ignore_invalid_certsign>列表)<br><b>+QSSLCFG: "session_cache",</b> (支持的<SSL_ctxID>范围),<br>(支持的<session_cache_enable>列表)<br><br><b>OK</b> |
| 设置命令<br>配置指定 SSL 上下文的 SSL 版本:<br><b>AT+QSSLCFG="sslversion",&lt;SSL_ctxID&gt;[,&lt;SSL_version&gt;]</b>   | 响应<br>若省略可选参数,则查询指定 SSL 上下文的 SSL 版本:<br><b>+QSSLCFG: "sslversion",&lt;SSL_ctxID&gt;,&lt;SSL_version&gt;</b><br><br><b>OK</b><br><br>若指定可选参数,则配置指定 SSL 上下文的 SSL 版本:<br><b>OK</b><br>或者<br><b>ERROR</b>  |
| 设置命令<br>配置指定 SSL 上下文的加密套件:<br><b>AT+QSSLCFG="ciphersuite",&lt;SSL_ctxID&gt;[,&lt;cipher_suites&gt;]</b>   | 响应<br>若省略可选参数,则查询指定 SSL 上下文的加密套件:<br><b>+QSSLCFG: "ciphersuite",&lt;SSL_ctxID&gt;,&lt;cipher_suites&gt;</b><br><br><b>OK</b><br><br>若指定可选参数,则配置指定 SSL 指定上下文的加密套件:<br><b>OK</b><br>或者<br><b>ERROR</b>   |
| 设置命令<br>配置指定 SSL 上下文的受信任 CA 证书路径:<br><b>AT+QSSLCFG="cacert",&lt;SSL_ctxID&gt;[,&lt;cacertpath&gt;]</b>    | 响应<br>若省略可选参数,则查询指定 SSL 上下文的受信任 CA 证书路径:<br><b>+QSSLCFG: "cacert",&lt;SSL_ctxID&gt;,&lt;cacertpath&gt;</b><br><br><b>OK</b><br><br>若指定可选参数,则配置指定 SSL 上下文的受信任 CA 证书路径:<br><b>OK</b><br>或者<br><b>ERROR</b>   |
| 设置命令<br>配置指定 SSL 上下文的受信任 CA 证书路径:<br><b>AT+QSSLCFG="cacertex",&lt;SSL_ctxID&gt;[,&lt;cacertpath&gt;]]</b> | 响应<br>若省略全部可选参数,则查询全部 SSL 上下文的受信任 CA 证书路径:<br><b>+QSSLCFG: "cacertex",0,&lt;cacertpath&gt;</b><br>.....  |

|   |   |
|---|---|
|   | <p><b>+QSSLCFG: "cacertex",5,&lt;cacertpath&gt;</b></p> <p><b>OK</b></p> <p>若只省略&lt;cacertpath&gt;，则查询指定 SSL 上下文的受信任 CA 证书路径：</p> <p><b>+QSSLCFG: "cacertex",&lt;SSL_ctxID&gt;,&lt;cacertpath&gt;</b></p> <p><b>OK</b></p> <p>若指定全部可选参数，则配置指定 SSL 上下文的受信任 CA 证书路径：</p> <p><b>OK</b></p> <p>或者</p> <p><b>ERROR</b></p> |
| <p>设置命令</p> <p>配置指定 SSL 上下文的客户端证书路径：</p> <p><b>AT+QSSLCFG="clientcert",&lt;SSL_ctxID&gt;[,&lt;client_cert_path&gt;]</b></p> | <p>响应</p> <p>若省略可选参数，则查询指定 SSL 上下文的客户端证书路径：</p> <p><b>+QSSLCFG:"clientcert",&lt;SSL_ctxID&gt;,&lt;client_cert_path&gt;</b></p> <p><b>OK</b></p> <p>若指定可选参数，则配置指定 SSL 上下文的客户端证书路径：</p> <p><b>OK</b></p> <p>或者</p> <p><b>ERROR</b></p>  |
| <p>设置命令</p> <p>配置指定 SSL 上下文的客户端密钥：</p> <p><b>AT+QSSLCFG="clientkey",&lt;SSL_ctxID&gt;[,&lt;client_key_path&gt;]</b></p>     | <p>响应</p> <p>若省略可选参数，则查询指定 SSL 上下文的客户端密钥：</p> <p><b>+QSSLCFG: "clientkey",&lt;SSL_ctxID&gt;,&lt;client_key_path&gt;</b></p> <p><b>OK</b></p> <p>若指定可选参数，则配置指定 SSL 上下文的客户端密钥：</p> <p><b>OK</b></p> <p>或者</p> <p><b>ERROR</b></p>   |
| <p>设置命令</p> <p>配置指定 SSL 上下文的身份验证模式：</p> <p><b>AT+QSSLCFG="secllevel",&lt;SSL_ctxID&gt;[,&lt;secllevel&gt;]</b></p>          | <p>响应</p> <p>若省略可选参数，则查询指定 SSL 上下文的身份验证模式：</p> <p><b>+QSSLCFG: "secllevel",&lt;SSL_ctxID&gt;,&lt;secllevel&gt;</b></p> <p><b>OK</b></p> <p>若省略可选参数，则配置指定 SSL 上下文的身份验证模式：</p> <p><b>OK</b></p> <p>或者</p>   |



