SIM7000系列_SSL_应用文档

LPWA 模组

芯讯通无线科技(上海)有限公司
上海市长宁区金钟路633号晨讯科技大楼B座6楼
电话：86-21-31575100
技术支持邮箱：support@simcom.com
官网：www.simcom.com

名称：	SIM7000系列_SSL_应用文档
版本：	1.01
日期：	2020.07.28
状态：	已发布

版权声明

芯讯通无线科技(上海)有限公司
上海市长宁区金钟路 633 号晨讯科技大楼 B 座 6 楼
电话：86-21-31575100
邮箱：simcom@simcom.com
官网：www.simcom.com

了解更多资料，请点击以下链接：
http://cn.simcom.com/download/list-230-cn.html

技术支持，请点击以下链接：
http://cn.simcom.com/ask/index-cn.html 或发送邮件至 support@simcom.com

关于文档

版本历史

版本	日期	作者	备注
1.00	2018-08-07	来文洁	第一版
1.01	2020-07-28	来文洁	修改文档结构和风格

适用范围

本文档适用于以下产品型号：

型号	类别	尺寸(mm)	备注
SIM7000E/C/A/G	Cat-M1(/NB1/EGPRS)	24*24	
SIM7000E-N SIM7000C-N	NB1	24*24	

目录

1 介绍

1.1 本文目的

基于 AT 指令手册扩展，本文主要介绍 SSL 业务流程。
参考此应用文档，开发者可以很快理解并快速开发相关业务。

1.2 参考文档

[1] SIM7000 Series_AT Command Manual

1.3 术语和缩写

2 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。

3 可支持 SSL 的 TCP/UDP 的 AT 命令

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

4 Bearer 配置

模块开机会自动激活 PDN 并获取 PS 业务地址。前提是数据卡和天线正常。

4.1 PDN 自激活

模块开机会自动激活 PDN 并获取 PS 业务地址。前提是数据卡和天线正常。

```
//PDN 自动激活示例.

AT+CPIN?                                  //检查 SIM 卡状态
+CPIN:READY

OK
AT+CGDCONT=1,"IP",""                      //在 CAT-M 或 NB-IOT 网络，如果需要可以在网络
                                          注册前配置 APN
                                          //APN 设置为空，模块将采用基站下发的 APN（推
                                          荐用此方式）。使用 AT+CGAPN 可查看具体下发的
                                          APN。
OK
AT+CSQ                                    //检查射频信号
+CSQ: 13,99

OK
AT+CGATT?                                 //检查是否成功注册 PS 服务.
+CGATT: 1                                 //1 表示已经注册成功

OK
AT+COPS?                                  //查询网络信息，运营商及网络制式
+COPS: 0,0,"CHN-CT",9                     //9 即 NB-IOT 网络

OK
AT+CGNAPN                                 //查询网络下发 APN 参数。
+CGNAPN: 1,"ctnb"

OK
AT+CNCFG=1,"ctnb","cdma","1234"           //如果需要的话激活之前请使用 AT+CNCFG 设置
                                          APN\用户名\密码等。
```

```
                                        在 CAT-M 或 NB-IOT 网络，如果设置的 APN 和
                                        CGNAPN 查询的 APN 相同或者 APN 设置为空，将
                                        使用默认的 PDN，否则将会向网络激活一路新的
                                        PDN。
                                        //在 GSM 网络下，此 APN 必须向运营商查询
OK
AT+CNACT=1                              //激活网络承载
OK

+APP PDP: ACTIVE
AT+CNACT?                               //查询注册网络成功后分配的 IP 地址
+CNACT: 1,"10.94.36.44"

OK
```

4.2 手动改变 APN 配置

若有需要改变 APN 配置的情景，请参照如下步骤。

```
//APN 配置示例.

AT+CFUN=0                               //关闭 RF
+CPIN: NOT READY

OK
AT+CGDCONT=1,"IP","ctnb"                //在 CAT-M 或 NB-IOT 网络，如果需要可以在网络
                                        注册前配置 APN。
                                        //使用 AT+CGAPN 可查看网络下发的 APN。
OK
AT+CFUN=1                               //打开 RF
OK

+CPIN: READY
AT+CGATT?                               //检查是否成功注册 PS 服务
+CGATT: 1                               //1 表示已经注册成功

OK
AT+CGNAPN                               //在 CAT-M 或 NB-IOT 网络注册成功后查询网络下
                                        发的 APN。GSM 网络下 APN 为空。
+CGNAPN: 1,"ctnb"
```

```
OK
AT+CNCFG=1,"ctnb","cdma","1234"          //如果需要的话激活之前请使用 AT+CNCFG 设置APN\用户名\密码等。
                                         //在 CAT-M 或 NB-IOT 网络，如果设置的 APN 和CGNAPN 查询的 APN 相同或者 APN 设置为空，将使用默认的 PDN，否则将会向网络激活一路新的PDN。
OK
AT+CNACT=1                               //激活网络承载。
OK

+APP PDP: ACTIVE
AT+CNACT?                                //查询注册网络成功后分配的 IP 地址
+CNACT: 0,1,"10.94.36.44"

OK
```

