SIM7000 系列_SSL_应用文档_V1.00

手册名称	SIM7000 系列_SSL_应用文档
版本	1.00
日期	2018-04-16
状态	发布
文档控制号	SIM7000 系列_SSL__应用文档_V1.00

一般事项

SIMCom把本手册作为一项对客户的服务，编排紧扣客户需求，章节清晰，叙述简要，力求客户阅读后，可以通过AT命令轻松使用模块，加快开发应用和工程计划的进度。

SIMCom不承担对相关附加信息的任何独立试验，包含可能属于客户的任何信息。而且，对一个包含SIMCom模块、较大型的电子系统而言，客户或客户的系统集成商肩负其系统验证的责任。

由于产品版本升级或其它原因，本手册内容会不定期进行更新。除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。手册中信息修改，恕不另行通知。

版权

本手册包含芯讯通无线科技（上海）有限公司的专利技术信息。除非经本公司书面许可，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，并不得以任何形式传播，犯规者可被追究支付赔偿金。对专利或者实用新型或者外观设计的版权所有，SIMCom保留一切权利。

版权所有©芯讯通无线科技（上海）有限公司2018年

目录

版本历史

日期	版本	修改点描述	作者
2018-04-16	1.00	第一版	

1 SSL 功能

1.1 SSL 介绍

安全套接层（Secure Sockets Layer，SSL），一种安全协议，是网景公司（Netscape）在推出 Web 浏览器首版的同时提出的，目的是为网络通信提供安全及数据完整性。SSL 在传输层对网络连接进行加密。

SSL 采用公开密钥技术，保证两个应用间通信的保密性和可靠性，使客户与服务器应用之间的通信不被攻击者窃听。它在服务器和客户机两端可同时被支持，目前已成为互联网上保密通讯的工业标准。现行 Web 浏览器亦普遍将 HTTP 和 SSL 相结合，从而实现安全通信。此协议和其继任者是 TLS（Transport Layer Security，TLS）。

TLS 利用密钥算法在互联网上提供端点身份认证与通讯保密，其基础是公钥基础设施（public key infrastructure，PKI）。不过在实现的典型例子中，只有网络服务者被可靠身份验证，而其客户端则不一定。这是因为公钥基础设施普遍商业运营，电子签名证书通常需要付费购买。协议的设计在某种程度上能够使主从式架构应用程序通讯本身预防窃听、干扰（Tampering）、和消息伪造。

SIM7000 系列模块目前支持 TLS1.0，TLS1.1，TLS1.2，DTLS1.0，DTLS1.2。

2 可支持 SSL 的 TCP/UDP 的 AT 命令

模块提供设备端使用的 AT 命令如下：

命令	描述
AT+CACID	设置 TCP/UDP 标识
AT+CASSL	设置协议类型及 SSL 配置的标识符
AT+CASSLCFG	设置 SSL 证书及超时时间
AT+CAOPEN	打开一个 TCP/UDP 连接
AT+CASEND	发送数据
AT+CARECV	接收数据
AT+CACLOSE	关闭一个 TCP/UDP 连接
AT+CSSLCFG	配置 SSL 参数

3 测试用例

3.1 建立一个普通的 TCP/UDP 连接

语法	说明
AT+CNACT=1,"cmnet" OK +APP PDP: ACTIVE AT+CNACT? +CNACT: 1,"10.181.182.177" OK	开启无线连接 参数 cmnet 为 APN，此参数需要根据不同卡设置不同的 APN 值 获取本地 IP
AT+CACID=0 OK	设备标识符
AT+CASSL=0,0,0 OK	设置协议类型 第一个参数为对应的标识符 第二个参数为是否使用 SSL，如果是普通的 TCP/UDP 连接，该参数为 0 第三个参数为协议类型，这里设置的 0 表示是 TCP。如果是 UDP，该位应设置为 1， 即 AT+CASSL=0,0,1 表示普通 UDP 协议
AT+CAOPEN=0,"116.247.119.165",5171 +CAOPEN: 0,0 OK	建立一个 TCP 连接 返回 URC 第一个参数为标识符，第二个参数为建立连接的结果，0 表示建立成功
AT+CASEND=0,5 > OK +CASEND: 0,0,5	请求发送 5 个字节数据 输入数据 数据发送成功
AT+CARECV=0,100 +CARECV: 0,20 GFDSGFDGFDSGHFDSHFDS OK	请求获取服务器发送的 100 个字节数据 实际接收到 20 个字节数据 输出接收到的数据
AT+CACLOSE=0 OK	关闭标识符为 0 的连接
AT+CNACT=0	断开无线连接

OK +APP PDP: DEACTIVE	

3.2 建立一个 SSL 连接

SSL 建立通信时需要对通信双方的身份进行验证，分为单向认证和双向认证。

单向认证是客户端去验证服务器的证书。服务器发送自己的服务器证书给客户端，客户端会验证签发该服务器证书的根证书是否可以信任，如果可以信任才会继续进行下面的通信流程。