|   |  |
|---|--|
| <p>设置命令</p> <p>配置指定 SSL 上下文是否忽略证书有效性验证:</p> <p><b>AT+QSSLCFG="ignorelocaltime",&lt;SSL_ctxID&gt;[,&lt;ignore_ltime&gt;]</b></p>         | <p><b>ERROR</b></p> <p>响应</p> <p>若省略可选参数,则查询指定 SSL 上下文是否忽略证书有效性验证:</p> <p><b>+QSSLCFG: "ignorelocaltime",&lt;SSL_ctxID&gt;,&lt;ignore_ltime&gt;</b></p> <p><b>OK</b></p> <p>若指定可选参数,则配置指定 SSL 上下文是否忽略证书有效性验证:</p> <p><b>OK</b></p> <p>或者</p> <p><b>ERROR</b></p> |
| <p>设置命令</p> <p>配置指定 SSL 上下文在 SSL 协商阶段的最大超时时间:</p> <p><b>AT+QSSLCFG="negotiatetime",&lt;SSL_ctxID&gt;[,&lt;negotiate_time&gt;]</b></p>   | <p>响应</p> <p>若省略可选参数,则查询指定 SSL 上下文在 SSL 协商阶段的最大超时时间:</p> <p><b>+QSSLCFG: "negotiatetime",&lt;SSL_ctxID&gt;,&lt;negotiate_time&gt;</b></p> <p><b>OK</b></p> <p>若指定可选参数,则配置指定 SSL 上下文在 SSL 协商阶段的最大超时时间:</p> <p><b>OK</b></p> <p>或者</p> <p><b>ERROR</b></p>         |
| <p>设置命令</p> <p>打开或关闭指定 SSL 上下文的服务器名称指示功能:</p> <p><b>AT+QSSLCFG="sni",&lt;SSL_ctxID&gt;[,&lt;SNI&gt;]</b></p>                            | <p>响应</p> <p>若省略可选参数,则查询指定 SSL 上下文是否打开服务器名称指示功能:</p> <p><b>+QSSLCFG: "sni",&lt;SSL_ctxID&gt;,&lt;SNI&gt;</b></p> <p><b>OK</b></p> <p>若指定可选参数,则打开或关闭指定 SSL 上下文的服务器名称指示功能:</p> <p><b>OK</b></p> <p>或者</p> <p><b>ERROR</b></p>                                      |
| <p>设置命令</p> <p>启用或禁用指定 SSL 上下文的关闭 SSL 连接的延迟时间:</p> <p><b>AT+QSSLCFG="closetimemode",&lt;SSL_ctxID&gt;[,&lt;close_time_mode&gt;]</b></p> | <p>响应</p> <p>若省略可选参数,则查询指定 SSL 上下文是否启用延迟时间:</p> <p><b>+QSSLCFG: "closetimemode",&lt;SSL_ctxID&gt;,&lt;close_time_mode&gt;</b></p>  |

