Application

SIM7080 Series_TCPUDP(S)_Application Note

Version:1.01

Release Date: Feb 26, 2020

About Document

Document Information

Document	
Title	SIM7080 Series_TCPUDP(S)_Application Note
Version	1.01
Document Type	Application Note
Document Status	Released/Confidential

Revision History

Revision	Date	Owner	Status / Comments
1.00	Oct 27, 2019	Wei.zhang	First Release
1.01	Feb 26,2020	Wenjie.lai	Add product types

Related Documents

[1] SIM7080 Series_AT Command Manual_V1.02

This document applies to the following products:

Name	Type	Size (mm)	Comments
SIM7080G	CAT-M/NB	17.6*15.7 *2.3	N/A
SIM7070G/SIM7070E	CAT-M/NB/EGPRS	24*24*2.4	N/A
SIM7070G-NG	NB/EGPRS	24*24*2.4	N/A
SIM7090G	CAT-M/NB	14.8*12.8*2.0	N/A

Copyrights

Contents

1 Purpose of this document

Based on module AT command manual, this document will give an entire and complete concept and TCPIP architecture introduction.
Developers could understand and develop application quickly and efficiently based on this document.

2 SSL function

2.1 SSL Introduction

SSL (Secure Sockets Layer), a security protocol. It was put forward by Netscape in the first version of Web browser. The aim is to provide security and data integrity for network communications. SSL encrypts the network connections at the transport layer.

SSL uses public key technology to ensure the confidentiality and reliability of communication between two applications and to ensure that communication between client and server applications is not eaves dropped by attackers. It can be supported at both ends of the server and client, and has become an industrial standard for secure communication over the Internet. Current Web browsers generally combine HTTP and SSL to achieve secure communication. This Agreement and its successor are TLS (Transport Layer Security, TLS).

TLS uses key algorithm to provide endpoint authentication and communication security on the Internet, It is based on the public key infrastructure. In typical implementations, however, only the network server is authenticated reliably, while the client is not necessarily. This is because the public key infrastructure is generally commercial, and electronic signature certificates usually need to be paid for. The protocol is designed to enable master-slave architecture application communication itself to prevent tapping, tampering, and message forgery.

SIM7080 series modules currently support TLS1.0, TLS1.1, TLS1.2, DTLS1.0, DTLS1.2.

3 AT commands that support SSL's TCP/UDP

The module provides AT commands that can be used by device terminals as follows:

Command	Description
AT+CACFG	Set TCP/UDP parameters
AT+CASSLCFG	Set SSL parameters
AT+CAOPEN	Open a TCP/UDP connection
AT+CASEND	Send data via an established connection

AT+CARECV	Receive data via an established connection
AT+CACLOSE	Close a TCP/UDP connection
AT+CSSLCFG	Configure SSL parameters of a context identifier
AT+CASERVER	Open a TCP/UDP Server

For detail information, please refer to “SIM7080 Series_AT Command Manual”.

4 Test cases

4.1 PDN Auto-activation

AT Command	Response	Description
AT+CPIN?	+CPIN:READY OK	Check SIM card status
AT+CSQ	+CSQ: 20,0 OK	Check RF signal
AT+CGATT?	+CGATT: 1 OK	Check PS service. 1 indicates PS has attached.
AT+COPS?	+COPS: 0,0,"CHN-CT",9 OK	Query Network information, operator and network mode 9, NB-IOT network
AT+CGNAPN	+CGNAPN: 1,"ctnb" OK	Query CAT-M or NB-IOT network after the successful registration of APN
AT+CNCFG=0,1,”ctnb”	OK	Configure PDP 0th , network type ipv4/v6,APN is “ctnb”
AT+CNACT=0,1	OK +APP PDP: 0,ACTIVE	Activate network, Activate 0th PDP.

4.2 Build an ordinary TCP/UDP connection

AT Command	Response	Description
AT+CNCFG=0,1,”ctnb”	OK	Configure PDP 0th,network type ipv4/v6,APN is “ctnb” PDP, this needs to set different APN values according to different cards.
AT+CNACT=0,1	OK	Activate network, Activate 0th PDP.

	+APP PDP: 0,ACTIVE	
AT+CNACT?	+CNACT: 0,1,"10.181.182.177" +CNACT: 1,0,"0.0.0.0" +CNACT: 2,0,"0.0.0.0" +CNACT: 3,0,"0.0.0.0" OK	Get local IP
AT+CASSLCFG=0,"SSL",0	OK	Set the 0th connection's SSL enable option. If TCP/UDP connection, the parameter is 0.
AT+CAOPEN=0,0,"TCP", "117.131.85.139",6004	+CAOPEN: 0,0 OK	Create a TCP connection with 0th PDP on 0th connection. Return to URC the first parameter is the identifier, the second parameter is the result of the connection, and the 0 indicates success.
AT+CASEND=0,5	> OK +CASEND: 0,0,5	Request to send 5 bytes of data Input data Data sent successfully
	+CADATAIND: 0	Data come in on 0th connection.
AT+CARECV=0,100	+CARECV: 10,GET / HTTP OK	Request to get 100 byte data sent by the server. Output received data
AT+CACLOSE=0	OK	Close the connection with an identifier of 0.
AT+CNACT=0,0	OK +APP PDP: 0,DEACTIVE	Disconnect 0th data connection

4.3 Build a TCP/UDP connection with SSL

When SSL establishes communication, it is necessary to verify the identity of both sides of the communication, which is divided into one-way authentication and two-way authentication.