双向认证客户端验证服务器证书后，客户端需要发送自己的证书给服务器，让服务器去验证自己的客户端证书。其验证过程都是一样的，都需要去确认签发证书的根证书是否可以信任。

3.2.1 建立一个单向认证的 SSL 连接

由于目前模块只能作为客户端，当需要建立一个单向认证的连接时，需要导入的是服务器的根证书。如果不导入任何证书，模块会默认所有的服务器都是可以信任的。

语法	说明
AT+CNACT=1,"cmnet" OK +APP PDP: ACTIVE AT+CNACT? +CNACT: 1,"10.181.182.177" OK	开启无线连接 参数 cmnet 为 APN，此参数需要根据不同卡设置不同的 APN 值 获取本地 IP
AT+CACID=0 OK	设备标识符
AT+CSSLCFG="sslversion",0,1 OK	设置标识符为 0 的 SSL 的协议类型 1 表示 TLS1.0
AT+CASSL=0,1,0 OK	设置协议类型 第一个参数为对应的标识符 第二个参数为是否使用 SSL，1 表示开启 SSL 功能 第三个参数为 AT+CSSLCFG 对应的 SSL 配置的标识符
AT+CASSLCFG=0,"cacert","root.pem" OK	设置根证书，该根证书必须是通过 AT+CSSLCFG 转换过的证书。 该项可以省略，如果省略默认所有的服务器证书都是可以信任的

AT+CAOPEN=0,"116.247.119.165",5171 +CAOPEN: 0,0 OK +CARECV: 0,38	建立一个 SSL 连接 连接建立成功 收到 38 个字节数据，当成功建立连接或者成功发送数据后，模块会主动去读取一次数据，这时如果收到了服务器数据，会上报该 URC，如果没有收到数据，不上报该 URC
AT+CARECV=0,100 +CARECV: 0,38 220 Serv-U FTP Server v15.0 ready... OK	读取 100 个字节数据 实际收到数据为 38 字节 输出数据
AT+CACLOSE=0 OK	关闭标识符为 0 的连接
AT+CNACT=0 OK +APP PDP: DEACTIVE	断开无线连接

3.2.2 建立一个双向认证的 SSL 连接

建立一个双向认证的 SSL 连接需要设置客户端证书。该客户端证书需要先通过 AT+CSSLCFG 进行转换。

模块可以支持的证书格式是.PEM，.DER，.P7B。

语法	说明
AT+CNACT=1,"cmnet" OK +APP PDP: ACTIVE AT+CNACT? +CNACT: 1,"10.181.182.177" OK	开启无线连接 参数 cmnet 为 APN，此参数需要根据不同卡设置不同的 APN 值 获取本地 IP
AT+CACID=0 OK	设备标识符
AT+CSSLCFG="sslversion",0,1 OK	设置标识符为 0 的 SSL 的协议类型 1 表示 TLS1.0
AT+CASSL=0,1,0 OK	设置协议类型 第一个参数为对应的标识符 第二个参数为是否使用 SSL，1 表示开启 SSL

	功能 第三个参数为 AT+CSSLCFG 对应的 SSL 配置的标识符
AT+CASSLCFG=0,"cacert","root.pem" OK	设置根证书 如果省略默认所有的服务器证书都是可以信任的
AT+CASSLCFG=0,"clientcert","client.pem" OK	设置客户端证书，该根证书必须是通过 AT+CSSLCFG 转换过可以直接使用的证书
AT+CAOPEN=0,"116.247.119.165",5171 +CAOPEN: 0,0 OK	建立一个 SSL 连接 连接建立成功
AT+CASEND=0,5 > OK +CASEND: 0,0,5	请求发送 5 个字节数据 输入数据 数据发送成功
AT+CACLOSE=0 OK	关闭标识符为 0 的连接
AT+CNACT=0 OK +APP PDP: DEACTIVE	断开无线连接

3.2.3 使用 AT+CSSLCFG 转换 SSL 证书

AT+CSSLCFG="convert",2,"root.pem" OK	配置需要转换的证书类型，2 表示是根证书 配置需要转换的证书名称，转换成功后的名称与现有证书名称一致
AT+CSSLCFG="convert",1,"client.pem","client.key" OK	配置需要转换的证书类型，1 表示是客户端证书 配置需要转换的证书名称，客户端证书需要输入证书文件跟私钥文件 转换成功后的名称与证书名称一致，即是“client.pem”

附录

A. 参考文档

编号	文档名称	说明
[1]	SIM7000 Series AT Command Manual	

B. 术语和缩写

术语	描述
SSL	安全套接层（Secure Sockets Layer，SSL）
TLS	Transport Layer Security

联系我们：

芯讯通无线科技（上海）有限公司

地址：上海市金钟路 633 号晨讯科技大楼 A 楼

邮编：200335

电话：+86 21 3252 3300

传真：+86 21 3252 3020

网址：www.simcomm2m.com