|  |   |
|--|---|
|  | <p><b>OK</b></p> <p>若指定可选参数，则启用或禁用指定 SSL 上下文的 SSL 关闭延迟时间：</p> <p><b>OK</b></p> <p>或者</p> <p><b>ERROR</b></p>  |
| <p>设置命令</p> <p>配置指定 SSL 上下文是否忽略多级证书链验证：</p> <p><b>AT+QSSLCFG="ignoremulticertchainverify",&lt;SSL_ctxID&gt;[,&lt;ignore_multicertchain_verify&gt;]</b></p> | <p>响应</p> <p>若省略可选参数，则查询指定 SSL 上下文是否忽略多级证书链验证：</p> <p><b>+QSSLCFG: "ignoremulticertchainverify",&lt;SSL_ctxID&gt;,&lt;ignore_multicertchain_verify&gt;</b></p> <p><b>OK</b></p> <p>若指定可选参数，则配置指定 SSL 上下文是否忽略多级证书链验证：</p> <p><b>OK</b></p> <p>或者</p> <p><b>ERROR</b></p> |
| <p>设置命令</p> <p>配置指定 SSL 上下文是否忽略无效证书签名：</p> <p><b>+QSSLCFG="ignoreinvalidcertsign",&lt;SSL_ctxID&gt;[,&lt;ignore_invalid_certsign&gt;]</b></p>              | <p>响应</p> <p>若省略可选参数，则查询指定 SSL 上下文是否忽略无效证书签名：</p> <p><b>+QSSLCFG: "ignoreinvalidcertsign",&lt;SSL_ctxID&gt;,&lt;ignore_invalid_certsign&gt;</b></p> <p><b>OK</b></p> <p>若省略可选参数，则配置指定 SSL 上下文是否忽略无效证书签名：</p> <p><b>OK</b></p> <p>或者</p> <p><b>ERROR</b></p>             |
| <p>设置命令</p> <p>打开或关闭指定 SSL 上下文的会话恢复功能：</p> <p><b>AT+QSSLCFG="session_cache",&lt;SSL_ctxID&gt;[,&lt;session_cache_enable&gt;]</b></p>                       | <p>响应</p> <p>若省略可选参数，则查询指定 SSL 上下文是否打开会话恢复功能：</p> <p><b>+QSSLCFG: "session_cache",&lt;SSL_ctxID&gt;,&lt;session_cache_enable&gt;</b></p> <p><b>OK</b></p> <p>若指定可选参数，则打开或关闭指定 SSL 上下文的会话恢复功能：</p> <p><b>OK</b></p>  |

|        |                      |
|--------|----------------------|
|        | 或者<br><b>ERROR</b>   |
| 最大响应时间 | 300 毫秒               |
| 特性说明   | 该命令立即生效；<br>参数配置不保存。 |

## 参数

|                 |  |
|-----------------|--|
| <SSL_ctxID>     | 整型。SSL 上下文标识符。范围：0~5。                              |
| <SSL_version>   | 整型。SSL 版本。   |
|                 | 0           SSL 3.0                                |
|                 | 1           TLS 1.0                                |
|                 | 2           TLS 1.1                                |
|                 | 3           TLS 1.2                                |
|                 | 4           全部                                     |
| <cipher_suites> | 十六进制数值。SSL 加密套件。                                   |
|                 | 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         |
|                 | 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     |
|                 | 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    |
|                 | 0XC011     TLS_ECDHE_RSA_WITH_RC4_128_SHA          |
|                 | 0XC012     TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA     |
|                 | 0XC013     TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA      |
|                 | 0XC014     TLS_ECDHE_RSA_WITH_AES_256_CBC_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       |
|                 | 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                                    |
|   | 0XC02F        | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256                                   |
|   | 0XC030        | MBEDTLS_TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384                           |
|   | <u>0xFFFF</u> | 支持所有加密套件  |
| <b>&lt;ignore_ltime&gt;</b>                 |               | 整型。是否忽略证书有效性验证。<br>0 不忽略<br>1 忽略  |
| <b>&lt;cacertpath&gt;</b>                   |               | 字符串类型。受信任 CA 证书路径。  |
| <b>&lt;client_cert_path&gt;</b>             |               | 字符串类型。客户端证书路径。  |
| <b>&lt;client_key_path&gt;</b>              |               | 字符串类型。客户端密钥路径。  |
| <b>&lt;seclevel&gt;</b>                     |               | 字符串类型。身份验证模式。<br>0 无身份验证模式<br>1 进行服务器身份验证<br>2 如果远程服务器要求，则进行服务器和客户端身份验证 |
| <b>&lt;negotiate_time&gt;</b>               |               | 整型。表示 SSL 协商阶段的最大超时时间。范围：10~300；默认值：300；单位：秒。                           |
| <b>&lt;SNI&gt;</b>                          |               | 整型。打开或关闭服务器名称指示功能。<br>0 关闭<br>1 打开                                      |
| <b>&lt;close_time_mode&gt;</b>              |               | 整型。启用或禁用关闭 SSL 连接的延迟。<br>0 禁用，此时关闭延迟时间的单位为秒<br>1 启用，此时 SSL 关闭延迟时间的单位为毫秒 |
| <b>&lt;ignore_multicertchain_verify&gt;</b> |               | 整型。表示是否忽略多级证书链验证。<br>0 不忽略<br>1 忽略                                      |
| <b>&lt;ignore_invalid_certsig&gt;</b>       |               | 整型。表示是否忽略无效证书签名。<br>0 不忽略<br>1 忽略                                       |
| <b>&lt;session_cache_enable&gt;</b>         |               | 整型。打开或关闭 SSL 会话恢复功能。<br>0 关闭<br>1 打开                                    |