One way authentication is the client to verify the certificate of the server. The server sends the server certificate to the client. The client verifies that the root certificate that issued the server certificate is trustworthy, and if so continues the communication process.

After the two-way authentication client verifies the server certificate, the client needs to send its own certificate to the server and let the server verify its client certificate. The validation process is the same, all need to confirm whether the root certificate of the certificate can be trusted.

4.3.1 Build a one-way authentication SSL(TLS) connection

Because of modules can only serve as clients. When you need to establish a one-way authentication connection, you need to import the root certificate of the server. If no certificate is imported, the module will default that all the servers can be trusted.

AT Command	Response	Description
AT+CNCFG=0,1,"ctnb"	OK	Configure PDP 0th,network type ipv4/v6,APN is "ctnb" PDP, this needs to set different APN values according to different cards.
AT+CNACT=0,1	OK +APP PDP: 0,ACTIVE	Activate network, Activate 0th PDP.
AT+CSSLCFG="SSLVERSION",0,3	OK	Set the protocol type of SSL with an identifier of 0. 3 indicate TLS1.2
AT+CASSLCFG=0,"SSL",1	OK	Whether to use SSL, 1 means to turn on the SSL function.
AT+CASSLCFG=0,"CRINDEX",0	OK	Set protocol type. Identifier for AT+CSSLCFG corresponding SSL configuration.
AT+CASSLCFG=0,"CACERT","root.pem"	OK	Set root certificate. The root certificate must be a certificate that has been converted through AT+CSSLCFG. This item can be omitted. If omitted, all server certificates are trusted by default.
AT+CAOPEN=0,0,"TCP","117.131.85.139",6005	+CAOPEN: 0,0 OK + CADATAIND: 0	Create a SSL connection with 0th PDP on 0th connection identifier Connection success Data come in on 0th connection. When a connection is successfully established or data is successfully sent, the module actively reads the data once, and if the server data is received, the URC is reported. If no data is received, the URC will not be reported.
AT+CARECV=0,100	+CARECV: 10,GET / HTTP OK	Read 100 byte data Output data
AT+CASEND=0,5	> OK +CASEND: 0,0,5	Request to send 5 bytes of data Input data Data sent successfully
AT+CACLOSE=0	OK	Close the connection with an identifier of 0.
AT+CNACT=0,0	OK +APP PDP: DEACTIVE	Disconnect data connection

4.3.2 Build a two-way authentication SSL(TLS) connection

To establish a two-way authentication SSL connection, you need to set up a client certificate. The client certificate needs to be transformed through "AT+CSSLCFG" first.

The certificate format that the module can support is .PEM, .DER and .P7B.

AT Command	Response	Description
AT+CNCFG=0,1,"ctnb"	OK	Configure PDP 0th,network type ipv4/v6,APN is "ctnb" PDP, this needs to set different APN values according to different cards.
AT+CNACT=0,1	OK +APP PDP: 0,ACTIVE	Activate network, Activate 0th PDP.
AT+CSSLCFG="SSLVERSION",0,3	OK	Set the protocol type of SSL with an identifier of 0. 3 indicate TLS1.2
AT+CASSLCFG=0,"SSL",1	OK	Set the 0th connection's SSL enable option. Whether to use SSL, 1 means to turn on the SSL function.
AT+CASSLCFG=0,"CRINDEX",0	OK	Identifier for AT+CSSLCFG corresponding SSL configuration.
AT+CASSLCFG=0,"CACERT","root.pem"	OK	Set root certificate. The root certificate must be a certificate that has been converted through AT+CSSLCFG. This item can be omitted. If omitted, all server certificates are trusted by default.
AT+CASSLCFG=0,"CERT","client.pem"	OK	Set up client certificates. The root certificate must be converted to a certificate that can be directly used by AT+CSSLCFG.
AT+CAOPEN=0,0,"TCP","117.131.85.139",6005	+CAOPEN: 0,0 OK	Create a SSL connection with 0th PDP on 0th connection identifier. Connection success
AT+CASEND=0,5	> OK +CASEND: 0,0,5	Request to send 5 bytes of data Input data Data sent successfully
AT+CACLOSE=0	OK	Close the connection with a connection identifier of 0.
AT+CNACT=0,0	OK +APP PDP: 0,DEACTIVE	Disconnect 0th PDP

4.3.3 Build a PSK authentication SSL (DTLS)connection

To establish PSK DTLS connection, you need to set up a psktable. The psktable needs to be transformed through "AT+CSSLCFG" first.

The psktable file format and how to convert, see section 4.3.4.