5 SSL 示例

5.1 建立一个普通的 TCP/UDP 连接

```
//建立一个普通的 TCP/UDP 连接

AT+CNACT=1,"cmnet"                          //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

OK

+APP PDP: ACTIVE
AT+CNACT?                                   //获取本地 IP
+CNACT: 1,"10.181.182.177"

OK
AT+CACID=0                                  //设备标识符
OK
AT+CASSLCFG=0,ssl,0                         //是否使用 SSL，如果是普通的 TCP/UDP 连接，参数为 0

OK
AT+CASSLCFG=0,protocol,0                    //设置协议类型，这里设置的 0 表示是 TCP。如果是 UDP，该位应设置为 1

OK
AT+CAOPEN=0,"116.247.119.165",5171          //建立一个 TCP 连接
+CAOPEN: 0,0                                //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

OK
AT+CASEND=0,5                               //请求发送 5 个字节数据
>                                           //输入数据
                                            //数据发送成功

OK
+CASEND: 0,0,5
+CADATAIND: 0                               //表示第 0 路有数据
AT+CARECV=0,100                             //请求获取服务器发送的 100 个字节数据
+CARECV: 0,GFDSGFDGFDSGHFDSHFDS             //输出接收到的数据

OK
AT+CACLOSE=0                                //关闭标识符为 0 的连接
```

```
OK
AT+CNACT=0                                  //断开无线连接
OK

+APP PDP: DEACTIVE
```

5.2 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。

5.2.1 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。

```
//建立一个单向认证的 SSL 连接

AT+CNACT=1,"cmnet"                          //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
OK

+APP PDP: ACTIVE
AT+CNACT?                                   //获取本地 IP
+CNACT: 1,"10.181.182.177"

OK
AT+CACID=0                                  //设备标识符
OK
AT+CSSLCFG="sslversion",0,1                 //设置标识符为 0 的 SSL 的协议类型。1 表示 TLS1.0
OK
AT+CASSLCFG=0,ssl,1                         //是否使用 SSL，1 表示开启 SSL 功能
OK
```

```
AT+CASSLCFG=0,crindex,0                    //设置协议类型
                                           //为 AT+CSSLCFG 对应的 SSL 配置的标识符
OK
AT+CASSLCFG=0,"cacert","root.pem"          //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
OK
AT+CAOPEN=0,"116.247.119.165",5171         //建立一个 SSL 连接。
+CAOPEN: 0,0                               //连接建立成功

OK                                         //第 0 路有数据，当成功建立连接或者成功发送数据
+CADATAIND: 0                              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                            //读取 100 个字节数据
+CARECV: 0,                                //输出数据
220 Serv-U FTP Server v15.0 ready...

OK
AT+CACLOSE=0                               //关闭标识符为 0 的连接
OK
AT+CNACT=0                                 //断开无线连接
OK

+APP PDP: DEACTIVE
```

5.2.2 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。

```
//建立一个双向认证的 SSL 连接

AT+CNACT=1,"cmnet"                         //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
OK

+APP PDP: ACTIVE
AT+CNACT?                                  //获取本地 IP
+CNACT: 1,"10.181.182.177"
```

```
OK
AT+CACID=0                                  //设备标识符
OK
AT+CSSLCFG="sslversion",0,1                 //设置标识符为0的SSL的协议类型。1表示TLS1.0
OK
AT+CASSLCFG=0,ssl,1                         //是否使用 SSL，1 表示开启 SSL 功能
OK
AT+CASSLCFG=0,crindex,0                     //设置协议类型
                                            //为 AT+CSSLCFG 对应的 SSL 配置的标识符
OK
AT+CASSLCFG=0,"clientcert","client.pem"     //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
OK
AT+CAOPEN=0,"116.247.119.165",5171          //建立一个 SSL 连接
+CAOPEN: 0,0                                //连接建立成功

OK
AT+CASEND=0,5                               //请求发送 5 个字节数据
>                                           //输入数据

OK                                          //数据发送成功
+CASEND: 0,0,5
AT+CACLOSE=0                                //关闭标识符为 0 的连接
OK
AT+CNACT=0                                  //断开无线连接
OK

+APP PDP: DEACTIVE
```

5.2.3 使用 AT+CSSLCFG 转换 SSL 证书

```
//使用 AT+CSSLCFG 转换 SSL 证书

AT+CSSLCFG="convert",2,"root.pem"           //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
OK
AT+CSSLCFG="convert",1,"client.pem","client //配置需要转换的证书类型，1 表示是客户端证书
.key”                                       //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”

+CNACT: 1,"10.181.182.177"

OK