### 2.2.2. AT+QSSLOPEN 打开 SSL Socket 连接远程服务器

该命令用于建立 SSL 连接，即打开 SSL socket 连接远程服务器。在模块和网络协商期间，**AT+QSSLCFG** 将用于握手过程中的参数配置。与网络成功握手后，模块可以通过此 SSL 连接发送或接收数据，还可以基于一个 SSL 上下文建立多个 SSL 连接。

根据第 1.2 章中的步骤，需先执行 **AT+QIACT** 以激活 PDP 上下文，然后执行 **AT+QSSLOPEN**。等待指定的时间（可参考下面的最大响应时间）后将输出 **URC +QSSLOPEN: <clientID>,<err>**。如果在此期间未收到 URC 响应，则可以使用 **AT+QSSLCLOSE** 关闭 SSL 连接。

| AT+QSSLOPEN 打开 SSL Socket 连接远程服务器   |   |
|---|---|
| 测试命令<br>AT+QSSLOPEN=?   | <p>响应</p> <p><b>+QSSLOPEN:</b> (支持的&lt;PDP_ctxID&gt;范围),(支持的&lt;SSL_ctxID&gt;范围),(支持的&lt;clientID&gt;范围),&lt;serveraddr&gt;,&lt;server_port&gt;[, (支持的&lt;access_mode&gt;范围)]</p> <p><b>OK</b></p>  |
| 设置命令<br>AT+QSSLOPEN=<PDP_ctxID>,<SSL_ctxID>,<clientID>,<serveraddr>,<server_port>[,<access_mode>] | <p>响应</p> <p>若&lt;access_mode&gt;=2 并且成功建立 SSL 连接:<br/><b>CONNECT</b></p> <p>若有任何错误:<br/><b>ERROR</b></p> <p>若&lt;access_mode&gt;=0/1:<br/><b>OK</b></p> <p><b>+QSSLOPEN: &lt;clientID&gt;,&lt;err&gt;</b><br/>当&lt;err&gt;=0, 表示成功打开 SSL socket; 否则, 表示打开 SSL socket 失败:</p> <p>若有任何错误:<br/><b>ERROR</b></p> |
| 最大响应时间  | 最大网络响应时间为 150 秒, 需再加上<negotiate_time>配置的时间  |
| 特性说明  | /   |

## 参数

|                  |  |
|------------------|--|
| <PDP_ctxID>      | 整型。PDP 上下文标识符。范围: 1~15。                            |
| <SSL_ctxID>      | 整型。SSL 上下文标识符。范围: 0~5。                             |
| <clientID>       | 整型。Socket 索引。范围: 0~11。                             |
| <serveraddr>     | 字符串类型。远程服务器地址。                                     |
| <server_port>    | 整型。远程服务器监听端口。                                      |
| <access_mode>    | 整型。表示 SSL 连接的数据访问模式。<br>0 缓存模式<br>1 直吐模式<br>2 透传模式 |
| <err>            | 整型。操作结果码。详细信息请参考第 5 章。                             |
| <negotiate_time> | 整型。表示 SSL 协商阶段的最大超时时间。范围: 10~300; 默认值: 300; 单位: 秒。 |

### 2.2.3. AT+QSSSEND 通过 SSL 连接发送数据

建立 SSL 连接后，模块可以通过该连接发送数据。

| AT+QSSSEND 通过 SSL 连接发送数据   |  |
|--|--|
| 测试命令<br><b>AT+QSSSEND=?</b>  | 响应<br><b>+QSSSEND: (支持的&lt;clientID&gt;范围)[,(支持的&lt;sendlen&gt;范围)]</b><br><br><b>OK</b>   |
| 设置命令<br>发送不定长数据<br><b>AT+QSSSEND=&lt;clientID&gt;</b>                | 响应<br><b>&gt;</b><br>响应>后，输入要发送的数据。点击 <b>CTRL+Z</b> 发送，点击 <b>ESC</b> 取消操作。<br><br>若已建立 SSL 连接且数据发送成功：<br><b>SEND OK</b><br><br>若已建立 SSL 连接但缓存已满：<br><b>SEND FAIL</b><br><br>若 SSL 连接未建立、异常断开或参数错误：<br><b>ERROR</b> |
| 设置命令<br>发送定长数据<br><b>AT+QSSSEND=&lt;clientID&gt;,&lt;sendlen&gt;</b> | 响应<br><b>&gt;</b><br>响应>后，输入要发送的数据，直至数据长度达到<sendlen>配置的长度。<br><br>若已建立 SSL 连接且数据发送成功：<br><b>SEND OK</b><br><br>若已建立 SSL 连接但缓存已满：<br><b>SEND FAIL</b><br><br>若 SSL 连接未建立、异常断开或参数错误：<br><b>ERROR</b>                 |
| 最大响应时间   | 300 毫秒   |
| 特性说明   | /  |