AT Command	Response	Description
AT+CNCFG=0,1,"ctnb"	OK	Configure PDP 0th, network type ipv4/v6,APN is "ctnb" PDP, this needs to set different APN values

		according to different cards.
AT+CNACT=0,1	OK +APP PDP: 0,ACTIVE	Activate network, Activate 0th PDP.
AT+CSSLCFG="SSLVERSION",0,5	OK	Set the protocol type of SSL with an identifier of 0. 5 indicate DTLS1.2
AT+CASSLCFG=0,"SSL",1	OK	Whether to use SSL, 1 means to turn on the SSL function.
AT+CASSLCFG=0,"CRINDEX",0	OK	Set protocol type Identifier for AT+CSSLCFG corresponding SSL configuration
AT+CASSLCFG=0,"PSKTABLE","psktable.secrets"	OK	Select psktable configure file. The psktable must be a file that has been converted through AT+CSSLCFG. This item does not be omitted, If the server uses PSK Cipher Suites.
AT+CAOPEN=0,0,"UDP","117.131.85.139",6013	+CAOPEN: 0,0 OK + CADATAIND: 0	Create a SSL connection with 0th PDP on 0th connection identifier. Connection success Data come in on 0th connection. When a connection is successfully established or data is successfully sent, the module actively reads the data once, and if the server data is received, the URC is reported. If no data is received, the URC will not be reported.
AT+CARECV=0,100	+CARECV: 10,GET / HTTP OK	Read 100 byte data Output data
AT+CACLOSE=0	OK	Close the connection with an identifier of 0.
AT+CNACT=0,0	OK +APP PDP: DEACTIVE	Disconnect data connection

4.3.4 Transform SSL certificates

AT Command	Response	Description
AT+CSSLCFG="CONVERT",2,"root.pem"	OK	Configuring the type of certificate to be converted, and 2 is a root certificate. Configure the name of the certificate to be converted, and the name after the conversion is consistent with the existing certificate name.
AT+CSSLCFG="CONVERT",1,"client.pem","client.key"	OK	Configure the type of certificate to be converted, and 1 is client certificate. Configure the certificate name that needs to be converted, and the client certificate needs to enter the certificate file and the private key file.

		The name after conversion is identical to the name of the certificate, that is "client.pem".
AT+CSSLCFG="CONVERT",3,"psktable.secrets"	OK	Configure the type of psktable to be converted, and 3 is psktable. The psktable file format as follows: <Identity_1>:<psk_key1> <Identity_2>:<psk_key2> e.g. user_zhang:303132333435363738 The Identity is sting type and psk_key is hexadecimal string(e.g. If the psk is string "123", you must write that "313233")

4.4 Build an TCP/UDP Server

4.4.1 Build TCP Server

AT Command	Response	Description
AT+CNCFG=0,1,"ctnb"	OK	Configure PDP 0th, network type is ipv4/v6, APN is "ctnb" PDP, this needs to set different APN values according to different cards.
AT+CNACT=0,1	OK +APP PDP: 0,ACTIVE	Activate network, Activate 0th PDP.
AT+CASERVER=0,0,"TCP",6000	+CASERVER: 0,0 OK +CANEW: 0,1,117.131.85.139,5004 + CADATAIND: 1	Create TCP server with 0th PDP on port 6000 of 0th connection Create success Have a new client access on 0th connection and the client has been assigned to 1th connection. Date come in on 1th connection.
AT+CARECV=1,100	+CARECV: 10,GET / HTTP OK	Read 100 byte data Actual output 10 byte data
AT+CASEND=1,5	> OK +CASEND: 1,0,5	Request to send 5 bytes of data Input data Data sent successfully
AT+CACLOSE=1	OK	Close the connection with a connection identifier of 1.
AT+CACLOSE=0	OK	Close the connection with a connection identifier of 0.

AT+CNACT=0,0	OK +APP PDP: DEACTIVE	Disconnect 0th PDP

4.4.2 Build UDP Sever

AT Command	Response	Description
AT+CNCFG=0,1,"ctnb"	OK	Configure PDP 0th,network type ipv4/v6,APN is "ctnb" PDP, this needs to set different APN values according to different cards.
AT+CNACT=0,1	OK +APP PDP: 0,ACTIVE	Activate network, Activate 0th PDP.
AT+CASERVER=0,0,"TCP",6000	+CASERVER: 0,0 OK +CANEW: 0,1,117.131.85.139,5004 +CADATAIND: 1	Create TCP server with 0th PDP on port 6000 of 0th connection Create success Have a new client access on 0th connection and the client has been assigned to 1th connection. Data come in on 1th connection.
AT+CARECV=1,100	+CARECV: 10,GET / HTTP OK	Read 100 byte data Actual output 10 byte data
AT+CASEND=1,5	> OK +CASEND: 1,0,5	Request to send 5 bytes of data Input data Data sent successfully
AT+CACLOSE=1	OK	Close the connection with a connection identifier of 1.
AT+CACLOSE=0	OK	Close the connection with a connection identifier of 0.
AT+CNACT=0,0	OK +APP PDP: DEACTIVE	Disconnect 0th PDP

Contact

SIMCom Wireless Solutions Co.,Ltd

Address: Building B, No.633 Jinzhong Road, Changning District, Shanghai P.R.China 200335
Tel: +86-21-31575126
Support: support@simcom.com