## 参数

|            |                             |
|------------|-----------------------------|
| <clientID> | 整型。Socket 索引。范围：0~11。       |
| <sendlen>  | 整型。发送数据的长度。范围：1~1460；单位：字节。 |

## 备注

发送的数据包括定长数据和不定长数据，最大长度都为 1460 个字节。

### 2.2.4. AT+QSSLRECV 通过 SSL 连接接收数据

当 SSL 连接的数据访问模式为缓存模式时，模块收到网络发送的数据时将上报 URC **+QSSLURC: "recv",<clientID>**。可以通过 **AT+QSSLRECV** 读取缓存的数据。

#### AT+QSSLRECV 通过 SSL 连接接收数据

|   |   |
|---|---|
| 测试命令<br><b>AT+QSSLRECV=?</b>                                | 响应<br><b>+QSSLRECV: (支持的&lt;clientID&gt;范围),(支持的&lt;readlen&gt;范围)</b><br><br><b>OK</b>   |
| 设置命令<br><b>AT+QSSLRECV=&lt;clientID&gt;,&lt;readlen&gt;</b> | 响应<br>若指定 Socket 连接接收到数据：<br><b>+QSSLRECV: &lt;have_readlen&gt;&lt;CR&gt;&lt;LF&gt;&lt;data&gt;</b><br><br><b>OK</b><br><br>若缓冲区为空：<br><b>+QSSLRECV: 0</b><br><br><b>OK</b><br><br>若 SSL 连接未建立、异常断开或参数错误：<br><b>ERROR</b> |
| 最大响应时间  | 300 毫秒  |
| 特性说明  | /   |

## 参数

|                |   |
|----------------|---|
| <clientID>     | 整型。Socket 索引。范围：0~11。                     |
| <readlen>      | 整型。需读取数据的最大长度。范围：0~1500；单位：字节；默认值：1500。   |
| <have_readlen> | 整型。通过 <b>AT+QSSLRECV</b> 读取的数据实际长度。单位：字节。 |

<data> 字符串类型。实际读取的数据。单位：字节。

### 2.2.5. AT+QSSLCLOSE 关闭 SSL 连接

该命令用于关闭 SSL 连接。如果基于同一 SSL 上下文的所有 SSL 连接都已关闭，则模块将释放 SSL 上下文。

| AT+QSSLCLOSE 关闭 SSL 连接   |  |
|--|--|
| 测试命令<br><b>AT+QSSLCLOSE=?</b>  | 响应<br><b>+QSSLCLOSE:</b> (支持的<clientID>范围),(支持的<close_timeout>范围)<br><br><b>OK</b> |
| 设置命令<br><b>AT+QSSLCLOSE=&lt;clientID&gt;[,&lt;close_timeout&gt;]</b> | 响应<br>如果 SSL 连接成功关闭:<br><b>OK</b><br><br>若发生任何错误:<br><b>ERROR</b>                  |
| 最大响应时间   | 取决于<close_timeout>配置的时间  |
| 特性说明   | 该命令立即生效;<br>参数配置不保存。   |

#### 参数

|                 |   |
|-----------------|---|
| <clientID>      | 整型。Socket 索引。范围：0~11。   |
| <close_timeout> | 整型。AT+QSSLCLOSE 执行的超时时间。范围：0~65535；默认值：10。0 表示立即执行该命令。<close_timeout> 的单位取决于 AT+QSSLCFG="closetimemode" 的配置，若 <close_time_mode>=0，则 <close_timeout> 的单位为秒；若 <close_time_mode>=1，则 <close_timeout> 的单位为毫秒。 |

### 2.2.6. AT+QSSLSTATE 查询 Socket 连接状态

该命令用于查询 Socket 连接状态，且仅能查询 SSL 连接状态。

| AT+QSSLSTATE 查询 Socket 连接状态                  |  |
|--|--|
| 测试命令<br><b>AT+QSSLSTATE=?</b>                | 响应<br><b>OK</b>  |
| 设置命令<br><b>AT+QSSLSTATE=&lt;clientID&gt;</b> | 响应<br><b>+QSSLSTATE:</b> <clientID>,"SSLClient",<IP_address>,<re |



|                             |  |
|-----------------------------|--|
|                             | <p>mote_port&gt;,&lt;local_port&gt;,&lt;socket_state&gt;,&lt;PDP_ctxID&gt;,&lt;serverID&gt;,&lt;access_mode&gt;,&lt;AT_port&gt;,&lt;SSL_ctxID&gt;</p> <p>OK</p>  |
| 执行命令<br><b>AT+QSSLSTATE</b> | <p>响应</p> <p>(+QSSLSTATE: &lt;clientID&gt;,"SSLClient",&lt;IP_address&gt;,&lt;remote_port&gt;,&lt;local_port&gt;,&lt;socket_state&gt;,&lt;PDP_ctxID&gt;,&lt;serverID&gt;,&lt;access_mode&gt;,&lt;AT_port&gt;,&lt;SSL_ctxID&gt;)的列表</p> <p>OK</p> |
| 最大响应时间                      | 300 毫秒   |
| 特性说明                        | /  |

## 参数

|                |   |
|----------------|---|
| <clientID>     | 整型。Socket 索引。范围：0~11。   |
| <IP_address>   | 字符串类型。远程服务器地址。  |
| <remote_port>  | 整型。远程服务器端口。范围：0~65535。  |
| <local_port>   | 整型。本地端口。范围：0~65535。   |
| <socket_state> | 整型。SSL 连接状态。<br>0 "Initial" 连接尚未建立<br>1 "Opening" 客户端正在连接<br>2 "Connected" 客户端连接已建立<br>4 "Closing" 连接正在关闭   |
| <PDP_ctxID>    | 整型。PDP 上下文标识符。范围：1~15。  |
| <serverID>     | 整型。此参数为预留参数。  |
| <access_mode>  | 整型。表示 SSL 连接的数据访问模式。<br>0 缓存模式<br>1 直吐模式<br>2 透传模式  |
| <AT_port>      | 字符串类型。Socket 服务的 COM 口。<br>"usbmodem" USB modem port<br>"usbat" USB AT port<br>"uart1" UART port 1<br>"cmux1" MUX port 1<br>"cmux2" MUX port 2<br>"cmux3" MUX port 3<br>"cmux4" MUX port 4。 |
| <SSL_ctxID>    | 整型。SSL 上下文标识符。范围：0~5。   |

## 2.3. URC 详解

### 2.3.1. +QSSLURC: "recv" 通知主机接收数据

该 URC 用于通知主机读取从对端接收的数据。

| +QSSLURC: "recv" 通知主机接收数据                                      |  |
|--|--|
| +QSSLURC: "recv",<clientID>                                    | 缓存模式下接收数据时上报的 URC。SSL 数据可通过 <b>AT+QSSLRECV</b> 接收。 |
| +QSSLURC: "recv",<clientID>,<current_recvlength><CR><LF><data> | 直吐模式下接收数据时上报的 URC。                                 |

#### 参数

|                      |                       |
|----------------------|-----------------------|
| <clientID>           | 整型。Socket 索引。范围：0~11。 |
| <current_recvlength> | 整型。实际接收的数据长度。单位：字节。   |
| <data>               | 需读取的数据。单位：字节。         |

### 2.3.2. +QSSLURC: "closed" 通知异常断开连接

该 URC 用于通知主机连接已断开。断开连接可能由多种原因引起，例如网络关闭连接或 GPRS PDP 被去激活，指定 Socket 的 SSL 连接状态可能为"closing"，此时需执行 **AT+QSSLCLOSE=<clientID>**将 SSL 连接状态改为"initial"。

| +QSSLURC: "closed" 通知异常断开连接   |                          |
|-------------------------------|--------------------------|
| +QSSLURC: "closed",<clientID> | 基于指定 Socket 的 SSL 连接已关闭。 |

#### 参数

|            |                        |
|------------|------------------------|
| <clientID> | 整型。Socket 标识符。范围：0~11。 |
|------------|------------------------|

## 3 举例

### 3.1. 配置并激活 PDP 上下文

#### 3.1.1. 配置 PDP 上下文

```
AT+QICSGP=1,1,"UNINET","",1 //配置上下文为 1。“UNINET”表示中国联通。
OK
```

#### 3.1.2. 激活 PDP 上下文

```
AT+QIACT=1 //激活上下文为 1。
OK //激活成功。
AT+QIACT? //查询上下文状态。
+QIACT: 1,1,1,"10.7.157.1"
OK
```

#### 3.1.3. 去激活 PDP 上下文

```
AT+QIDEACT=1 //去激活上下文 1。
OK //去激活成功。
```

### 3.2. 配置 SSL 上下文

```
AT+QSSLCFG="sslversion",1,1 //设置 SSL 上下文标识符和 SSL 版本都为 1。
OK
AT+QSSLCFG="ciphersuite",1,0X0035 //设置 SSL 上下文标识符为 1，SSL 加密套件为
TLS_RSA_WITH_AES_256_CBC_SHA。
OK
AT+QSSLCFG="secclevel",1,1 //设置 SSL 上下文标识符为 1，身份验证模式为进行服务器
身份验证。
OK
```

```
AT+QSSLCFG="cacert",1,"UFS:cacert.pem" //设置 SSL 上下文标识符为 1，受信任 CA 证书路径为
UFS:cacert.pem。
OK
```

### 3.3. SSL 客户端在缓存模式下工作

#### 3.3.1. 建立 SSL 连接并进入缓存模式

```
AT+QSSLOPEN=1,1,4,"220.180.239.212",8010,0
OK

+QSSLOPEN: 4,0 //成功建立 SSL 连接。
AT+QSSLSTATE //查询所有 SSL 连接的状态。
+QSSLSTATE: 4,"SSLClient","220.180.239.212",8010,65344,2,1,4,0,"usbmodem",1
OK
```

#### 3.3.2. 缓存模式下发送数据

##### 3.3.2.1. 发送不定长数据

```
AT+QSSLSEND=4 //发送不定长数据。
>
Test data from SSL
<CTRL+Z>
SEND OK
```

##### 3.3.2.2. 发送定长数据

```
AT+QSSLSEND=4,18 //发送数据且数据长度为 18 个字节。
>
Test data from SSL
SEND OK
```

#### 3.3.3. 缓存模式下接收数据

```
+QSSLURC: "recv",4 //Socket 4 (<clientID> = 4) 接收到数据。
AT+QSSLRCV=4,1500 //读取数据。需读取数据的长度为 1500 个字节。
```

```
+QSSLRCV: 18 //实际读取数据长度为18个字节。
Test data from SSL

OK
AT+QSSLRCV=4,1500
+QSSLRCV: 0 //缓冲区无数据。

OK
```

### 3.3.4. 关闭 SSL 连接

```
AT+QSSLCLOSE=4 //关闭 SSL 连接 (<clientID> = 4)。取决于网络，最大响应时间为 10 秒。

OK
```

## 3.4. SSL 客户端在直吐模式下工作

### 3.4.1. 建立 SSL 连接并进入直吐模式

```
AT+QSSLOPEN=1,1,4,"220.180.239.212",8011,1
OK

+QSSLOPEN: 4,0 //成功建立 SSL 连接。
AT+QSSLSTATE //查询所有 SSL 连接的状态。
+QSSLSTATE: 4,"SSLClient","220.180.239.212",8011,65047,2,1,4,1,"usbmodem",1

OK
```

### 3.4.2. 直吐模式下发送数据

```
AT+QSSLSEND=4 //发送不定长数据。
>
Test data from SSL
<CTRL+Z>
SEND OK
AT+QSSLSEND=4,18 //发送数据且数据长度为 18 个字节。
>
Test data from SSL
SEND OK
```

### 3.4.3. 直吐模式下接收数据

```
+QSSLURC: "recv",4,18
Test data from SSL
```

### 3.4.4. 关闭 SSL 连接

```
AT+QSSLCLOSE=4 //关闭 SSL 连接 (<clientID> = 4)。取决于网络，
                最大响应时间为 10 秒。

OK
```

## 3.5. SSL 客户端在透传模式下工作

### 3.5.1. 建立 SSL 连接并在透传模式下发送数据

```
AT+QSSLOPEN= 1,1,4,"220.180.239.212",8011,2 //建立 SSL 连接。
CONNECT //进入透传模式。
//客户端直接通过 COM 端口向网络发送数据。(该举
//例中数据不可见)
OK //+++或者 DTR (需先执行 AT&D1) 可用于退出透
    传模式。若服务器异常断开 SSL 连接，将上报结
    果码 NO CARRIER。
```

### 3.5.2. 建立 SSL 连接并在透传模式下接收数据

```
AT+QSSLOPEN=1,1,4,"220.180.239.212",8011,2 //建立 SSL 连接。
CONNECT //进入透传模式。
<Received data> //客户端正在读取数据。
OK //通过+++或者 DTR (需先执行 AT&D1) 退出透
    传模式。若服务器断开 SSL 连接，将上报结果码
    NO CARRIER。
```

### 3.5.3. 关闭 SSL 连接

```
AT+QSSLCLOSE=4 //关闭 SSL 连接 (<clientID> = 4)。取决于网络，
                最大响应时间为 10 秒。

OK
```

# 4 SSL 连接失败原因的排查

若 SSL 连接打开失败，请进行以下排查：

1. 通过 **AT+QIACT?** 查询指定 PDP 上下文的状态，检查指定 PDP 上下文是否已被激活。
2. 由于无效的 DNS 服务器无法将域名转换为 IP 地址，若远程服务器地址为域名，还请通过 **AT+QIDNSCFG=<contextID>** 检查 DNS 服务器地址是否有效。关于 **AT+QIDNSCFG** 的详细信息，可参考文档 [1]。
3. 通过 **AT+QSSLCFG** 检查 SSL 配置，尤其是 SSL 版本及加密套件，以确保服务器端可以支持。若 **<seclvl>=1/2**，则需通过 **AT+QFUPL** 上传受信任 CA 证书。若服务器配置了 “SSLVerifyClient required”，则需通过 **AT+QFUPL** 上传客户端证书和客户端密钥。关于证书有效性验证的更多细节，请参考第 1.5 章。关于 **AT+QFUPL** 详细信息，可参考文档 [2]。

# 5 结果码

如果在执行 SSL 相关 AT 命令后返回 **ERROR**，都可以通过 **AT+QIGETERROR** 查询错误的详细信息，但需注意 **AT+QIGETERROR** 仅返回最后一个 SSL 命令的错误代码。关于 **AT+QIGETERROR** 的详情请参考文档 [1]。

表 5：结果码

| <err> | 结果码                           | 描述           |
|-------|-------------------------------|--------------|
| 0     | Operation successful          | 操作成功         |
| 550   | Unknown error                 | 未知错误         |
| 551   | Operation blocked             | 操作被阻止        |
| 552   | Invalid parameter             | 无效参数         |
| 553   | Memory not enough             | 内存不足         |
| 554   | Create socket failed          | 创建Socket失败   |
| 555   | Operation not supported       | 不支持该操作       |
| 556   | Socket bind failed            | Socket绑定失败   |
| 557   | Socket listen failed          | Socket监听失败   |
| 558   | Socket write failed           | Socket写入失败   |
| 559   | Socket read failed            | Socket读取失败   |
| 560   | Socket accept failed          | Socket接受失败   |
| 561   | Open PDP context failed       | 打开PDP上下文失败   |
| 562   | Close PDP context failed      | 关闭PDP上下文失败   |
| 563   | Socket identity has been used | Socket标识已被使用 |
| 564   | DNS busy                      | DNS业务繁忙      |



|     |                          |            |
|-----|--------------------------|------------|
| 565 | DNS parse failed         | DNS解析失败    |
| 566 | Socket connection failed | Socket连接失败 |
| 567 | Socket has been closed   | Socket已关闭  |
| 568 | Operation busy           | 操作繁忙       |
| 569 | Operation timeout        | 操作超时       |
| 570 | PDP context break down   | PDP上下文崩溃   |
| 571 | Cancel send              | 取消发送       |
| 572 | Operation not allowed    | 不允许操作      |
| 573 | APN not configured       | 未配置APN     |
| 574 | Port busy                | 端口繁忙       |

# 6 附录 参考文档及术语缩写

表 6: 参考文档

| 文档名称                                       |
|--|
| [1] Quectel_LTE_Standard(A)系列_TCP(IP)_应用指导 |
| [2] Quectel_LTE_Standard(A)系列_FILE_应用指导    |
| [3] Quectel_LTE_Standard(A)系列_AT 命令手册      |

表 7: 术语缩写

| 缩写     | 英文全称  | 中文全称        |
|--------|---|-------------|
| APN    | Access Point Name                               | 接入点名称       |
| CA     | Certificate Authority                           | 证书授权        |
| CR     | Carriage Return                                 | 回车符         |
| DNS    | Domain Name Server                              | 域名服务器       |
| DTR    | Data Terminal Ready                             | 数据终端就绪      |
| LF     | Line Feed                                       | 换行符         |
| PDP    | Packet Data Protocol                            | 分组数据协议      |
| SNI    | Server Name Indication                          | 服务器名称指示     |
| SSL    | Security Socket Layer                           | 安全套接层协议     |
| TCP/IP | Transmission Control Protocol/Internet Protocol | 传输控制协议/网际协议 |
| TLS    | Transport Layer Security                        | 安全传输层协议     |
| UART   | Universal Asynchronous Receiver/Transmitter     | 通用异步收发机     |
| UFS    | Universal Flash Storage                         | 通用闪存存储      |
| URC    | Unsolicited Result Code                         | 非请求结果码      |
| USB    | Universal Serial Bus                            | 通用串行总线      |